ID: 356388
Cookbook: browseurl.jbs
Time: 03:50:41
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

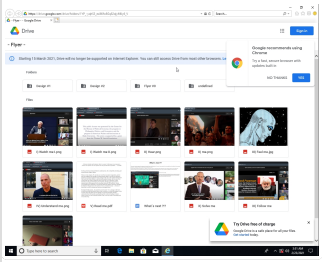
Analysis Report https://drive.google.com/drive/folders/1...

Overview

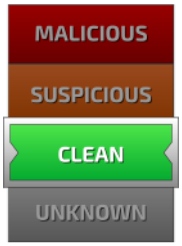
General Information

Sample URL:	http://https://drive.google.com/drive/folders/1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V
Analysis ID:	356388

Most interesting Screenshot:



Detection

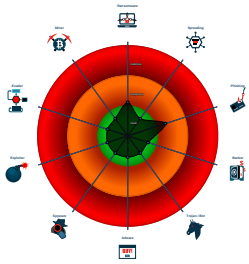


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6968 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 7032 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6968 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

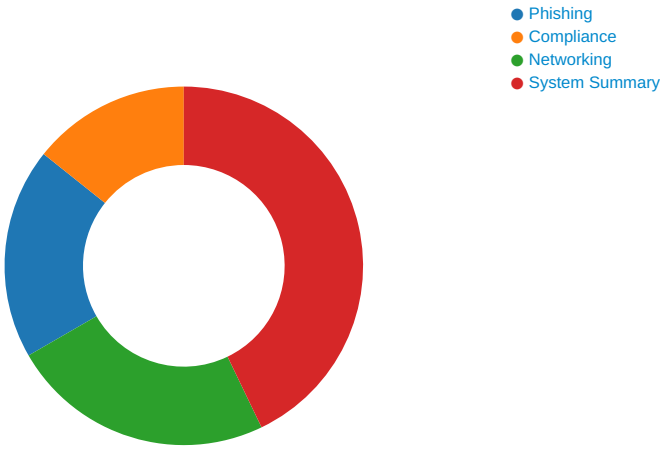
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Mitre Att&ck Matrix

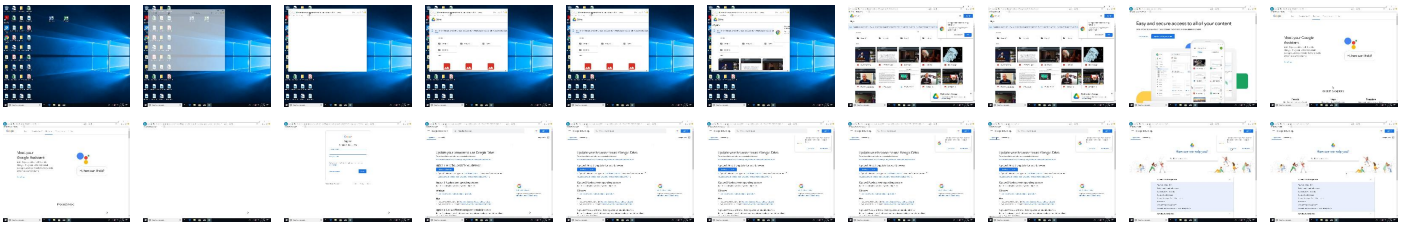
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

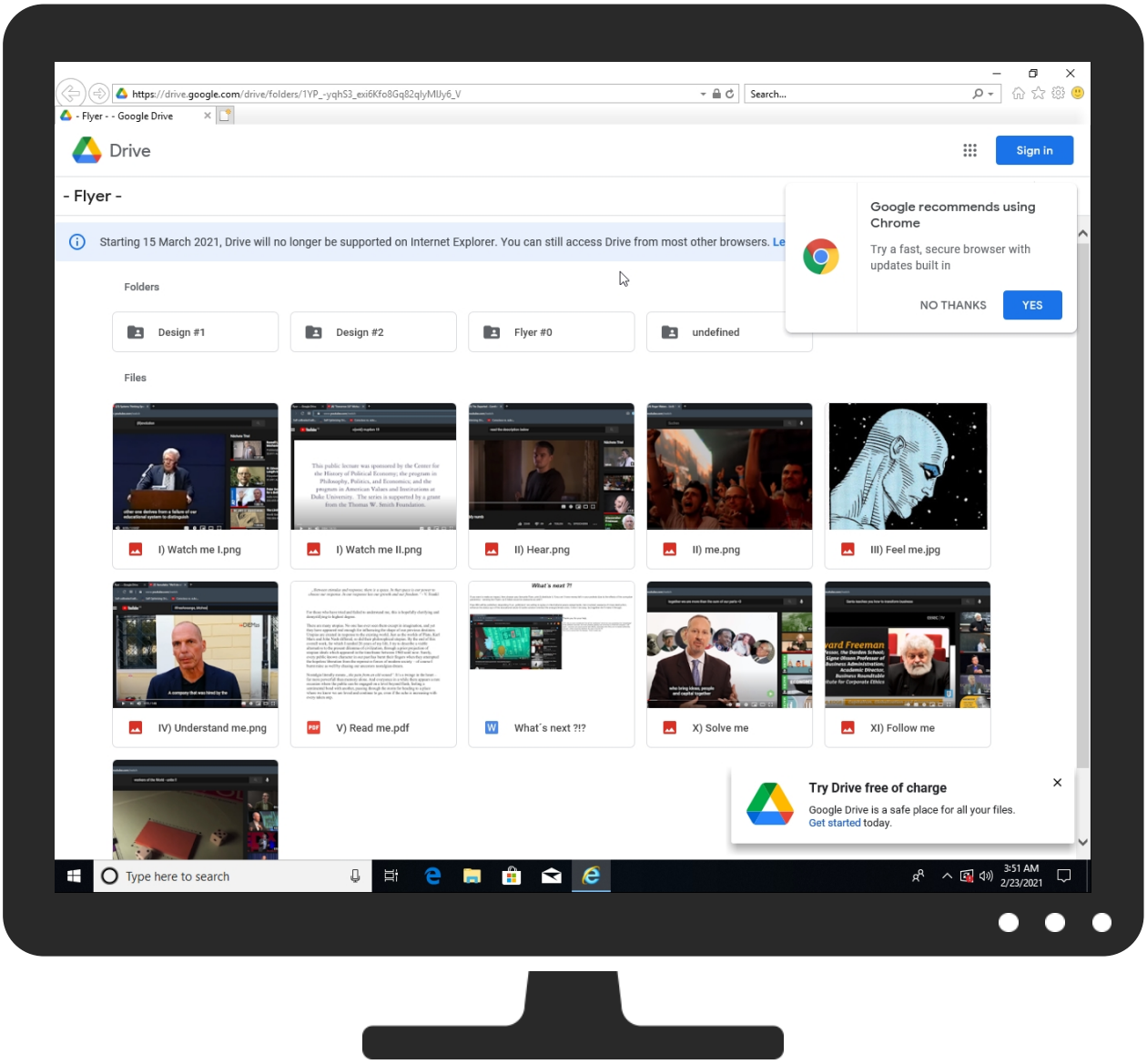
Behavior Graph

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://drive.google.com/drive/folders/1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V	0%	Virustotal		Browse
http://https://drive.google.com/drive/folders/1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
www.google.co.uk	0%	Virustotal		Browse
ghs-svc-https-sni.ghs-ssl.googlehosted.com	0%	Virustotal		Browse
about.google	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en/about/products?tab	0%	URL Reputation	safe	
http://https://about.google/favicon.ico~	0%	URL Reputation	safe	
http://https://about.google/favicon.ico~	0%	URL Reputation	safe	
http://https://about.google/favicon.ico~	0%	URL Reputation	safe	
http://https://about.google/favicon.ico~	0%	URL Reputation	safe	
http://https://wellbeing.google	0%	URL Reputation	safe	
http://https://wellbeing.google	0%	URL Reputation	safe	
http://https://wellbeing.google	0%	URL Reputation	safe	
http://https://wellbeing.google	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/finance?tab	0%	URL Reputation	safe	
http://https://pixel.google/business/	0%	Avira URL Cloud	safe	
http://https://maps.google.co.uk/maps?hl	0%	URL Reputation	safe	
http://https://maps.google.co.uk/maps?hl	0%	URL Reputation	safe	
http://https://maps.google.co.uk/maps?hl	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://tv.google/	0%	Avira URL Cloud	safe	
http://https://about.google/intl/en-GB/products/?tab=ohexi6Kfo8Gq82qIyMlJy6_V	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://www.google.co.uk/intl/en-GB/about/products?tab	0%	URL Reputation	safe	
http://https://sketch.com	0%	URL Reputation	safe	
http://https://sketch.com	0%	URL Reputation	safe	
http://https://sketch.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pagead46.l.doubleclick.net	216.58.212.130	true	false		high
www.google.co.uk	142.250.186.67	true	false	• 0%, Virustotal, Browse	unknown
ghs-svc-https-sni.ghs-ssl.googlehosted.com	216.58.212.179	true	false	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
kstatic.googleusercontent.com	35.241.11.240	true	false		high
about.google	216.239.32.29	true	false	• 0%, Virustotal, Browse	unknown
www.blog.google	unknown	unknown	false		high
accounts.youtube.com	unknown	unknown	false		high
drive-thirdparty.googleusercontent.com	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://staging-realtimesupport-googleapis.sandbox.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://www.google.co.uk/intl/en/about/products?tab	so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://about.google/favicon.ico~	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.youtube.com/user/googlehelp?sub_confirmation=1	6283888[1].htm.2.dr	false		high
http://lh3.ggpht.com	L4FCQBHD.js.2.dr	false		high

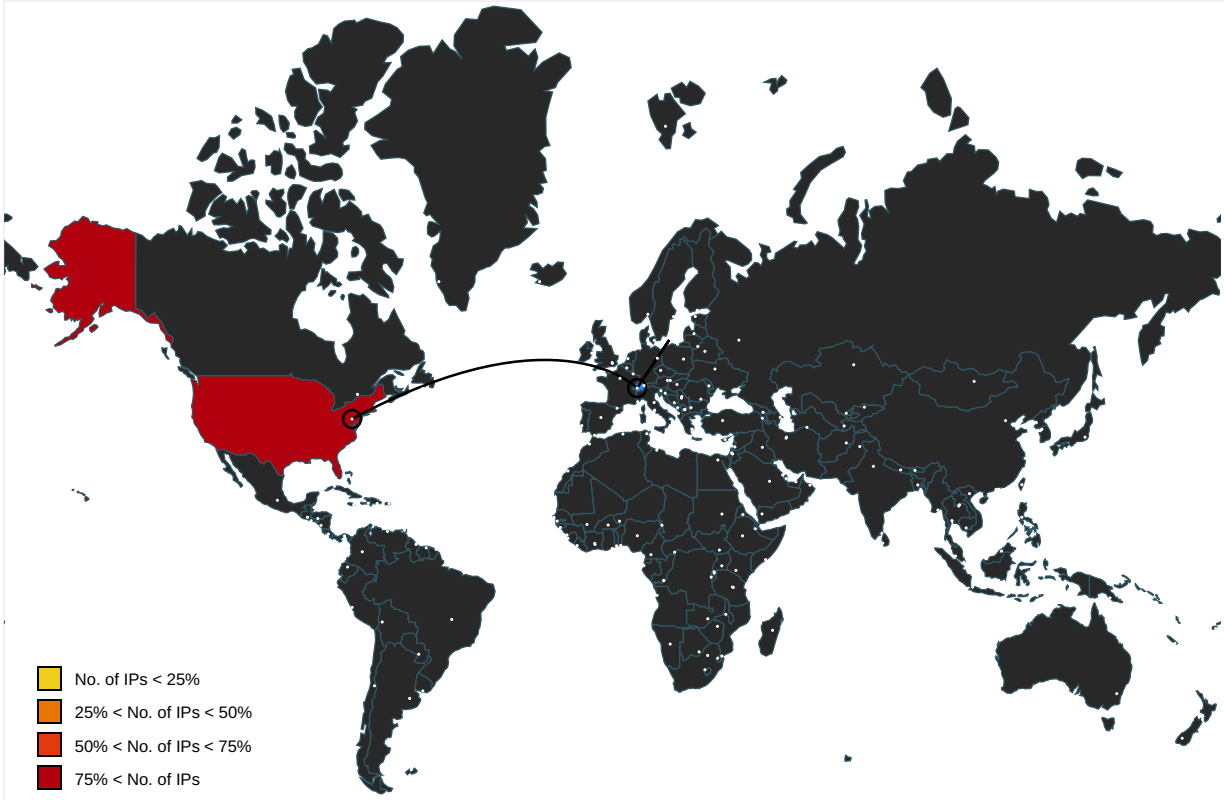
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/JgSh5ERmn7HG3qq2q0QIT_mr81ypzkxlWhr6F0kL9mKYgEMr6IlqFXBBchcOt7XVGO	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/Qvc6rWiGG_a6LNQ7Yx5vMmve_5ku8TG7z4vmWG7VBkbcOQfOSE2BS7eBcD1NUOWTsb	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/9NuRdiRepVI3n1txfg7Ky2wWzB3DvXkWABXeFMSn2tzDYYkv8T_RMA9R17fWi0ziUD	products[2].htm.2.dr	false		high
http://https://wellbeing.google	products[2].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://kstatic.googleusercontent.com/files/540ac1df440f3a3708b6f31b7fa0c4fd7fd4471dc0614cab5482e110	drive[1].htm.2.dr	false		high
http://https://www.android.com/intl/en_uk/play-protect/	products[2].htm.2.dr	false		high
http://https://instagram.com/$1	main.min[1].js.2.dr	false		high
http://https://lh3.googleusercontent.com/XLXz2efC7k6vYBTRN0yrrmuT8NHG1M-rmGYFlzBw0mzuQE-J9prHLgb50S-Er2TqQP	products[2].htm.2.dr	false		high
http://https://www.google.co.uk/finance?tab	so[1].htm.2.dr, so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://about.google/intl/en-GB/products/?tab=oh	{036910D3-7582-11EB-90EB-ECF4BBEA1588}.dat.1.dr, ~DFFDB6A73FD4315454.TMP.1.dr	false		unknown
http://https://lh3.googleusercontent.com/I95wjYii8vhFSSx-aSYdh2hPAMjgZkA9yjarSQoOd98COwOxkAVn_dulBcTcfbsa7L	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/hUIKh_wtukvD7GcdxBFSGj8ztVY2UXtHXe_kxcooyBYZk58BdguEORmhqJg9Zh4dQT	products[2].htm.2.dr	false		high
http://https://www.youtube.com	L4FCQBHD.js.2.dr	false		high
http://https://www.blog.google/products/pixel/google-pixel-3/	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/JtYUq9HfkkOryxudgp34oqI8qFu9a6mmL64OXjcDX7mfEwcX_pxmTdurvxssofY4sw	products[2].htm.2.dr	false		high
http://https://twitter.com/hashtag/	main.min[1].js.2.dr	false		high
http://https://pixel.google/business/	products[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/33fCN1bFbB2G1iGDGzlBd_BAWes-Nlv-Qt8ByRpEBU43Lu_mF6twx5kmmN4OE6Z_Gz	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/5WLz7CvnjBuQDDrFDsJW0EMrL-r6a-b0YUhF48zk7l4lK3yLzhBzeG3I01KIycLfE-	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/8bC8ZC9RQ_cJj5lSa8LjCfRClGeSyp4SkN72C0tMSUIqGPVjEpHeUDfAScLNKy82Mi	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/wGnSqicvbFincaZcKqlQO1bhdtbhEuYYGAPrdSjmljz0TAJzokpnjs9Yc3q_RMMvVW	products[2].htm.2.dr	false		high
http://scrollmagic.io	ScrollMagic.min[1].js.2.dr	false		high
http://https://lh3.googleusercontent.com/u2XGSr0jis3w5sLeuh8UMqGHgtdqPVPi77xYhPJdMO9C41wYUue3EKPJvwp-ovAlTz	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/z3dgQsXgGqfadzIUmpGI_poIUy7H6fgqIbtW_qzLXcBww0nOby8TEE3e_fW84Qa7z	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/7_OgzDSggIvMvDRN2idJKkslPU439TrrHqPpmJ20UqynnvG6Es8csy2eABIScl5_wT	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/gi7EU_u6liuIRSxunfy5LLqsEJrC08L12aufZc3rP_w8hD8ouiVW89vfe7pTQrSsLX	products[2].htm.2.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/	m=b[1].js.2.dr	false		high
http://https://lh3.googleusercontent.com/q6qMZrrMLLqdCto6icsSvaZVetRFFAcTw2YjAAQnA_M5eEyQhBomDBuEYo8h0utfCN	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/Y1i12gHz-cP0Ir3LztFSUMijuVGSe9qetVu98aQNchjhxw9byxecnFAFfhxGFyd79t	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/aMTzdOYbB8kBrLq-k5PesENOhnr-7qtytONnM1GOl-drEs9jvyhYJDNaN9-n_Am7rZ	products[2].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/c8RAvBBD-WtA4UuEGqUBkwaIvLQm5JvWZcGyD4aoVnilh2423ADEQo0i8SKppTakye	products[2].htm.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	analytics[1].js.2.dr	false		high
http://https://lh3.googleusercontent.com/Jqo0sXz5HJpnbEwCf5qwcWSbwXbKiivjx2e1WpRjAg3pAPaj2DiOHs42I1zwyhvtXd	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/Pk8YenR3VOTvN9iNHAGWp3pWYZiaYMXXWUkfAjt_LMrf222t9zn815V-GfMRJ1Hjgq	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/vT9C73tlLqkcLZfHuDlr5LJkCqOiKb5hiZxXTeWbbgTpkyguhmI-h6ujB0F8KdHnld	products[2].htm.2.dr	false		high
http://https://drive-customization.virtru.com/current.html	1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V[1].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/tC78k3bL_DjdIByD4HSnnblCZF0nlR599IWYDDghEJDn7dwg-tuOIXGVR1TwxePI06	products[2].htm.2.dr	false		high
http://https://www.blog.google/products/gmail/5-ways-new-gmail-can-help-you-get-more-done/	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/UqZcYFgfFclRU46MshhuCQD79idBZ8hyIe5WkQ1VLzG47w-Mgu6yGriGkL_YiYF2qa	products[2].htm.2.dr	false		high
http://https://www.google.org	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/9ks6e2i7ubrVUEkBwpoJeXTceixbWT3ppLdca04jQg6VPMqXiz6B8KEeczJhnRWmjR	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/TVNK8r0QEiNhXwfjVlziAqFcBQPkuPHKyilz6atnzslwMho1no8n4EJV30tOT0T6y3	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/inMunrmxQKU2dsDv0PT1JaELzFlTn5ASRr_dBzGbAZj5Kcqk7TqXJZiP7duVgQFUVx	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com	1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V[1].htm.2.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/16/type/image/jpeg	1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V[1].htm.2.dr	false		high
http://https://drive-customization-develop01.develop.virtru.com/current.html	1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V[1].htm.2.dr	false		high
http://https://www.g2.com/	drive[1].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/Iyn9yCCDxgHqvjX5jMZ_looun-kL0Sk60FraoMU5-JQG2WstyK6QNzj3JguQRbvQmW	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/9CAaLlPoQ9YB_HQXK9B8e80czwAhK22t_eA7pxvRHaydwo33SKlVtpccCwGWSj6gR7	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/m5HIvqrNJHr2w5VXuNapBWKSx6YZTU7llhffkIgDQU_VbpYAfkgXt2Un2ks_wzTn7v	products[2].htm.2.dr	false		high
http://https://maps.google.co.uk/maps?hl	so[1].htm.2.dr, so[1].htm0.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.docusign.com/partner/docusign-google-drive	drive[1].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/RRrLsW4MKWRjEePTK_VmuWzXVWn20fnY1R3CfspbNMObSv-cb5mb4GxiOGOSehSOEq	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/PVDn9Oj6dMbqqydywzGuLAPkbLwDX3Uuv1t6K8MORXFuQAVBLPNAy_yaQBc7bE-qmL	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/DaeHJ1cE8YmvDBsBfBOxacn27nsLy35yHgxW41xMHbQbgmCrEd6GAMYWBY9ucReiZD	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/PP8KjNgc-EqOm5a6yZ1w6mqbFzoyzLfCZcjhmRvWn6imgVjCiPj9j_MKz6jJuggsro	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/RVN6CEbRo-JWFNzAUUo25416-ggk6Pa1JcTIUBclXVozbY7HwFbifurANGg3TqXmsz	products[2].htm.2.dr	false		high
http://https://www.blog.google/press/	products[2].htm.2.dr	false		high
http://https://about.google/favicon.ico	imagestore.dat.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/2qz9gwasYkOhPEumfqd3_x8HiiRu6flQR1d-1DRAV8qfkqmQx7Rygzohal7DXbB-ur	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/XuX--BV0zkkLgxF4L5fJ0A1zg1yqjZ5TRyjEyaKMg873pOoy04PFwpUeUNw9kDpeoc	products[2].htm.2.dr	false		high
http://https://www.waze.com/	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/i84lgLkRUH_h2PLjUYVEcp5cLv_9vR3_mvAjyGnrUoQnJKtlf_kgHROEvA24fY6xzR	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/sdgJP4Hp6YRDQeEwjfR_mlb6hDuSXkyWPDq_PhpKYOTmOM_oMQ5Mxu9WD23dZU0bVQ	products[2].htm.2.dr	false		high
http://https://tv.google/	products[2].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://kstatic.googleusercontent.com/files/8317f83271acdf124799a6f1888da1313d29696309f46e1876ad3216	drive[1].htm.2.dr	false		high
http://https://kstatic.googleusercontent.com/files/667fa0a2a1aa16fb1a877a3b3f2725cc03b156c36f458422c4279744	drive[1].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/kMpf6E3q3k3eVJtZPHDEN5wmzCX6sXXss1EySWWF3c-MG4cMgO5vBMypNdkH394LIt	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/vNgpLTvnDUr6-QM8s4OuuESGDXs_brbGoPR-7vfwdxQI7M4MVFV0CC_Hil4qRDSp4P	products[2].htm.2.dr	false		high
http://https://www.android.com/intl/en_us/	products[2].htm.2.dr	false		high
http://https://www.youtube.com/yt/about/	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/mK6uPlO8TKCVSU8TsniV0pOUB0SSETbAPB_QUaaJ96qbBdZwaygmzf_bWRTIHmCNKg	products[2].htm.2.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/16/type/application/vnd.openxmlformats-officedocument	YZ6L1DZT.js.2.dr	false		high
http://https://help.salesforce.com/articleView?id=admin_files_connect_google_xds.htm&type=5	drive[1].htm.2.dr	false		high
http://lh4.ggpht.com	L4FCQBHD.js.2.dr	false		high
http://https://lh3.googleusercontent.com/BAwQk6jAMu2s_7Jh-8-_CsvSwEAaeLsVhL8z82VOoEkoaujxll1kYL3Pz4jkYpLbRp	products[2].htm.2.dr	false		high
http://https://staging-casespartner-pa-googleapis.sandbox.youtube.com	operatordeferred_bin_base__en[1].js.2.dr	false		high
http://https://lh3.googleusercontent.com/6xlGJ-dkwosfUisVYzRKNE1Wcr5QDDfRfZ4bXktF-Nn0J0ucHd_Jl1wjXTls7lt5mv	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/wbRbWxRbQyojtDDUj_ITsoMZNbSAnroic0AYABmbab8qE-sgODk26wLCYUcJrqW11-	products[2].htm.2.dr	false		high
http://https://abc.xyz/investor/	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/_RS8nTX8HLPW-dDr374dEdQTaYn-7LI8HVVk0INaAmk7t8MYZKDssvGnep-GwPR94L	products[2].htm.2.dr	false		high
http://https://about.google/intl/en-GB/products/?tab=ohexi6Kfo8Gq82qIyMlJy6_V	~DFFDB6A73FD4315454.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/HUcJ2yilLdMblMI04h5DE1tf_0iCxgOmiu-7mpulXRJTol_vVsnrlQcs4esQq1ygtH	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/ra4Ks1fsGsLSlzWoAU-9Ls2V5vEFCsA9thbtIkCHNFYeLC-ver57N4-GCGFZ-GBGw6	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/oJtxC9wrYYcStJ4Ds2ylblE6GyJtbi_HWy01cp88xJGkrELh-SZ6N-kdrMmRglHFy7	products[2].htm.2.dr	false		high
http://https://kstatic.googleusercontent.com/files/1215f100aed56568e58a202bef5caf51ebcc316ed033a7d042d6d6c1	drive[1].htm.2.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/16/type/application/vnd.google-apps.presentation	YZ6L1DZT.js.2.dr	false		high
http://https://lh3.googleusercontent.com/gi7X34TTW6Uy2F1aiwO9N5GHmkftlVOmfdvWRKUrK3ASh4LV3cKMn-cIJKMj0AiLwV	products[2].htm.2.dr	false		high
http://https://lh3.googleusercontent.com/QCApHf5BOpvrWAy9bUSGjE8SNIcWHZkY3rvo35SMCQrQA5clvXy2HK1Rb5Ogo_htBD	products[2].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://drive-thirdparty.googleusercontent.com/128/type/application/vnd.oasis.opendocument.text	1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V[1].htm.2.dr	false		high
http://https://www.google.co.uk/intl/en-GB/about/products?tab	so[1].htm.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sketch.com	Atlassian_01[1].svg.2.dr, logo_Salesforce (1)[1].svg.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://kstatic.googleusercontent.com/files/686902a5a73584f00448ecb41b20642e6a67bb8a30856e62f31cec5a	drive[1].htm.2.dr	false		high
http://https://signaler-pa.youtube.com	operatordeferred_bin_base__en[1].js.2.dr, m=sy154,sy151,sy153,sy155,sy152,change[1].js.2.dr	false		high
http://https://kstatic.googleusercontent.com/files/7f3a6ff42f9b19117c333a2cecdb09c083cdc5ef945fd616124dd56b	drive[1].htm.2.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.130	unknown	United States		15169	GOOGLEUS	false
35.241.11.240	unknown	United States		15169	GOOGLEUS	false
142.250.186.33	unknown	United States		15169	GOOGLEUS	false
216.239.32.29	unknown	United States		15169	GOOGLEUS	false
216.58.212.179	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356388
Start date:	23.02.2021
Start time:	03:50:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://drive.google.com/drive/folders/1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@3/318@7/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://drive.google.com/?tab=oo • Browsing link: https://www.google.co.uk/intl/en-GB/about/products?tab=oh • Browsing link: https://accounts.google.com/ServiceLogin?hl=en-GB&passive=true&continue=https://drive.google.com/drive/folders/1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V&service=writely&ec=GAZAMQ • Browsing link: https://support.google.com/drive/?p=unsupported_browser

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.113.196.254, 13.107.3.254, 13.107.246.254, 40.88.32.150, 168.61.161.212, 52.147.198.201, 88.221.62.148, 142.250.74.206, 142.250.185.142, 142.250.186.67, 142.250.185.234, 142.250.186.131, 142.250.185.227, 142.250.185.163, 216.58.212.141, 142.250.185.238, 142.250.185.206, 142.250.185.164, 172.217.23.110, 142.250.185.74, 13.88.21.125, 51.104.139.180, 216.58.212.174, 142.250.186.104, 142.250.186.170, 152.199.19.161, 142.250.186.42, 142.250.185.208, 142.250.185.240, 142.250.186.48, 142.250.186.112, 142.250.186.144, 142.250.186.176, 216.58.212.144, 142.250.185.80, 142.250.185.112, 142.250.185.174, 142.250.186.138, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.gstatic.com, arc.msn.com.nsatc.net, storage.googleapis.com, s-ring.msedge.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, realtimesupport.clients6.google.com, drive.google.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, www.google-analytics.com, fonts.googleapis.com, plus.l.google.com, ajax.googleapis.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, clients4.google.com, skypedataprdcolcus17.cloudapp.net, s-ring.s-9999.s-msedge.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, www3.l.google.com, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, clients.l.google.com, t-ring.t-9999.t-msedge.net, people-pa.clients6.google.com, cs9.wpc.v0cdn.net, scone-pa.clients6.google.com, clients6.google.com, support.google.com, ogs.google.com, adservice.google.com, a1449.dscg2.akamai.net, arc.msn.com, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, go.microsoft.com, www.googletagmanager.com, id.google.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, www-googletagmanager.l.google.com, t-ring.msedge.net, skypedataprdcoleus16.cloudapp.net, play.google.com, go.microsoft.com.edgekey.net, gstatic.com, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, apis.google.com, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BACZYXTY\accounts.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	255
Entropy (8bit):	4.640237897456458
Encrypted:	false
SSDEEP:	6:JFK1rUFWcqa/0ewulek1rUFxmAq930ewulek1rUFxmAq930ewulekb:JsrUua/2uosrUna932uosrUna932uoS
MD5:	6BB0A91F3AB76B8CA09FA035DEA31EEB
SHA1:	2C5436173932 92EEE58D2A7B2CC7B60AEA5D88AC
SHA-256:	47F3BE34C1F1491447F609E95B8BAF12941D074BB7E6A588B6B9C38AE2199354
SHA-512:	ED7E5C7B4222DA55C29F1D2717BE6831A069B3150107611ADF62E6AC8B5EC6CC7D574434E3989C272066249CF5F5E7073821B53D713A919ECEFFA03491A4250F
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="__sak" value="1" ltime="3667375008" htime="30869902" /></root><root><item name="promo" value="{}" ltime="3667375008" ht ime="30869902" /></root><root><item name="promo" value="{}" ltime="3667375008" htime="30869902" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BC6XF3KU\support.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3880
Entropy (8bit):	5.016293594210251
Encrypted:	false
SSDEEP:	48:1fFJcZ/eUjTgqkKfFJcZ/eUjTgqkKfFJcZ/eUjTgqkKfqkKff:BF6lPTgqkIF6lPTgqkIF6lPTgqkIqkIf
MD5:	87AB41942C6F655D97704E02D982EC79
SHA1:	3481BF13D1BF7F1B7863DA79A5A3FAB3C064184D
SHA-256:	5726B2B51C8D4DEE6512EABEE64F5B0D01BAC1332212D7FEAF5E3D67E1591048
SHA-512:	3602A8E9EDC340CD035DA8B96C13737191CD11B35A45BE1674FBE01EBC3F08FC9456AC82279BE95BDC2ACB6244DA428A21799978223083300D04E01ED9FB58C D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BC6XF3KU\support.google[1].xml	
Preview:	<root></root><root></root><root></root><root><item name="refererViewId" value="1805964885" ltime="3836635008" htime="30869902" /><item name="StatsDeferredClearcut" value="[["webdrive","en",[[55,[]]],[],[],null,null,[],null,null,null,"en",[],1,17515,[],1,null,1,[],[10800235,10800244,10800253,10800284,10800286,10800300,10800303,10800352,10800380,10800403,10800485,10800552,10800561,10800589,10800621,10800635,10800639,10800112],null,null,"drive",null,null,[],null,null,null,null,1,[[4,["6283888",1805964885,1,[]],null,null,[1,32,8,"https://support.google.com/drive/?hl=en"],[],[],null,0]],"637496455200913679-1909421549",2,null,null,false,null,null,"GB",[],1,null,22,3,null,null,1805964885,null,null,null,1,null,2,[]],"support.google.com"]" ltime="3836635008" htime="30869902" /><item name="ScaledStatsDeferredClearcut" value="[[2,null,357898634],null,[null],[null,"6283888",,null,null,null,"GB&q

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\drive.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.898536121970218
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFws7VWFIJVq5z7vXVEyLVV6u9xTBFqSRneZLKb:JFK1rUFdWFIJVq5PVEyLVz39lekb
MD5:	FD4413A6C9D6EAABF3C89AB2A4CA8E2A
SHA1:	13DC655C056A6C72AC83BB8C816FDB2C98E520D7
SHA-256:	309C364177699A4581A2928615A1B55B767C4A5A6E8A8FAF2E2E3BB5B5852901
SHA-512:	5DC4CC800C8FBCBB90C3DCBCA43956C480855FEBE27AAD3638E75DE135CA0631F4D52C9B27676067C5DA7657C9BB427F1C8EA95E39F215F6CE088C7A6BC8DBF
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="ui:previousBuild" value="drive.web-frontend_20210210.00_p1" ltime="3368715008" htime="30869902" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\about[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aKb:JFK1rFK1rFKb
MD5:	B9C5EB570521110110BB7DFF12AF780D
SHA1:	27F5BEBC2200FD8D0B51A93D1357EA954BE44079
SHA-256:	90171F10A6467C9DC31143859BAB69D045B67B39E2E49D92BB7168B383C4D1AB
SHA-512:	BC81539E62D643808CBDA3D86050058F379B2F0347CE65CBBA9797D386401C886B22AC4C0B2BE68197AE10C83A1E22A14232CD531C8D139DD3C031DB423EA3
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{036910D1-7582-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8476859765899847
Encrypted:	false
SSDEEP:	192:rmZKZE2bWEtuifKCozM0QBb2DdsfoCljX:riWTSQfHJ4wR
MD5:	3FA2FFBC91B23071E20C8DB7A3D94C08
SHA1:	6F210CE56E7716AACA97CA06915B671B1A867E30
SHA-256:	2D3B5AC7B19F3484586F54055162709DEA88623F6DA518E01CF6CF9DB3E979D2
SHA-512:	03BA0FB492F3D99D35EE36EE5347B1968EAECDA69C7E53E36ECDAD7BFFC02ED82363908EB33D0A02B3977F9DEEC84D6621A14C6D5EA136FAE8764687B9B742A
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r.y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{036910D3-7582-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{036910D3-7582-11EB-90EB-ECF4BBEA1588}.dat	
Size (bytes):	153768
Entropy (8bit):	3.055776892235786
Encrypted:	false
SSDEEP:	384:rKSIBXYIM3bFQMRMeSzjjOlMrOPNkVX9EW9kDOcUEcmG+dUn/0EI9MrdUVmZZmYa:ogdUDdU1
MD5:	D98FDD7584A4E40C6AEFF81417057E8E
SHA1:	6B5D44AEE03BF4D1C8038EF09A14D41718745BDD
SHA-256:	613A6279F00355C15DE7E8CDF30BF2CC2892276CA36150EF1307511B7C99D568
SHA-512:	9FF91ACF9264E0497D922FD23E2F3A4A42C62CD8E0FE8C6CB07DC1DAE40E656360E972CF6514D6FDD4B8E29B8D096CF829BA4B668565329B0688D986A21640(
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0BBE12AE-7582-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5638149832134056
Encrypted:	false
SSDEEP:	48:Iw/GcpruGwpaFG4pQFGrapbS2GQpKQG7HpRrTGIpG:rVZGQX61BSOArTBA
MD5:	B1F8666712FAFE7D40F62D121F4118E8
SHA1:	2ADABB0911017DE40E359CB003FCFEFAD988754D
SHA-256:	C0BA9B4B9497BEA6ABF458B37E7260B77C7E69E4F4BE0189F29375BB047D6F31
SHA-512:	F3FE6BFC536F667BFDB9D3CF6BA9FD4EC0B761672A6BF86F303AF1D0258A58193EF5A3B84E153A12DFA3A6BAF4C126D9FD9F3636445945E8B0C0106E97974AE C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	19959
Entropy (8bit):	4.611042323437257
Encrypted:	false
SSDEEP:	192:204LKaiUqNrTZwHiI6tSqWceBPGDvI6tBPqWceBPGbvI6tpPqWceBPGM:2dqZt456LW7Bb62W7BL6mW7BL
MD5:	33D3F106DCD5490C15A72A3AA7C9A91B
SHA1:	342F08AFDE7F40FCB97154B357AC011E6CD48B2A
SHA-256:	1632C9F409C1316B78D8C534B9B42047CB081368026F1BC4FE4F37209AED3BF3
SHA-512:	C4C3E88EA8C2888433852AB5FD9983650DE2C93716A5E19E0986A64D746D59C1FE09F6D02462FCC56CA4C5714BC9390EDC5BE4E80A21E1FCFC3555EC566946
Malicious:	false
Reputation:	low
Preview:	H.h.t.t.p.s.:././.s.s.l...g.s.t.a.t.i.c...c.o.m./.i.m.a.g.e.s./.b.r.a.n.d.i.n.g./.p.r.o.d.u.c.t./.1.x./.d.r.i.v.e._.2.0.2.0.q.4._.3.2.d.p...p.n.g.?....PNG.....IHDR... ... .szz.....IDATx.b ..... +.....m..dW.@..tm.Y.....m.....m.m..L.|.....{..b...t.....=H..qt..V..X..<jQc...p...fdU.\2.....9T...Jz!9...L.)&.....n....`~.T.\.\.$.....qQ.....LFOx.....^&,"bB..Lh9$_.6<...A...Q.T&y.,'... p...W`.2.?X(.o.4.J?.2...@.4...*..X..c.....[UZJ...MN.].z..f..DFe.J.....:!r...0X.....).....^*..!....u..c..R4.GH....Y....E....Q.....+!..)...e".....,.Ge.r.T..!..r..(.|.9f...}.....(...s..N...[..~.%6QF ..g..r.....CN.e"(..uY.h._1.H.e....r.k..%^S.c..<..0.s.j..,D.....].y.2(..OC.o\.3..".....cw...:;.btq.....w=.....R-[].4..]...?.....o..K../cC.<O...y..O.....{.-'Ln9..M.*6t.(.....o.K.$....bz.X. _d.....Z].U.....t....Bf.Zl.^vA._..g.{l....V...{....=.jua..[...k.....j....Y\...!..+.m..X..t(....".Mz.26l....7X.C...-...Z.lvl.....y}x.....7.m.VV....IEND.B`. m4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\046-GDU-MET-Blog-Chrome-Animation-JH[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1280 x 533
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	7.953352242657674
Encrypted:	false
SSDEEP:	3072:+5P5b+lC5Uu9JPY/eBg0tK6+NBcMjnaYTwZO:c+WjY/eBldacMDJ+O
MD5:	62C2B4EA759C65D2DE81EE323E6EF2A9
SHA1:	30A2271B8D01F128E6AF8A269A79E25C33481A74

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\046-GDU-MET-Blog-Chrome-Animation-JH[1].gif	
SHA-256:	E77521C94C97A6CA8A85EB32A816279B80B27A47D6217748F8DBE01673D7CD62
SHA-512:	1D2986DD99BD07809C1312E911B5BF2E3AC2B702D445C56198CD9F99FD09FD4975D8E926DBBF2423608FAAA66ABEEB37AFBF8440C3DB676BEFA56A7B9A18F317
Malicious:	false
Reputation:	low
Preview:	GIF89a.....0....o..j..r..s..j....!w.-.M1.P2.Q3}.4.S5.T8.V;..<..>.\A..B..C..E..E.aM.hS..U.oZ..].vb..e.}f..n..p..r..w..w.z..|..... .....th....pc.....{n....ug.xk....x.....SF.....|q..... .....B3.J<.....SF.[O.bV.....g\.si.....t.....{.....3..6..L..x.....,..b..... .!..NETSCAPE2.0.....!.....,.....o..j..r..s..j....!w.-.M1.P2.Q3}.4.S5.T8.V;..<..>.\A..B..C..E..E.aM.hS..U.oZ..].vb..e.}f..n..p..r..w..w.z..|.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\15977105_1416167725060465_6666549417477591233_n[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 200x190, frames 3
Category:	downloaded
Size (bytes):	16677
Entropy (8bit):	7.951141710512406
Encrypted:	false
SSDEEP:	384:D2H+11h+28xUgxzBesPueYkdvA8h4kWiev1bOvG/+e09voe:am10TPPb3ujjv1iu+e09ge
MD5:	2C428A49D996CC978DD96C49AEB837B3
SHA1:	96A693806E87FA81FFF02EC9576BE004F9493027
SHA-256:	90878117E3479BFD1C55AC23E401F79DD35BE28058C0835BA7F2196877564F75
SHA-512:	19B57743AE90AF2E046837276B635AA76B4ED62F98F2482FCBC86DE835F88D9B7EA0ABF9E52723CE59801D615F879FC5CC7BE0FF2919BBDC42FADBA15B02A8DE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/u/0/d/1Ih6fMHQOsSQLoDiDC0dHFlzOnpBc6Tru=w200-h190-p-k-nu-iv4
Preview:	.....JFIF.....O.....!1.A...."Qa#q.. .$2...3R...Bcrsu....%&46bt..CDd....5.....;.....!1..AQaq...."2.....3B...#Rb....$r.....?..}....:r..^..... ..<..L..jc..^....i..F....E..lF7...$`3..U..3. ..UuG.1. ...L3E.F.....(.....8.!x.SA.LR.i..V.2L.9.Dj...x...ij>kz....r.z.\.....t(.S....9rd^..o/1..?G..1..nU..Y.<.{v2".1..>]j...I=.....8.....Nx-..b..X.*.Z)`.e.@..%$Ua...<..[.e.,.&v.i.I....I%s$...Wv$..x...d7.`p.....-.....:.l.....2.K.L....3....>dP.....2.....8.du.....N.8..8..L.....c...a).....i..(.....e.).1rv.4.H.^E.z..<t.68...MOP.i9.jP.....&?..X.V...<u..g....|.as.u....(#.$.....$h.... ...wrx...)e..b..`.(...2.X.....hI.....M.....cX.....hp.2+..:.T.D%:.jm...._.....f.MiY,..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	298212
Entropy (8bit):	5.631643741452814
Encrypted:	false
SSDEEP:	3072:ez/9jW6NFQ4Kq6hMVGXIK8OsOY7Y0YbYSeY0mPCjwHabAHZRbJ26YgTB:cpWquqMd8Ohwls7eY0mPCjwHabG2mB
MD5:	5CBF583FF26E1660BB3516BA090A98C0
SHA1:	6D6D9B0C5B5E2EC2323F7D899DB23CD70D156E87
SHA-256:	24EEE722F4FF994C1E105242D8F59E7A1E572394BACBFB0635EBDE15DEC54F7A
SHA-512:	08FBE49EA0DC4E096450B5DD0076D634DF0094125687B6BA31E903F818E2A4475900EE1F5F4360B8F9FFB9967EF7765901BB4509C73B5D09538663BD9AE8C39B
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en" dir="ltr" class="a-Lk"><head><meta name="format-detection" content="telephone=no"><meta name="google" value="notranslate"> <meta name="viewport" content="width=1000, user-scalable=no"><title>- Flyer - . Google Drive</title><script>(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.'use strict';var f;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}var k=this||self;function m(){}function n(a){var b=typeof a;return"object"==b&&null!=a||"function"==b}function ca(a,b,c){return a.call.apply(a.bind,arguments)}.function da(a,b,c){if(!a)throw Error();if(2<arguments.length){var d=Array.prototype.slice.call(arguments,2);return function(){var e=Array.prototype.slice.call(arguments);Array.prototype.unshift.apply(e,d);return a.apply(b,e)}}return function(){return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26228, version 1.1
Category:	downloaded
Size (bytes):	26228
Entropy (8bit):	7.98323449413518
Encrypted:	false
SSDEEP:	768:DBOEuz6T0146JY/J6unqhOYK0GJenzOoyo6:DBHuea4j/vnqo304enzUo6
MD5:	6DD4AD69D53830BDF5232A13482BD50D
SHA1:	6FFF1079D7E5D02A2259CB5D7833E790239E01CF
SHA-256:	5CE48D9E9D748AD4686094D3CC33F5AE1E272A5B618F5C6D146C4D12EF02E4A6
SHA-512:	FC91E8C4EAE384D38667E330C5A5E4BF82EBAC9A23AB88439D7C22CCDD125DE7F1371DD953F18DEE60EF68B680DF49A32F684157D90F20E1DAC3BFFC9DF8418

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\4UaGrENHsxJlGDuGo1OIlL3Owpg[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v16/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff
Preview:	wOFF.....ft.....`.....GDEF.....\.....RGPOS.....#..+..P.LGSUB.....OS/2.....U...`h...cmap.....~n..cvt .....y.....fpgm...$.....uo..gasp.....glyf.... ..=...m..N..head..Z....6...6..'.hhea..[.... ...$.0.6hmtx..[<.....})9loca..]....z.....&..maxp..`p... ... .>..name..`.....r.i6Ppost..a<.....O...prep..e....p..... ..x.U....Q.F..=#.`ZD.@@<..... "...Zp....+.c.f...).>Z.bm.Om..?...\\.zi.f.^b...[y/.....x..Z.....%.....033333333...e....r.....U..u.r.....sV..Z..^..c..>v..p7.x...w.i...Y.....X...N<.k...0...kc];.u.....4.j...@....y."....,....#.;..... ....9...1....q..b..c...{....i2.H..g..:.....du.FX.].w3...{y...G....E.....~..RdX.|.\..U.^.x!....e.|.:.RX.Wxg.*...&.5....2n.Q...5.{..2....Ia.Vb%....:.Yn..QI.Z...x..Z.6..?.....G..W.*^#.e..#|l2p.S+.?'. <E..<....M.H..".>..d....>n%.(..."....<".....U/z.%..=...Le.cL3.4..4..znxgX!JD%.....s....&.a..z1._....O+..g.dm.?.9Vj.1...B...8..S..... ._.E.... .[#_..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\5XKU1F81.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	223037
Entropy (8bit):	5.518716586345064
Encrypted:	false
SSDEEP:	1536:rYxxxxmuARiYcDMR1PNClBKi4sFZg24EoiCMbxxAOshhTvsujvFKetYfd/nZnXmz:H3cBZbxxKhFsvwQ2/DuEOhQ
MD5:	E7D2C74A6159FD4FF5A7269801770406
SHA1:	D6958146E479A43035E36C9C44660FC0E5761648
SHA-256:	55312D8962DEBEC73F59130059AA1D7A9DBACD21B01A4A3EED5721923AD6AC36
SHA-512:	8B70917BBFCD566CDA0BF12794C9C100C3561CC9850DA28904E36615863EB429CCDCD58BECD75244369D44A1DC974EB16640FF997034382DF0F363E7FAAE00
Malicious:	false
Reputation:	low
Preview:	"use strict";_F_installCss(".KL4X6e{background:#eeeeee;bottom:0;left:0;opacity:0;position:absolute;right:0;top:0}.TuA45b{opacity:.8}sentinel{}");.this.default_OneGoogleWidgetUi=this.default_OneGoogleWidgetUi||{};(function(_){var window=this;.try{._.VB=function(a,b){return a==b?!0:a&&b?a.width==b.width&&a.height==b.height:!1};_.v("sy2d");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var XB;_.WB=function(a){_.zi.call(this);this.g=a||window;this.i=_.pi(this.g,"resize",this.s,!1,this);this.j=_.Vf(this.g)};_.H(_.WB,_.zi);_.YB=function(a){a=a||window;var b=_.za(a);return XB[b]=XB[b]||new _.WB(a)};XB={};_.WB.prototype.Ra=function(){_.WB.Ab.Ra.call(this);this.i&&(_.xi(this.i),this.i=null);this.j=this.g=null};_.WB.prototype.s=function(){var a=_.Vf(this.g);_.VB(a,this.j)||(this.j=a,this.dispatchEvent("resize"))};.._.z();.._.v("n73qwf");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ZB=function(a){_.zi.call(this);thi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\CheckConnection[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	29586
Entropy (8bit):	5.446342058383256
Encrypted:	false
SSDEEP:	384:+hZSsk+V3s6Aqgww5O73u0ZY+1XgTJfZwa64VDmAk+aUTYRHm8vcKKx:+XQyeLww5O7+MHgdfZwIVo+WHm8Ux
MD5:	816D96DBC23C9A432BFEFC99821C8D3C
SHA1:	A06CE7D4A040B23E459FFBE5E0EE0A306D999E77
SHA-256:	E9C57FF4DAF3C8E4A153A29CA85B254021DDA9531C6F4F21934E84B12A3EE934
SHA-512:	D9AE65F370648218E7AF3DDAF16A9424FDB1080D33C0B255B340F6E8A7209BC6EB57813D4285DF093492B124F5ECCB8ACB280003D49C0F10920D9ED24017EFB
Malicious:	false
Reputation:	low
Preview:	<html><head><script nonce="V2KAds5BLmSoruM3MwVBnQ">"use strict";this.default_AccountsDomaincookiesCheckconnectionJs=this.default_AccountsDomaincookiesCheckconnectionJs||{};(function(_){var window=this;.try{./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var k=function(a){if(Error.captureStackTrace)Error.captureStackTrace(this,k);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a))},aa=function(a,b){a:{for(var c=a.length,d="string"===typeof a?a.split(""):a,e=0;e<c;e++)if(e in d&&b.call(void 0,d[e],e,a)){b=e;break a}b=-1}return 0>b?null:"string"===typeof a?a.charAt(b):a[b]},ba=function(a,b){b=l(a,b);var c;(c=0<=b)&&Array.prototype.splice.call(a,b,1);return c},ca=function(a){n(a)},fa=function(){var a={};a.location=document.location.toString();.if(da())try{a["top.location"]=top.location.toString()}catch(c){a["top.location"]="[external]"}else a["top.location"]="[external]";for(var b in ea)try{a[b]=ea[b].call()}catch(c){a[b]="[error] "+c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Chrome_Owned_96x96[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6177
Entropy (8bit):	7.941892268309048
Encrypted:	false
SSDEEP:	96:iYr3dN0F+QXKWXPTdNVeVTGTe+24Usw2i2DDF2ryznZE4OYF3ETHKI2HAr9UXPDf:iY8FXrf5N2TuB2Rvc2ryzZhtG7drgb
MD5:	C101133ECB2D66F0EA98131267D2A10A
SHA1:	8C038B9B39FA23E0AD2226F0016BF51FA0B86E37
SHA-256:	E3654539251DF82D59096E81C875D1244FFB7AB92DBF3CE26F63F675121D8918
SHA-512:	751E9BFD75D1685A490972FE0D40FDBCDA97607F6A500D051B400B002ED8C1D7CF9DAB019388B74796C9AFEAED4E317AC6B40A7E936D234536AEB0CB6C0D8434
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Chrome_Owned_96x96[1].png	
IE Cache URL:	http://https://www.google.com/images/hpp/Chrome_Owned_96x96.png
Preview:	.PNG.....IHDR...`...`.....w8....IDATx..]y....}..-.z.....P#" (.q...*.K.K..`.'9N.q.sb....1F.1..".D..3.!.5...EQ.....M.....?...o...5...y...W..}....8<.....8<.^.._/l....Q.....5[.C3@f.a{.....B.P...b.. .....S0o...Qg...].b.N....(1.6.....I(.D@.....L..q.q2...8I.6.mP(.V*F.^..$.....W.....%..|...@.h...6E.-I@>...%.H.I.w.8.H4y..=....K..qX_....J.....`.~..*..m.6.:y...;.'..j.6_....~....MV2.".os. [.J....P .D..B.;C...7.....,....9...Vb.E.)"....A...m...{.}"...+....mW_....=.G...1.....H..4....z..I...#.=rgR.O[.(.....<.....@..".ig..&wv.?0..q.....W..M.pi.....zj...oA<z.GWm.5V....."\ .*9':4.....}.....=.....mPo.q.....p.....R.....v.BQ?.....a..w;~....t.!$`.E!3..QJ....("....y_.! ...A.....CN...#.#.OJ4v..H..P..Q..a! e....q..\<..mH>`...CM.*..8.YC.H.2.....`....k5.~.n..!!`.....I..X. <1.&A.....R6....a.@.#..~@.`I.&..^t.....3./..K.....W.DM...k.E...~.9w.T.^..c_..\)..\.....z..R.....#.@...o_z.....9.g:...A.....5S...-.u..(.1.(....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Chrome_Themes_By_Black_Artists.max-600x600[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 600 x 250, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	49767
Entropy (8bit):	7.987600229289206
Encrypted:	false
SSDEEP:	1536:i57n/egmzuGKB/Wqk2tFAEz+lQwxWAB6c/1MBM:i58zujQq/inWAQc
MD5:	AC63831B3DAEA159557D98E6CAA110AE
SHA1:	776515163FF0AEB03EEB92AE9B6309775C2477B0
SHA-256:	54A3D91BD3C404528EB67F34C7BFCAE08ABC3A9498300D9EF3B560EC2120C656
SHA-512:	F1BF4730722645E40A2BCFACCDD476F96115521E56CD3BE4311979740AB01AA70B06A7AF5A734EC9A92B6BB63ECF9CD15A41D06CD6CD8FCAA1BB43ABEFF01 153
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...X.....}-9.....IDATx..w.eW]..k..N.uzI&3!.$..-."Ez.QT.....}..Q.El.....B.....:.$So...]Vy.X..{'.0.D.dv>..3...{.g=.....79..9.....5.I..s`-.....H$X..8..%s>.\.@..?w..P. ..z/{....n..}.(.@. ..i.....B1...G\.K..}p.0...^...)...^.{....`3....}x&.if...o.....Y..!w....q.....?{?..q.6....B...d.`K0..J@H**.P.L.....c[X...(.:.<%.#j.:.A...y... ....r...2..m.0Vk..Y.G....[H.^..tc.,.X. 0..1A..e..F.....*.O....y..x...t..P...*.....a,....&...,.....I.....=....}.9.T@.P...t.}..m..E...Y.....C.A..kH3.....-.SN.A..@.;.t.....K+.3.Z.RT*U....>.".3:..:...{c.h8.../.(...c.=.k. LH..uc.!.. ....g..>G...eXYn.....H^...*8....\m..{_`../.../..v8K.O..&`p8.s8g..\>..{..:*p.a.-...Z..Rh...f.6...x.y.M...=.o....O._..*.H*t.F!..".qe.._.a...Y...4....1...I...?.....LLMc.>n.D.g..u...../....YDw....2 ....)X.h...d.....Z.~.....V.z..B,..u6.)...O.H...=\..x.....^..G..d...e..Y.AU.A.Mq....@.....+..Y....:.D4....pX{.%"D.....%....G=.:G.bZUID....A^0.9S.J..+...J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\GettyImages-157584725.max-600x600[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 600x400, frames 3
Category:	downloaded
Size (bytes):	28316
Entropy (8bit):	7.9690435720023896
Encrypted:	false
SSDEEP:	768:nH2NJDVK6lzlqJUMMyInh1zC3hdNk7eLOSOyi4ddDr5GJmue:nH2NJ9lz4JqnzC3XNOezOyrDWW
MD5:	C407381A64FE5C2869416876C36BBE88
SHA1:	100E1BA9C208411BD9C23175CF16CD8C3AE0B695
SHA-256:	A10D13EB051078CBBC5EAF4CFE1432B49A0D399010E34B6ECA78BBE44F876889
SHA-512:	8C9BC249F7A4931B7FB9F3FF88C17396903CF7024674B70E1EA90036B3D96E0316FBCBF1A164A0707469FC8B4E427D30FBEBC23C1D5EAE7ABC7C25AB39666EE 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://storage.googleapis.com/gweb-uniblog-publish-prod/images/GettyImages-157584725.max-600x600.jpg
Preview:	......JFIF.....C.....!.....".$".$.....C.....X.."..... Ol.?..X....k...k5....e...N...$+.....9Z8.;Y.0...aF..tP.L..A&Y.....S.....].fx...q.....W..\l.q...y.<2...N.3....9ZT+...0B.yMf...A.m.>....1.....i.8*!.j.:Z.._M..:*..TEy....L..0g`T,..l.... ._.z.zM2.#O.yW!..BYb....B.....h.....hT:.7.gx....5.3.9=nub.]....9.....X..|.@r.UsJ. .:Gc..\...`g'.....jcI...+.4.....x.,..P.Eb.*...P.b...*.T5.....}r...l.k.3..t]...3....k.<v.}...6.>.(O..NX.OM..! ...0..2..;.w9&..'...p.2...._a...,e..#eqXQ..79I-x3..-{.i..W...!.Z.i..y.7].ili..623...5X.j../c....Q....)...3....m....6M~..=..WOQe.\XuY...[P.v.....vM...T...g....i>Ds.a.(D.....3I9.JF$e.#.... 2...W)K.....p}s....Xv.m...+..=.U.z..A...=...T.r..@....IG*.T.5+WgS...%y...#.....m..b.;..6.M...;<..6k..aR.m..#..n..Z.'$..-k#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOkCnqEu92Fr1Mu52xM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 91728, version 1.1
Category:	downloaded
Size (bytes):	91728
Entropy (8bit):	**7.992950761576241**
Encrypted:	**true**
SSDEEP:	1536:ExcBHw4cGFSC/jzB/xuY5Qguzbr7jXSs5hUGWz/zR9QnmZAcMGnVqfi4WMKrF:ExcB1cSjruY+guf+s5+GWz/zDQmZZjk4
MD5:	F5902D5EF961717ED263902FC429E6AE
SHA1:	A51B4110C32440D54C5F299B8DDA8E3B38B8ACAA
SHA-256:	E1B2181CA3A817D49D830FCE920478488170E6921FCE6126D71E2EB2E7031805
SHA-512:	EDE7C2F731B270A187171B43E9C8E21A1A411F09F8127213DC6552B516BB194BBDE39A64CB3874E1936B845561F23D1331069D4A50EBB1D8DD18307C7898521A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1Mu52xM.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOkCnqEu92Fr1Mu52xM[1].woff	
Preview:	wOFF.....fP.....l.....GDEF.....s...b.B..GPOS.....,d..]....GSUB../l...|.....YOS/2..:....Q...`...Rcmap..;<...M...F.wX.cvt ..D....R...R..-.fpgm..D....4....s...gasp..F..... ...glyf..F .....$.Ihdmx..L.....:[Lahead..Nt...6...6...ehhea..N....#...$....hmtx..N.....83d..loca..YT.....|..Qmaxp..c.... ... .>..name..c4.....G..Kpost..eD..... .a.dprep..e\.. .....D..].x.....XK...{w.Y.m...6..Qm...6.m.Lrb....%l.9..J.T^V5...d.&k,Y..L.T..9Z...Z.5..@.Vm.]d.!k.Y..:F.....:....+x...d..}|.....?.'..1..bFg.....#...bq..2...\.k.&.q=l.F..-...cgw..=..{./.w....[... {.|.wd?..|.....A..C.....S.....!%...1g.yB....a.P.;..8$...q.....4n..q....J....]....._%..dd2..$cq|2.'%Sqfr..&..e..?%...~..7..._%.....ZI.h.V.....`-.....o..i..x....nD..E....AX...am.a..^G.e.6 .P....DR.ivnq)....v4M..mh.k.;.`.....J]w_7.m.....T.`.8"..R.5fx.....\q...<.B...z|.....$.`B.%.p".$.hb.%.x.H$.dRH..&.`.i.X`.u6.d.mv.e.}.8.cN8.s...kn..{.x.g^x.w>$L.$F.$A.$C.$G..H.. R.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmSU5vAA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 85692, version 1.1
Category:	downloaded
Size (bytes):	85692
Entropy (8bit):	**7.99326757388753**
Encrypted:	**true**
SSDEEP:	1536:aGVcBHw44GFWe1vgl3VNkhJk51/BjpLm++q6Szs/PIGc8znTVu:aGVcB145e1vglMhG1J1LpAyiP/znRu
MD5:	C73EB1CEBA3321A80A0AFF13AD373CB4
SHA1:	3EA2C95E21CC88D82BB111C99883484C64D657DB
SHA-256:	18827349C7FEBD4B8D01AA907C67EA9B8011242078326B24703978454FDF351A
SHA-512:	E11A2C6C7A2DCB2B08F66E1D92D9AE0EEA44ABC117666FE49382D55F5C4499C71CA9994DBD67227F2516EADBFC371C9A56E05EC530FE9C5BAF900E2D84AE02C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmSU5vAA.woff
Preview:	wOFF.....N.....GDEF.....s...b.B..GPOS.....,d..].....GSUB../l...|.....YOS/2..:....R...`....cmap..;<...M...F.wX.cvt ..D....X...X/...fpgm..D....4.....".gasp..F..... ...glyf..F$...3...V....hdmx..5X.....G`Rphead..6....6...6.Y.ihhea..7(... ...$....hmtx..7H.....8U.?loca..A.....tmaxp..K.... ... .>.\name..K.....`gYaGpost..M..... .m.dprep..M. .....:z/.Wx.....XK...{w.Y.m...6..Qm...6.m.Lrb....%l.9..J.T^V5...d.&k,Y..L.T..9Z...Z.5..@.Vm.]d.!k.Y..:F.....:....+x...d..}|.....?.'..1..bFg.....#...bq..2...\.k.&.q=l.F..-...cgw..=..{./.w.... [...{.|.wd?..|.....A..C.....S.....!%...1g.yB....a.P.;..8$...q.....4n..q....J....]....._%..dd2..$cq|2.'%Sqfr..&..e..?%...~..7..._%.....ZI.h.V.....`-.....o..i..x....nD..E....AX...am.a..^G.e .6.P....DR.ivnq)....v4M..mh.k.;.`.....J]w_7.m.....T.`.8"..R.5fx.....\q...<.B...z|.....$.`B.%.p".$.hb.%.x.H$.dRH..&.`.i.X`.u6.d.mv.e.}.8.cN8.s...kn..{.x.g^x.w>$L.$F.$A.$C.$G..H ..R.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOlCnqEu92Fr1MmWUlfBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20356, version 1.1
Category:	downloaded
Size (bytes):	20356
Entropy (8bit):	7.972919215442608
Encrypted:	false
SSDEEP:	384:of+dt1ebKR28EPpAXxR5wthZZv4B8Te/h4+ctr5NH9NwZaUp4VsEgm:of+P1eeRcU8Hqdy+UHHbEw/
MD5:	ADCDE98F1D584DE52060AD7B16373DA3
SHA1:	0A9B76D81989A7A45336EBD7B48ED25803F344B9
SHA-256:	806EA46C426AF8FC24E5CF42A210228739696933D36299EB28AEE64F69FC71F1
SHA-512:	7B1D6CC0D841A9E5EFEC540387BC5F9B47E07A21FDC3DC4CE029BB0E3C74664BBC9F1BCCFD8FB575B595C2CC1FD16925C533E062C4C82EEE0C310FFD2B4C927
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmWUlfBBc-.woff
Preview:	wOFF.....O.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....Q...`u...cmap...\.....W.cvt ...T...H...H+~..fpgm.....3...._...gasp..... ....glyf.....;...k....hdmx..H....m....!$..head..H....6...6...\hhea..I,.....$.&..hmtx..IL...y.....XF.loca..K.....`.C.maxp..M.... ... .(..name..M.....~..9.post..N..... .m.dprep..N.....)* v60x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x....dK...{....?..F?.|.~.m...ms.{.Z..;.....U.]7s.....\.=D.=.7...>....x...D..O|.U:...|o..3.x.j.r"B..... .1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H|#z_.O.....R..A...9..A..!.(./...".:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%..... j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#/..B.....N+p.m`...].IQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOmCnqEu92Fr1Mu4mxM[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20268, version 1.1
Category:	downloaded
Size (bytes):	20268
Entropy (8bit):	7.970212610239314
Encrypted:	false
SSDEEP:	384:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0clWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\KFOmCnqEu92Fr1Mu4mxM[1].woff	
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff
Preview:	wOFF.....O,.....P.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t...cmap...$.....W.cvt .....T...T+...fpgm...p...5....w.`.gasp.....glyf.....;Q..lD..&0hdmx..H....n..... ..head..Hx...6...6.j.zhhea..H.....$....hmtx..H....t.....Xdloca..KD.....BC%.maxp..M0... ... .(..name..MP.....t.U9.post..N ..... .m.dprep..N4.....I.f..x...1..P.....PB..U.=I.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R...A.J.x.l..h.a.....l.m.6.1+.X....i...y....&...._..63..5....2>...x|D...ct.Kx..H@b.3..l..#u.....L.*.....^.*.4.....rP..{.*.....Q...JT.:Xu>..T./>...oq.....~..@.....lq../.... ..#..".&.8.H$..r...J)..jj...&..f.=.9..N9....'F..8.4.....m...m...m.m..n..&.X..}....S.|.....n.....PHaE...J*...4..MjJ.*..nW)..rn3'/.....ks5zY5c...Mgg.5..p..rR{c...p..t\.8.c=..p...X.(.....7....=.....!...H .....(.0...(.q.JT?.b..z].'T...m..vNi.....t....:P.R..H....t.....&?.:.j.51+.S."j.SK'I.^....}S.i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Read me Flyer.pdf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 190, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	30146
Entropy (8bit):	7.927640583322369
Encrypted:	false
SSDEEP:	768:tsqBKFGBEJOsGO/yfmW6onDQqWubZTL2kXISrhPcfgXuxEUMi:LLE4sAZ6SdtbN/7xcoXuxh
MD5:	21E167E6BE766951B214AFE723904D4B
SHA1:	B874A30EDF11F269197B126B76D7D9CEA8710CE5
SHA-256:	8A6446ABB78C0E5094E30706A763AAC45A0E7AB1B98813FAD86E8882341CF7BF
SHA-512:	C7E95AA3077DC731CF4F3F8F07343D662F5C32B7712FA81F9ADBE14909AF471CA24D410C2E8BA406D74542CC4B0EFE58AC1A03B0B8DC044EF071B2112FCDEDB1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/u/0/d/1GLyzOFq_eeELxV_D7nsgdOSJJVo7fvGt=w200-h190-p-k-nu-iv3
Preview:	.PNG.....IHDR.....A.....sBIT.....O... .IDATx..Wp..>.s....rN.....$..eY.V.e.k{..z.....\..U....*.I.lY..U...3.....D.q.L...L.'.....%).B.....t..s.....;8....`...Kw...o...../80.....:...../80.....H...gvv.s..r.....hthh.5.L.i..K.lv...P(.....@<..Mg..._...{.h__..Ng.X>..n....X.D"...d2999..rgff"....r2.....x..?..hd2yhh..p..A.^.....H..r6..`0.r9....j...#....X,^YY.X,.....5...d.j.Z,..E.<x..D...V..d2.....ayy..`....B!.P. .s.h4..hT*...fcccqq1.....`0t:...F.|>_..ONN.....1.E...D..j.j.x<~aa..b.....m...'.H...J..H$....T*.l6...NLL.R..>....].R....9.N'.J....x.^.....`P.....D.Z.P(b....L2.4...pX..j.....u.L6;;..x.^o$...k4...l0....?..C.....`0.t.^....XD".EQ...?yaa!..]]].P..O?U(....|>.d2.r98D..H...:.....N..~.6.u:....n.;.L...d29??.T*.....|....X.....#.... ...Z.R....!... ..sssZ..b.....i.....<>>..d.....".H.V3.....p8.b...Q.Tt:] .x<.L&...*.J...dr.\.....j0.....}....r.fffN.<..[o...@.~....dzz:..R.T.....f2.2.LOOO:.FQ....A...K$.#.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Screenshot (257)[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 190, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	49921
Entropy (8bit):	7.9776011012965125
Encrypted:	false
SSDEEP:	1536:GbdOh7rZMvgVmhGJb+lMUkbjY/Y5B7M05:GIhfZMY/+1kXjh5
MD5:	38BC7D555E2C6A34C8031249619D056C
SHA1:	72DA57BD50ADEB1D4D933EB6924680C85299D2BE
SHA-256:	DE257151A67F6FC9C6697F06C4C8D16AED271B8CF519A9E88D2EC7F703BA062B
SHA-512:	B8EDB97DE02FB892C8C2EA47945D63402A22BCF9886012908AAA4D5AC4093F4C831A74A0786CE8905ACB8A271E36F11712EE9CB1C4D033E424420759F6352AE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/u/0/d/1fiNW7t-TigsM4m1PoDuWPIlu4igvAu4x=w200-h190-p-k-nu-iv2
Preview:	.PNG.....IHDR.....A.....sBIT.....O... .IDATx..y.dGy'.}.q..=.....{..J.."....`..L.m..>....3g.g.....6.U..@hCB.*-%..}.=.n.|.....}'O..{....o...7..^U...2....^. b..3'^`.....e ....Gf..K.SJk.m..7.j..G..u(U.....GZ.....9'"..g.D.G$..Q.....s.M....iM.3m.g.U.T..!..Z.+....3..0./.]c.2.5.3.....uw....F?..2....7]w..]....Rey..<.B..X.....+.._^/,.//.....]..F...z....s,..z..<...B.E..cFG.....F...d.-..=./>.{...`jj.{.....tK.B..Z....^...'G.VJ..nOR..r.....}K.....3.#.C.vN.%...R_o._]/.C)e.....! . Dd./.....ceaZi..)^.WF.U..w..{...F...]..3.....R.R..x..r.....d.Z.....T*.....%..T*.....ZZYY]].....]\.....=?...d....A|...>.^p....?.....6.....W..?{j[....8<...n.*.....v9+.+Vg_a.....Nv.Cy..=.r...n....N....?..A.:{..;12...F^...R(.../....<..a..lqy...;.....z;_|.^.....==...?...3g.....;:2....V?.....w..M7...~..]].\..GG....&...{.vww.....$.L$.S..&....&.....2.drqa...[..@..I4....w./..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Screenshot (64)[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 190, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	45344
Entropy (8bit):	7.980855631317209
Encrypted:	false
SSDEEP:	768:3DnWgOta1aAPbwPBXI//ztnGDIgkWBagXV949Jl7cqTihszD0evc+ADwqhjAqyhA:TYaBPMPBuztGhkWP9494cqT82DLc+FqL
MD5:	310150A8220175395DFBB14AB19E17A8
SHA1:	CBDCB27997C5949462C1C3FE9B0AB52813616C44
SHA-256:	3B057B5F275CD5DE6A11A87EA34CB2ED338EC0589F46C2BAA0E37D4E0A730776
SHA-512:	11C58670E550F93E861D9244C0BBC09F4F5FD6FFE4E34FC28BA976C62544B8E1DE12A667A4199CF3F8227D99901AAF6E1B16A5DFE7A1F8CD98675B689AD4CC2E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/u/0/d/17zI3TkqwKMzXmck8YuW2yOMzAhXKxJ1e=w200-h190-p-k-nu-iv5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\Screenshot (64)[1].png	
Preview:	.PNG.....IHDR.....A.....sBIT.....O... .IDATx..[.%Gv....Y./...t.g.40.`....!9CR.e]).a.!.eEH.DX.9...E..z.O...`.7E8..h....DZ.....@...[Ue...!.j.s.. .....}...*.....y.../.....{..mK.D~\ ....Z43'....HPM)....x.Ps'IH..."..cT.....1...D..;E.d...../f.iUU?....~.->.....o...'n..6..?..O..O.....{.....~..S..tO.[o..V.1.>\Z.9...^.4.<..[gMn..NV.g..uT...7.GO."N.n..'o|p.....{w..E.!.y.....|. ;...xoo^.....n.O}..7>...K.o?.._.....o.g..W.....e..l..f...~...{..O.L.~..7?.....k3i.....wN7..?....g.;.K.....OO~.g....+.....5....&.zi.....W..;.....O.....oN..v..}...o....V../>u..... .}.....X...g.....?..s.....'_=..m..K.....<}.|ur.....+_...../\;.....nu....w.*|....e.-u.>....~...<?.xR.....L..?.....f?.>y.>.&...._/.?z....9.....U.U.....=....?..B..g...^..z...n.Y..q.i'.....d..*...^..6. .....x....A.....|y.`.M9.....SK`RORJ.....h....!.>.<.+..8..r.z.p.....$...QDH.h.....EP....N.W^.~....[.m0..#....."..0.....v-H.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\bscframe[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.906890595608518
Encrypted:	false
SSDEEP:	3:PouVn:hV
MD5:	FE364450E1391215F596D043488F989F
SHA1:	D1848AA7B5CFD853609DB178070771AD67D351E9
SHA-256:	C77E5168DFFDA66B8DC13F1425B4D3630A6656A3E5ACF707F4393277BA3C8B5E
SHA-512:	2B11CD287B8FAE7A046F160BEE092E22C6DB19D38B17888AED6F98F5C3E936A46766FB1E947ECC0CC5964548474B7866EB60A71587A04F1AF8F816DF8AFA221E
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\callout[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	31267
Entropy (8bit):	5.750637392742268
Encrypted:	false
SSDEEP:	768:xKX/d9SvRujiA03wX97QknoV4DivnKiCPY8CP2qcOQPFJ/N4a1KA:8FV03wXfnomDiUqcF1V1KA
MD5:	9735306357 46F6C72EF1F6EAE6532140
SHA1:	E49046CCED7339715DE9ACE6A684695DA8842709
SHA-256:	40E99C56BAA62A1BF8B85B98C630CB7FBDF706D74DD0A332FDEF5DE3F3AC5C34
SHA-512:	DA36EC50110C2A2754ADC9133CEBA91014D3CF0134383756878547F8745680D3C9D46790B04EBF3DB9FA968CBF757588D702231785D31061E60E95D3639AC233
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/callout?prid=19016401&pgid=19010599&puid=46b57e6661f85f&cce=1&origin=https%3A%2F%2Fdrive.google.com&cn=callout&pid=49&spid=49&hl=en-GB
Preview:	<!doctype html><html lang="en" dir="ltr"><head><base href="https://ogs.google.com/"><meta name="referrer" content="origin"><link rel="canonical" href="https://ogs.google.com/widget/callout"><link rel="preconnect" href="https://www.gstatic.com"><link rel="preconnect" href="https://ssl.gstatic.com"><link rel="preconnect" href="https://apis.google.com"><link rel="prefetch" href="https://apis.google.com/js/api.js"><script data-id="_gd" nonce="XSFiaei1E/JzTaC7YZ085A">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"-5431876383826487120","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1614048690519906,151685598,4111340601]\n","ZwjLXe":49,"cfb2h":"boq_onegooglehttpserver_20210216.01_p0","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333],"gGcLoe":false,"ikfjnc":["https://drive.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"OneGoogleWidge

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	51432
Entropy (8bit):	5.555402766212286
Encrypted:	false
SSDEEP:	1536:pYB9v4ye0RGPEil199MSjQT7Rx0WwXRF1OVxK4X:pK4ye0RkwXR+X
MD5:	380373FCD08CB642C251152059997DB6
SHA1:	12773E4A16BF1B1D37967CEF5FBA90666E93ABBB
SHA-256:	98C669FC51080B27E219227634C7054D28012A063D8E58FCDA823D3688A8A458
SHA-512:	8B2C0AEA25A3C5A50DBE4354307F9FFF03D13966F1557D59156347E06C443897DA2A764F806A95779D34F72BA387F079F9BFD0FCEE5C59B0503C5E547D93C571
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[1].js	
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ka,na,sa,ya,Aa,Ba,Ga;_.ha=function(a){return function(){return _.ba[a].apply(this,arguments)}};_.ba=[];ka=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};na="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.sa=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};ya=sa(this);Aa=function(a,b){if(b)a:{var c=ya;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&na(c,a,{configurable:!0,writable:!0,value:b})}};.Aa("Symbol",function(a){if(a)return a;va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cb=gapi[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	100884
Entropy (8bit):	5.524623565937768
Encrypted:	false
SSDEEP:	1536:pYB9v4ye0RGPEil199MSjQT7Rx0WCjfyQUEZPplJYoDpA1/HNpHWNXRRF1OVxK4c:pK4ye0RkCjiE3IJTpoHNpHkR+4roC
MD5:	9534D32DE45A6E13B5E87DC9FCBF2B14
SHA1:	D299559588546F555EFE81E77BE17A7C10F82CD1
SHA-256:	79F21D811C42ACBDED1B2A1B86D7E9BB45D58A1F477E6ACF86B5CEC33EFE46C6
SHA-512:	EA05BD5432EFDA0655A27AB00649E5B6902215AC042BF3CEF2E8D0107A4DA64803EEF58684B0558B5CC8509F3347BFE7757567A05AC6EDF0036AFBAF9988899
Malicious:	false
Reputation:	low
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ka,na,sa,ya,Aa,Ba,Ga;_.ha=function(a){return function(){return _.ba[a].apply(this,arguments)}};_.ba=[];ka=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};na="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.sa=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};ya=sa(this);Aa=function(a,b){if(b)a:{var c=ya;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&na(c,a,{configurable:!0,writable:!0,value:b})}};.Aa("Symbol",function(a){if(a)return a;va

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\client[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12508
Entropy (8bit):	5.46381824374459
Encrypted:	false
SSDEEP:	192:8iApwYKUa9uzv1cJJBA1pwgKCwm5Mi0+SczlLb:83pw9duQJO1pTwmR0+ScxLb
MD5:	0F79A731986EEDBC1633214065F2CA68
SHA1:	2788534B1DC63F77D382E0A7E8B6E313FBD60C90
SHA-256:	B3B5F711542C1CC43BF1531BA7E65F2C4FE5C9620EAF4E2F1345276E08C9FD0C
SHA-512:	66163035A397B8D563C8938446578E3F8256AA8B79298267477F1E484AE3493027C47F2045E0232304E6FC772C70AFFC0D199DA78F54DAED5FD33B2DF8286CC0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/client.js
Preview:	var gapi=window.gapi=window.gapi||{};gapi._bs=new Date().getTime();(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var g=this||self,h=function(a){return a};/*. gapi.loader.OBJECT_CREATE_TEST_OVERRIDE &&*/.var m=window,n=document,aa=m.location,ba=function(){},ca=/\[native code\]/,q=function(a,b,c){return a[b]=a[b]||c},da=function(a){a=a.sort();for(var b=[],c=void 0,d=0;d<a.length;d++){var e=a[d];e!=c&&b.push(e);c=e}return b},v=function(){var a;if((a=Object.create)&&ca.test(a))a=a(null);else{a={};for(var b in a)a[b]=void 0}return a},x=q(m,"gapi",{});var C;C=q(m,"___jsl",v());q(C,"I",0);q(C,"hel",10);var D=function(){var a=aa.href;if(C.dpo)var b=C.h;else{b=C.h;var c=/([#].*&|[#])jsh=([^&#]*)/g,d=/([?#].*&|[?#])jsh=([^&#]*)/g;if(a=a&&(c.exec(a)||d.exec(a)))try{b=decodeURIComponent(a[2])}catch(e){}}return b},fa=function(a){var b=q(C,"PQ",[]);C.PQ=[];var c=b.length;if(0===c)a();else for(var d=0,e=function(){++d===c&&a()},f=0;f<c;f++)b[f](e)},E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cookie_consent_bar.v3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	36039
Entropy (8bit):	5.389397218891307
Encrypted:	false
SSDEEP:	768:MWhUO1AWX9rU23ed9FjzHPcT2MELjO67VcUq:MW+CpS7HkiLjOCVXq
MD5:	5BD9866C2B127CAD638AB7926A712515
SHA1:	762CBE22E41F14D08B1B24267E05FA0C228292A3
SHA-256:	69E537364F29CADBC3DEC72590FB007D10BD79999DB55244705F6DF3260F9A33
SHA-512:	F4B07388340A68825E7D3729A17CA3C719656F9B6A4168DA6484AD7B4A50FD7464A1541677EB4146EDE0AD4BBA46F5DAF943671940410F9ACF06F71DCEA4D85
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/brandstudio/kato/cookie_choice_component/cookie_consent_bar.v3.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\cookie_consent_bar.v3[1].js	
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var h,aa="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a},ba=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object")};,ca=ba(this),k=function(a,b){if(b)a:{var c=ca;a=a.split(".");for(var d=0;d<.a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&aa(c,a,{configurable:!0,writable:!0,value:b})}},da=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};.k("Symbol",function(a){if(a)return a;var b=function(e,f){this.ta=e;aa(this,"description",{configurable:!0,writable:!0,value:f})};b.prototype.toString=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1535
Entropy (8bit):	5.216575502620903
Encrypted:	false
SSDEEP:	24:G9X3OYsRqPv3OYXRDD7OYs/UrR/iOYP7NxV/iOYNNxBl/iOYsNxDv/iOYXNxd/iI:IOLRqP/OgRrOLOMOS7N2OWNsOLNtCOg3
MD5:	C7C65789D4FA76EFA46B98F895DBA0D2
SHA1:	F2C778BD6C15C2317F15D1EC66A42F01DC3C9059
SHA-256:	AE554ABF96A20F868E21592CAC8C6BD3341242F08BCB015D48E9D96F9C46D659
SHA-512:	027A9705ED7AC98ED96D1DA3F0A6DC72F4F70CE8CDA5F3C8ECFD1B11ACDD75790299D0AB5534F909964ABA9E6168DB09A20749931F73FF57113E7393D78FDFD
Malicious:	false
Reputation:	low
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.@font-face {. font-family: 'Product Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/productsans/v12/pxiDypQkot1TnFhsFMOfGShVF9eI.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 100;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOkCnqEu92Fr1MmgVxIIzQ.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1974
Entropy (8bit):	5.275171274290024
Encrypted:	false
SSDEEP:	48:IOLRqP/OgRTOCR/iOLR/oiOgROOS7N2OWNsOLNtCOgNCOCNq:IOLeOgpOC4OLHOgQOS7N2OWNsOLNtCOS
MD5:	4DC93BAB9A1B95AD68BC5C8A5B9C7EBC
SHA1:	5F6AB65DC34B7A2AF2F2C754F1153FDD86041A4F
SHA-256:	646276D10D36650EC9070E32FB4CD103D53D35482C8835AC2DF6272BE8EC615D
SHA-512:	72B56ADA1007CDB39DCA2D4FF15F99806405517F2100CB1E211EDD47B02E148E5B26CFB5DE7561C6F385A45BC49494FD4146E678E8E8A3F5C586F3AEBC13B41
Malicious:	false
Reputation:	low
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UaGrENHsxJlGDuGo1OIlL3Owpg.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 700;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLV154tzCwA.woff) format('woff');.}.@font-face {. font-family: 'Google Sans Display';. font-style: normal;. font-weight: 400;. src: url(https://fonts.gstatic.com/s/googlesansdisplay/v14/ea8FacM9Wef3EJPWRrHjgE4B6CnlZxHVDv79pw.woff) format('woff');.}.@font-face {. font-family: 'Google Sans Display';. font-style: normal;. font-weight: 500;. src: url(https://fonts.gstatic.com/s/googl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\drive[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	82089
Entropy (8bit):	4.727483591792646
Encrypted:	false
SSDEEP:	768:chqGLx8Pqtla2tyturYBEebpP1lE4Xuj0XehidAU:chqG98Ct5OurGBhuiJ
MD5:	6DB8EA2EC9823529B92E022402703482
SHA1:	073F91C3A702D31BDC339D925DC516BBD91D8F06
SHA-256:	43C052228CBC5021FE6350AA609E8C0875E720D66934DF390D8EA29122DC83E3
SHA-512:	035184B336CEA083BD2D5458BBAF50DFE3A370A6A0337121F2AD5486F767D919458BA4511CA2D8F7C825389C42747ABF4701934284FDD77C504ABDC1687157F2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\drive[1].htm	
Preview:	<!DOCTYPE html>.<html lang="en-GB">. <head>. <meta content="IE=edge" http-equiv="X-UA-Compatible">. <meta charset="utf-8">. <meta content="initial-scale=1, minimum-scale=1, width=device-width" name="viewport">. <meta name="referrer" content="no-referrer">.. <meta content="Safely store and share your photos, videos, files and more in the cloud. Your first 15 GB of storage are free with a Google account." name="description">. <meta name="google-site-verification" content="cqXadt7fWeX89GynJ90zuOnE6nb7qwS8sRiUJukU0l4">.. <meta name="twitter:url" content="https://www.google.com/intl/en-GB/drive/">. <meta name="twitter:title" content="Cloud Storage for Work and Home . Google Drive">. <meta name="twitter:image" content="https://ssl.gstatic.com/images/branding/product/2x/hh_drive_96dp.png">. <meta name="twitter:description" content="Safely store and share your photos, videos, files and more in the cloud. Your first 15 GB of storage are free with a G

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\drive_2020q4_48dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	7.7498165067195846
Encrypted:	false
SSDEEP:	24:36OlERwTs/hDwgKTbafbACzdi7gV4MxrS+NxTqGdZ+v5MHMM:3YRwM/KTbafbACzc7U4iz+2ZqMH7
MD5:	6E8D3C2A8321B62700B5FC798487B406
SHA1:	EFCBD4AAEEAD0DF37D1BBACAAC8C8E4C0936E0E6
SHA-256:	CD0FFAC602FA720B3AB346AF26B327A4D4C7FC352F1FD634A27C06C25728D9D0
SHA-512:	6F6EB4D59DACB1A0B796CEE9A076503883A7DD76F4B0B7A2D125DFA40BB8AC28B1E68F174E1211B1680332A9515E4C235E5354648F838EB083303E5104843D6F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/images/branding/product/1x/drive_2020q4_48dp.png
Preview:	.PNG.....IHDR...0...0.....W.....EIDATx....\K...*.g.el'..e..Sl.m....".m...w;...\..`N.W|...&.8.e)....o.....+O2t.....oK.....K.T;..x.....2b\..ZB..^..0u.....W.2..D..s...L...(>.. y...zf..Y ...n..*..5..I....5./.....iC6...h...!..V.....,..7z..1...."_ze.o.l<...../..Y.dF.h...IN.QsH.....Q..D..,..I*/Y...$3@..".*.....[..-O?.....9Ad..e...SU.9...W5..l^_..r..H..Z...y...wl `...HvZ..5.....0...h.L..J.XE^....Mn.T.2b].!.\.[.....U....Q.zL..&t.S...e..<L-E.Sl..w.2.4k.....l.+..#.a2{1%.c\.!_.....$=.U.B..w.....ML....D..N.Y.....P...<.....J...+.....N?\S.....E#|..'..K....6.9...W`.....K.....YM...y.!...yDd..Vd...M.<7.....^.V.Ui.f#..<...p..a.....7x].Q#o..>1.....i...Zr.....Pc....&....}Y7.?-..?.B7.7..(....?.1*....V.../}._...ZB...>..Q..3...D31...].....u ..ZT..!..F.r.....E!.>.N...=...k.c.....\....,.@.N.8.pDk[.).. TV.p..R4..o.S4`P.....<....+0.....3..s.....#.gn.Q\....d^DH.0.|..gi.....T.p.^..b...`Y'"4....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\f[1].txt	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	49
Entropy (8bit):	4.472379875726697
Encrypted:	false
SSDEEP:	3:U9lAzEn8/se:Uh8//
MD5:	38F674DD88BFAF7B6C9AF58736A29B4E
SHA1:	759EECC4C3144A57916248F6684CB410F61CFE4D
SHA-256:	6AC3D9BB0BB61D51F786EA66AACE7C529A698984C9D72313147247DCBAC0A5BE
SHA-512:	69BE28C392DD0CC7EDE0CA534A98B15DF66DE80ED8EE0726D97D7BED4B555E113FB91E105C6C7D4D0767ECC873522DC22BD347DDB382555EAF7172C6143D9A9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://clients4.google.com/insights/consumersurveys/gk/prompt?site=l3i7sndninnbynr3jnttq6ux6i&lang=en-US&token=ChEIgMnNgQYQ4efvs_nX8MeSARIvAPgL7BADRt0a_NKaA0tayD8XN69MTymDfuQ_6VI03BdH2cxnm8zNlLpLPpHszfU&po=_callbacks____0klhexfs8
Preview:	/* API response */ _callbacks____0klhexfs8(null);

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\googleapis.proxy[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12544
Entropy (8bit):	5.464000498184137
Encrypted:	false
SSDEEP:	192:8iApwYKUa9uzv1cJJBA1pwgZCwm5Mi0+SczlLX:83pw9duQJO1pkwmR0+ScxLX
MD5:	63806386787C3D02E68B02460CDECB29
SHA1:	C093C27741353256A6F26EF3F321A566CE2B2AE1
SHA-256:	85C48B9F9DEA02626FC5068E7B505BF532EC04AB8DD641D7A5EC6C9A04D48995
SHA-512:	CA4822EF3BE6842E74C877D34AB8E5991CF343A11253D7D1A3C9C823EC9AB08977624A4BAAEC0FAB099C7F6C1F221AA5B6140CEA56BA8840572812FAF2FF227
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/googleapis.proxy.js?onload=startup

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\googleapis.proxy[1].js	
Preview:	var gapi=window.gapi=window.gapi||{};gapi._bs=new Date().getTime();(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var g=this||self,h=function(a){return a};/*. gapi.loader.OBJECT_CREATE_TEST_OVERRIDE &&*/.var m=window,n=document,aa=m.location,ba=function(){},ca=/\[native code\]/,q=function(a,b,c){return a[b]=a[b]||c},da=function(a){a=a.sort();for(var b=[],c=void 0,d=0;d<a.length;d++){var e=a[d];e!=c&&b.push(e);c=e}return b},v=function(){var a;if((a=Object.create)&&ca.test(a))a=a(null);else{a={};for(var b in a)a[b]=void 0}return a},x=q(m,"gapi",{});var C;C=q(m,"___jsl",v());q(C,"I",0);q(C,"hel",10);var D=function(){var a=aa.href;if(C.dpo)var b=C.h;else{b=C.h;var c=/([#].*&|[#])jsh=([^&#]*)/g,d=/([?#].*&|[?#])jsh=([^&#]*)/g;if(a=a&&(c.exec(a)||d.exec(a)))try{b=decodeURIComponent(a[2])}catch(e){}}return b},fa=function(a){var b=q(C,"PQ",[]);C.PQ=[];var c=b.length;if(0===c)a();else for(var d=0,e=function(){++d===c&&a()},f=0;f<c;f++)b[f](e)},E=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\googlelogo_color_120x44dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 240 x 88, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5087
Entropy (8bit):	7.942283110579468
Encrypted:	false
SSDEEP:	96:a86JBYSPgF0qi7stEOiUuaVQerOtB6FnZSfCBz78clWPR45POl:aJPLvqF+OiUua+eru6Fn4CRWPRF
MD5:	8D2B7F3D00F50B8AEBB7D1C002C64CA1
SHA1:	B3D5A78C18020868D322A0AC54C9D8E45A59A3B3
SHA-256:	29C50FA4422AC0A690AF5B0987DEE6A030A7EEAAFA9DDA8543CF022368F545AA
SHA-512:	997E17F65B314CF9C5E4C19ECFBBD94819A1BEAB3E5C709AAC8B342D9D7B378ABED766F375DD11E70430C1BE09B84D8862BA61556D2A2A7E18AE4B1030C6BE82
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_120x44dp.png
Preview:	.PNG.....IHDR.....X.....z.....IDATx..].tT.....*.K..k.J.....b'o&.h9.....V..(G=Z..%3I.#"..VZ.....Dq...(jeQP+...Hf..!1..;x../.....9..0.....Whhhhhhh.(+..(2!uJ8j^...*.b....{F.\..O.+*O~M.W.E....-..M...."...z.'444.E..m}"...1s^.....QT.2....T.W./k.+444r.P,y.I..E1...T9.b.4.y.1..D.....wA`...F7#n.d#j>..O..l.....S\..H.....g..H....;..j..$m.$;..%.z"o...Be..BCC.....<+g'/.Un;Zhhh...3b...uY.}ln."444.;...>...4.7.-.V...M..1.....d4..BJOS..vz>.(O..b...J.T..ih8.>....p49.$.Zw...i.....&.....D.....U.R.Lf/.!)#..O.....t.....&...*..".V-OZ.)...M...P..*~..y5$..yC.....M...f.a.....<..;.Z.....N2?.....9.Qa..F....l.PUz..$%.<...G0...F.....?.....UC...8R.t.....@M=G....'.....{.hr.D....q...&p....F.H_$]...M...yv..{u...&p.!R..X....44...H]...a'..M...../g.$.S..n..P..D$xi<..R...R../....`.9^..=Xo./.?kp.....Z...7....JKm..-5=...Z.+.k}.Zj}.....U.....|*/S2.G.l.....&.e.h..B.+.x](.;n...../.#.u..O.#.....x$0.axA..b.C$...J.E7.7..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\icon_AppleStore[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	22457
Entropy (8bit):	6.064787216239161
Encrypted:	false
SSDEEP:	384:6HwXsZfNIPZ/FAlxo3uicJdH/ANJ1OlzUiUs4RwipupN5m:gwX4ePfAro3uiuIolQiU4ltm
MD5:	F322D26163903C0200EB79A27E763269
SHA1:	582A45F60298C7E2CB68423BF91F50ED85DA39BF
SHA-256:	B8209A3AF9A1D3265BD8D98B5CCCE39C871D9E6C58152F963320AE233305B325
SHA-512:	C1952DC045548532A11556494810357C1F4456A31C36A55BBBA7E115DFC2B74473AD16DAB9DCA0726D77272C928CAD3AFCA557ED8924D37356810A6DF369EB8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kstatic.googleusercontent.com/files/540ac1df440f3a3708b6f31b7fa0c4fd7fd4471dc0614cab5482e110dee791fd6492b009e67d1bbc3467bd6ac63785f5120cb8070ab95de32830c63975290455
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="203px" height="60px" viewBox="0 0 203 60" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 63.1 (92452) - https://sketch.com -->. <title>Group 12</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01.jpg" transform="translate(-734.000000, -3295.000000)">. <g id="Group-67" transform="translate(-40.000000, 3022.000000)">. <g id="Group-16" transform="translate(421.000000, 111.000000)">. <g id="Group-82" transform="translate(122.000000, 162.000000)">. <g id="Group-12" transform="translate(231.000000, 0.000000)">. <rect id="Rectangle" fill="#000000" x="0" y="0" width="202.5" height="60" rx="4"></rect>. <image id="Bitmap" x="15.75" y="6

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\icon_Google AI Search_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2122
Entropy (8bit):	4.888168679210639
Encrypted:	false
SSDEEP:	48:cmQSitH4k5lJg9E3H4J4ezcde6qjM1glto+T2KDVxF:bCtH4/9EoJ4dqY+9z
MD5:	2EE15B66575D7A161A56AEA4C7C8E34D
SHA1:	5959919E875CDAF81FF0A1560F6B83F5EC3D4290
SHA-256:	344339EC3CE5FDCA6172AA31D3A797C896F7C2A53BAB787E8A218CA07019D209
SHA-512:	6B41C6BEA03591A0C7AE771E57B791456CA0F3FB604410CB0F1F6E3FA2A83BE6E7F37CF4DA6544A2B2F40F587189FD065B8D5A9373DDE1966F5CC34F1732D8C8
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\icon_Google AI Search_01[1].svg	
Reputation:	low
IE Cache URL:	http:// https://kstatic.googleusercontent.com/files/1215f100aed56568e58a202bef5caf51ebcc316ed033a7d042d6d6c1f90f56c39e5633d0fcb521d98e3d40022e901c535be27f73510 c7d95e0bf39c861bd46ff
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="70px" height="70px" viewBox="0 0 70 70" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http:// www.w3.org/1999/xlink">. Generator: Sketch 63.1 (92452) - https://sketch.com -->. <title>Group 10 Copy</title>. <desc>Created with Sketch.</desc>. <g id="P age-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01.jpg" transform="translate(-817.000000, -2466.000000)">. <g id="Group-66" transform="translate(-129.000000, 2312.000000)">. <g id="Group-13" transform="translate(946.000000, 154.000000)">. <g id="Group-10-Copy">. <circle id="Oval" fill="#F8F9FA" cx="35" cy="35" r="35"></circle>. <g id="Group-3" transform="translate(18.000000, 18.000000)">. <path d="M25.0142939,22.0125786 L23.4333905,22.0125786 L22.8730703,21.4722699 C24.834191,19.190966

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\icon_GooglePlay[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	23991
Entropy (8bit):	6.06714323735864
Encrypted:	false
SSDEEP:	384:6HYXsZfNlmlxkk8605ssiF3NxcbU5jXDwQlyiHnirsulh58EL4b0fVS2JvjsqYmv:gYX4e6K5sHF3Lc6zflTHnnus44FlT
MD5:	F49C69113754614E0435AF4C82A63A97
SHA1:	4C67DEC71BDA5AC5957F87CCF9DB9DA8E05D2CCB
SHA-256:	3807DBF9C64812653A3CC6BAB536D026BE7FB05DA88C19AEFA045EBC949EE759
SHA-512:	71D99986323051F6FBE173D3AF2C33D99C595C1DEA1185FC4FB2F5D68BC9C7236277AC6F3C9AF81036073639807DBAA52F3C771B57410113BA8D96DE4650E5F/
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://kstatic.googleusercontent.com/files/6e1905e140550741a844d866fa3fd7c11f4a9d6cb84081b66fe973ee7c0afd03e548ccf9cdf7d671c9d3f301e593b53bc2050a06d900 daf13acb0b267d88e691

Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="203px" height="60px" viewBox="0 0 203 60" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http:
	//www.w3.org/1999/xlink">. Generator: Sketch 63.1 (92452) - https://sketch.com -->. <title>Group 12</title>. <desc>Created with Sketch.</desc>. <g id="Page-1"
	stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01.jpg" transform="translate(-503.000000, -3295.000000)">.
	<g id="Group-67" transform="translate(-40.000000, 3022.000000)">. <g id="Group-16" transform="translate(421.000000, 111.000000)">. <g
	id="Group-82" transform="translate(122.000000, 162.000000)">. <g id="Group-12">. <rect id="Rectangle" fill="#000000" x="0" y="0"
	width="202.5" height="60" rx="4"></rect>. <image id="Bitmap" x="11.25" y="6" width="180" height="48" xlink:href="data:i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\icon_Integration Tool_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1432
Entropy (8bit):	5.056671455338289
Encrypted:	false
SSDEEP:	24:2dmoDSWLtH+EyEOeFeaxM2l1bp8lYIEDY3TAuDc8Dq/N7E6Ae:cmQSitHtyk5YU3TAlf9z
MD5:	9DE213733119491C445CB7D44377C7DB
SHA1:	02A572EF721247474E282333E8BB5C8984059804
SHA-256:	3A85C120F1A73ED3F1E83693BD38959D5BDCF79F5A7E4C3028272CE5F000AF7B
SHA-512:	C353E967A26CF8E5845EB7E6CB406C03DD59E45A1524A0929F3379DBA5881E2C92DF0D3B7E71BB41E5CD7B2DD8511E71AF9ED2951F41A65F94BDCDA48FA443 18
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://kstatic.googleusercontent.com/files/eea6c181578777b6eeefd9042e51e9284c4443b3ea45c13e64a1f9c976af2faf69235f792329961d1495c5f49405d54c6344dd53f536 c8191b5a79f87ce5d382
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="70px" height="70px" viewBox="0 0 70 70" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http:// www.w3.org/1999/xlink">. Generator: Sketch 63.1 (92452) - https://sketch.com -->. <title>Group 2</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01.jpg" transform="translate(-128.000000, -1708.000000)">. <g id="Group-65" transform="translate(128.000000, 1704.000000)">. <g id="Group-17" transform="translate(0.000000, 4.000000)">. <g id="Group- 2">. <circle id="Oval-Copy" fill="#F8F9FA" cx="35" cy="35" r="35"></circle>. <path d="M42,16 L21.4285714,16 C19.5428571,16 18,17 .51875 18,19.375 L18,43 L21.4285714,43 L21.4285714,19.375 L42,19.375 L42,16 Z" id="Shape" fill="#3467BB" fill-rule="nonzero"></path>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	404565
Entropy (8bit):	5.047366786916183
Encrypted:	false
SSDEEP:	768:6TFkj1NKq90QopBzuWsy5tIP6CeuEDzXo3HARWQxQsQLZcMFGkj1NKq90QopBzu0:yyW1IP6CeuEDzXoXA8QxQsQzFPT8N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\index.min[1].css	
MD5:	6A06E9A49BB500D7BA32CF287A23B483
SHA1:	BE1BFFDC726D5F61C4402673A7440B5440584EB8
SHA-256:	DC46C846D67C9C118FFA8A8D65C91611048009A2516C79481DBF2E2B3C31B74D
SHA-512:	FADAE34127763E8B37802F83376613CC6D5AF3B185FEAA070A4E05BC70F0C31957EEB1703DF3DCBCE1ADED12D392B95D01C9C9004EF012976EBD446C21BF29F9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/drive/static/css/index.min.css?cache=be1bffd
Preview:	.glue-grey-0{color:#fff}.glue-bg-grey-0{background-color:#fff}.glue-grey-50{color:#f8f9fa}.glue-bg-grey-50{background-color:#f8f9fa}.glue-grey-100{color:#f1f3f4}.glue-bg-grey-100{background-color:#f1f3f4}.glue-grey-200{color:#e8eaed}.glue-bg-grey-200{background-color:#e8eaed}.glue-grey-300{color:#dadce0}.glue-bg-grey-300{background-color:#dadce0}.glue-grey-400{color:#bdc1c6}.glue-bg-grey-400{background-color:#bdc1c6}.glue-grey-500{color:#9aa0a6}.glue-bg-grey-500{background-color:#9aa0a6}.glue-grey-600{color:#80868b}.glue-bg-grey-600{background-color:#80868b}.glue-grey-700{color:#5f6368}.glue-bg-grey-700{background-color:#5f6368}.glue-grey-800{color:#3c4043}.glue-bg-grey-800{background-color:#3c4043}.glue-grey-900{color:#202124}.glue-bg-grey-900{background-color:#202124}.glue-blue-50{color:#e8f0fe}.glue-bg-blue-50{background-color:#e8f0fe}.glue-blue-100{color:#d2e3fc}.glue-bg-blue-100{background-color:#d2e3fc}.glue-blue-200{color:#aecbfa}.glue-bg-blue-200{background-color:#aecbfa}.glue-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\intersection-observer.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	5538
Entropy (8bit):	5.237839452540637
Encrypted:	false
SSDEEP:	96:+E8YzVFXsV2sZ2nkfI+W4yVdbaiGoNqQGLSaAZEeRmhw5j6YlRX96EmnWslvFrw:+ajsV2sZPHg2iLNxh2jhw5jhlRX96Evp
MD5:	4CF3CC46583A93DACA26479000688930
SHA1:	946521F218EC8976A0BB746F0ADC8B5914FC132B
SHA-256:	C887E228130A224F1C486F2563CB634753F083D12E56F9D0D186EDF6C384D000
SHA-512:	D35CD5B3E3829B381DEA8CC87EECFFD9B435632C47C37E3EA0ED280115582C45C7C9B38AFEDB4B19C49EEAF2C1FD44AFC615212FE6D5D5BA0D786D89CA36687
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/external_hosted/intersectionobserver_polyfill/intersection-observer.min.js
Preview:	/*.. Copyright 2016 Google Inc. All Rights Reserved... Licensed under the W3C SOFTWARE AND DOCUMENT NOTICE AND LICENSE... https://www.w3.org/Consortium/Legal/2015/copyright-software-and-document..*/.(function(f,h){function t(a){this.time=a.time;this.target=a.target;this.rootBounds=a.rootBounds;this.boundingClientRect=a.boundingClientRect;this.intersectionRect=a.intersectionRect||q();this.isIntersecting=!!a.intersectionRect;a=this.boundingClientRect;a=a.width*a.height;var b=this.intersectionRect;b=b.width*b.height;this.intersectionRatio=a?b/a:this.isIntersecting?1:0}function d(a,b){b=b||{};if("function"!=typeof a)throw Error("callback must be a function");if(b.root&&1!=b.root.nodeType)throw Error("root must be an Element");.this.g=y(this.g.bind(this),this.C);this.F=a;this.h=[];this.i=[];this.s=this.M(b.rootMargin);this.thresholds=this.K(b.threshold);this.root=b.root||null;this.rootMargin=this.s.map(function(c){return c.value+c.B}).join(" ")}function y(a,b){var c=null;return function(){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo_Salesforce (1)[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	18819
Entropy (8bit):	4.2571944714493775
Encrypted:	false
SSDEEP:	384:4H/O2NHSgYlScVUaZr/vhwxKONcOxNnskMle+cuSAyNwjR:y/OEyNSWd1/vuxKSRxQe+0haN
MD5:	831386DF0549D4452307A962FA782465
SHA1:	2FF55D009CBFC9052E16911677620198EF238545
SHA-256:	EC8FFB5C3C528BEA30DF8086343A740AD79D49080167FCC823BB0B3C01A3C9A8
SHA-512:	5463DD6A6AC6412081A1A39BC730579EA2D83F88D858F8FA7339CBB2A7E76E863312C45C88B3A9D26B55D7FAD20C81B002D94C2857F536D8A12E2DA2693B06D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kstatic.googleusercontent.com/files/56d87c8f379a15041193391b51180fbb5935b90f781e9fd4c986c708a7bba4feb63e4a2bedd40f59781db773aed145886961efa322e1132a0ffbd5cf89841399
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="129px" height="89px" viewBox="0 0 129 89" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 63.1 (92452) - https://sketch.com -->. <title>salesforca-seeklogo.com</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01.jpg" transform="translate(-655.000000, -3885.000000)" fill-rule="nonzero">. <g id="Group-69" transform="translate(0.000000, 3533.000000)">. <g id="salesforca-seeklogo.com" transform="translate(655.000000, 352.000000)">. <path d="M69.9752304,86.2160326 C78.4827796,86.2160326 85.9053125,81.5356357 89.8579999,74.5874917 C93.2929641,76.1017377 97.0951076,76.943992 101.095528,76.943992 C116.439959,76.943992 128.88,64.5637619 128.88,49.2926977 C128.88,34.0198224 116.439959,21.6395921 101.095528,21.639

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo_drive_2020q4_color_1x_web_64dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\logo_drive_2020q4_color_1x_web_64dp[1].png	
Size (bytes):	1521
Entropy (8bit):	7.806754140086895
Encrypted:	false
SSDEEP:	24:l0JD1Ga0+7qvEPCwx3IUVu7+f7Hz9mNinRBt5c0Q0UUxGq/nMxz8pJCWX6s59Xzj:4GbvEPCau7+f7H3Rb5dQ0UUMyy4cGF9f
MD5:	8ED6586A85FE477ABA437425280266AC
SHA1:	5EF1C567E0E7AE2C389FC20C3AE9C98A3BF2CA8C
SHA-256:	A0A4F406ACB9922E59B71E763754893819403D585404C1B0C9B917293FA99CB8
SHA-512:	E3A8396F795FCD1845FC9B912788733D36FE6133CF757FF53F3A8085FEF12018B0A1A54289BD481688A6D25EB81D8522E01DB7EA6784D99472BD500C8E66221D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/i/productlogos/drive_2020q4/v8/web-64dp/logo_drive_2020q4_color_1x_web_64dp.png
Preview:	.PNG.....IHDR...@...@.....iq.....IDATx....$[..o..>.^....{.....m.=\.v.....q_.$.l.Nc...?N.....:.&NYIN9.S...=...O}o..:.e...9p..>p..2.....6.F...0T.}c}2s.+/...Xn...c.8.6.....R..[.R.. .T.E.T..\.....1!..mE.^0.B_...$...../.....[.#U.w...}.....?m[#.~..#...7N.....u.'u..o...w.....U..x.?...`M.....X...@M.(.....u...UG..52."|.....\.@.;.b.C..L.....HKn.....%...b..C.....R.<Xe`.... [.B,.p.F..>.....pb.jO7...z.z....&..(G..{.....J..b^.`.R.`.}..:F.<...P....'.....pU...c....n.....r)...>f.....E>..G...^.0.....(t....'....B.[..z..5.(..Z.s6)..xv....O....!..,N...Q.....H.....C...N9b...0...&...~ .z{..J.+l...^<..q...Z.m...x.C....D.V.({.....R..!_|....;1".....(.H._....N....'.`...%..&N..m...!bA.....H..B.CNo...X.A,..d%5.].M9..e9./z5...V..o.9...E....k.a..#..45h.br..I....X.@.D..,.E<.?K .....>..D....nr.0...\T.....EJd...+R....&.$(Ux..V..M(..e1R.....C.E....A...^.W%a.ah....(lB..<DElz....A....,b...|....{.#....[o.l%y..|.=.....q1x..Y.""..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=Y6bHqe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	7092
Entropy (8bit):	5.452016888545132
Encrypted:	false
SSDEEP:	192:+tHqUJjcx27oeosQqy52x2keUv42ug2yZNkv5:AqUJjcQsZsRyIDlv4UgB
MD5:	D5B62A36677579F631CCC94D63B6666C
SHA1:	2D670AFFF5E9258A41BD7BB36D08CC0D9FD57D02
SHA-256:	E743F06C32871805B7E14CCF9E0B3B22FA608453841B366B9B87415EC59303F7
SHA-512:	242B2F84B6D4AAE0F49277C828B934EBEBCDD46953FB5A08E6A0D0AB3DE2697087321937BF4D3688E8255C8393A7DC4DB3F5AF3948D7294F79033742B2A045B
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://drive.google.com/_/drive_fe/_/js/k=drive_fe.main.en_GB.undZutTYHf8.O/am=9REAJjCYIVFXBSlRIBA/d=0/ct=zgms/rs=AFB8gsxopC90wdj6ywyUKpWT1_xTqXA7r A/m=Y6bHqe
Preview:	this._D=this._D||{};(function(_){var window=this;.try{.var qRe=function(a){var b=new Map,c=[],d={};a=_.m(a);for(var e=a.next();!e.done;d={Lna:d.Lna},e=a.next())e=e.value, d.Lna=e[0],c.push(e[1].then(function(f){return function(h){b.set(f.Lna,h)}}(d)));return Promise.all(c).then(function(){return b})},rRe=function(a){var b=new Map,c={};a=_. m(a.entries());for(var d=a.next();!d.done;c={FQ:c.FQ},d=a.next()){var e=_.m(d.value);d=e.next().value;e=e.next().value;c.FQ={status:0};b.set(d,c.FQ);e.then(function(f){re turn function(h){f.FQ.status=1;f.FQ.value=h}}(c),.function(f){return function(h){f.FQ.status=2;f.FQ.reason=h}}(c))}return b},sRe=function(a){for(var b=new Map,c=_.m(Objec t.keys(a)),d=c.next();!d.done;d=c.next())d=d.value,b.set(d,a[d]);return b},tRe=[1,2],uRe=function(a){_.Q(this,a,0,-1,tRe,null)};_.O(uRe,_.M);var vRe=function(a){var b=new uRe;return _.B(b,1,a||[])},wRe=function(a,b){return _.B(a,2,b||[])},xRe=function(a){_.Q(this,a,0,-1,null,null)};_.O(xRe,_.M);xRe.prototype.V=function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=byfTOb,lsjVmc,LEikZe[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	36657
Entropy (8bit):	5.460175864368039
Encrypted:	false
SSDEEP:	768:r9MK5wpS8exLOucjPBkFG9ZGUsMgQRGpYkPWFo8h4f2Lyo14Uc3PvKFscBU49Q:r9M4KPjpQYkP1/6yoKwJUl
MD5:	5CF040FFEDEF2B2F8804517797393E53
SHA1:	6234C9ED00B38B91ECE34944011CEC51FDC05BED
SHA-256:	66C95DF927E523EB0AD4B95BF710C29774A42B7FFEBCD2E3DCBC3B678D3F06F9
SHA-512:	B4226A8BD2918265E943C2257A1C3084584FDC8AEBDA2AAA51751C57B5D1FC9A913F600F3532D33DDE87884C0CE7BBDAAED7788DBFA2DA6E10DB1A09112AF C1
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_OneGoogleWidgetUi=this.default_OneGoogleWidgetUi||{};(function(_){var window=this;.try{._.Uu=function(a,b,c,d){a=d||a;b=b&&"*"!=b?Stri ng(b).toUpperCase():"";if(a.querySelectorAll&&a.querySelector&&(b||c))return a.querySelectorAll(b+(c?"."+c:""));if(c&&a.getElementsByClassName){a=a.getElementsB yClassName(c);if(b){d={};for(var e=0,f=0,g;g=a[f];f++)b==g.nodeName&&(d[e++]=g);d.length=e;return d}return a}a=a.getElementsByTagName(b||"*");if(c){d={};for(f=e =0;g=a[f];f++)b=g.className,"function"==typeof b.split&&_.oa(b.split(/\s+/),c)&&(d[e++]=g);d.length=e;return d}return a};._.Vu=function(a,b,c,d){var e=_.Ri(a,b,function(f) {_.Si(e);return c.call(d,f)},null)};_.Wu=function(){return _.Bj("lm6cmf").Sa()};_.v("syu");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache- 2.0.*/.var $u,bv,dv,kv,ev,gv,fv,jv,hv,lv;_.Xu=function(a,b){this.j=this.v=this.o="";this.U=null;this.u=this.i="";this.s=!1;var c;a instanceof _.Xu?(this.s=void 0!==b?b:a.s,_.Yu(thi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=customization[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=customization[1].js	
Size (bytes):	716
Entropy (8bit):	5.093194614063178
Encrypted:	false
SSDEEP:	12:MRyFIUCQ6aZ4ZB47PouMhue6y5e6DIOQ1wWxA1oWsZPkbykBBV16hLZOiLw0:+yiQfZ4ZSFMhue95etOQ1VA1QZPkdVMf
MD5:	6129D37FC3B47289BFBB41A9862194FA
SHA1:	603191C516BD985EC549891C27DA158600885594
SHA-256:	AEB021D99F3B41E2121831734BF60461381E102907F34D6DA5CA74B3CB3995F1
SHA-512:	11CFBDE1023689E315C745B32DCB120C272653F0C11B23C6CB8B4872D040FBB5B75211E55E0EFB53B0ED7B1E681D4ABC1EE1FCCB2704DD0047D61E099EB8A0F2
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://drive.google.com/_/drive_fe/_/js/k=drive_fe.main.en_GB.undZutTYHf8.O/am=9REAJjCYIVFXBSlRIBA/d=0/ct=zgms/rs=AFB8gsxopC90wdj6ywyUKpWT1_xTqXA7rA/m=customization
Preview:	this._D=this._D||{};(function(_){var window=this;.try{._.t("customization");._.GNe=function(){this.Ao=new _.Io(!1);this.bVa=new _.Io(!1);this.yX=new _.wt;this.Tta=new _.wt};_.g=_.GNe.prototype;_.g.ready=function(){return this.Ao};_.g.XHb=function(a){this.Ao.set(a)};_.g.$Hb=function(a){this.bVa.set(a)};_.g.bDa=function(){return!1};_.g.Kda=function(a){this.yX.push(a)};_.g.CFb=function(a){this.yX.remove(a)};_.g.Sta=function(a){this.Tta.push(a)};_.g.DFb=function(a){this.Tta.remove(a)};.var HNe=function(){_.P.call(this)};_.N(HNe,_.Mf);HNe.prototype.initialize=function(a){a.registerService(_.cy,new _.GNe)};_.Of(_.si(_.Oa(),"customization"),HNe);.._.w();..}catch(e){_._DumpException(e)}.})(this._D);.// Google Inc..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=sy1am,kodfyd,SHdile,sy195,sy196,sy19e,sy11n,sy19a,sy198,sy1db,sy1hl,sy1jt,sy1ac,sy1j3,sy1j5,sy1j6,sy1js,YYGnn[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	20125
Entropy (8bit):	5.547433372877971
Encrypted:	false
SSDEEP:	384:sVR3Mu47J0e2deTOLEF60gOKkoyI01LW+PXWBaHNdN:sVRMH7J0eKeChsIyZ1CBMNj
MD5:	B1CDBB854C886FC3528948AF12726C09
SHA1:	A6556475F9E29E798E0F475119C90F08A9C93BBD
SHA-256:	923DD570BD5B89D0852ED139EE10EDAA157CB24DB606FE133CCA92AB88734317
SHA-512:	F2FC029EA209EFE59DC33D8703CCA4B246A73376B1C7B7D913BCED34370185BD9BD91CB108D15AAE6F0AD1C32F6C987846F9ED1658E9AE0397DA12C74021ABCA
Malicious:	false
Reputation:	low
Preview:	this._D=this._D||{};(function(_){var window=this;.try{._.YWe=function(a){return a?!!a.Fc():!1};_.t("sy1am");.._.w();..}catch(e){_._DumpException(e)}.try{._.t("kodfyd");._.bhh=function(a){_.BD.call(this,a.hb);var b=this;this.Sb=new _.ke;this.H=!1;this.$d=a.Da.$d;this.nAa=a.Da.nAa;this.Db=a.Da.Db;this.Mb=a.Da.Mb;this.W=new _.Yzf(this.La());this.Oa(this.Sb);this.Sb.listen(this.Mb,"n",function(){b.Po&&b.H&&(b.Po.Ua(!1),_.aa(b.Po),b.Po=void 0);b.H=!0})};_.N(_.bhh,_.BD);_.bhh.Nb=_.BD.Nb;_.bhh.Ta=function(){return{Da:{$d:_.mn,Db:_.Pb,nAa:_.vd,Mb:_.pe}}};_.bhh.prototype.handleError=function(a){_.Ub(this.La(),a,135)};_.CD(_.N$a,_.bhh);...._.w();..}catch(e){_._DumpException(e)}.try{.var ehh=function(a){return a.Fc()?_.Jd(a):!0},fhh=function(a){return a?a.getId()===a.Fc():!1},ghh=function(a,b,c,d){var e=void 0===d?0:d;d=new _.hi;b.length<=e?d.callback([]):(_.ki(a.ii.Fn(b[e],c).addCallback(function(f){if(f.ri())return[];var h=ghh(a,b,"path_untrashed_find",e+1);h.addCallback(function(k){return _.xa(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=sy1h5,k2LvNc[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	5097
Entropy (8bit):	5.518553481909021
Encrypted:	false
SSDEEP:	96:+ydIDv7GFm4gc9GZlsak3lYFAQ3LXhlOeTl3g:+IIDj/v/zZiFAohlOeTl3g
MD5:	4C524C682287FFC54186C8612F33CC1A
SHA1:	93E1E0957E6D96B72DA1E5D3FC720F173114BBCF
SHA-256:	6A37F1C49D758D6F7B1626B559DBAC7351C59F64A19B0A7A05C39C8C2AB8555C
SHA-512:	372E0DAEC089F8D468876DB3222B71977932F268F2519E40CE397E15D963E5682C66FBDB095D03EEAA25989645533CE6F2F112EA7CD1171BC69FEEDBB78BE3BD
Malicious:	false
Reputation:	low
Preview:	this._D=this._D||{};(function(_){var window=this;.try{._.xSg=function(a,b){return 0<_.sTa.parse(_.Yd(a.Qh()),b)};_.ASg=function(a,b){if(a>b)return _.X7.SF;for(var c=0;c<ySg.length;c++){var d=_.X7[ySg[c]];if(d!==_.X7.wW&&d!==_.X7.SF){var e=_.zSg(d);if(e.H.equals(a)&&e.V.equals(b))return d}return _.X7.SF};_.zSg=function(a){var b=_.d$d(),c=0;switch(a){case _.X7.dra:b=_.c$d();break;case _.X7.Iqa:c=-6;break;case _.X7.Hqa:c=-29;break;case _.X7.Jqa:c=-89}c&&b.H.add(new _.Tv("d",c));a=b.V;a.add(new _.Tv("d",1));b.V.set(a);return b};_.t("sy1h5");.var ySg;_.X7={wW:"piqGWb",GLa:"bAa4l",dra:"OmBWEe",Iqa:"R2Qlub",Hqa:"JS9eTb",Jqa:"Rxg41b",SF:"C7uZwb"};ySg=Object.keys(_.X7);_.Y7={};_.Y7[_.X7.wW]="Any time";_.Y7[_.X7.GLa]="Today";_.Y7[_.X7.dra]="Yesterday";_.Y7[_.X7.Iqa]="Last 7 days";_.Y7[_.X7.Hqa]="Last 30 days";_.Y7[_.X7.Jqa]="Last 90 days";_.Y7[_.X7.SF]="Custom\u2026";.._.w();..}catch(e){_._DumpException(e)}.try{.var BSg=function(a){a=a.Vua;for(var b="",c=a.length,d=0;d<c;d++){var e=a[d];b+=2==e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=syxb,sy1gg,P6NtRc[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=syxb,sy1gg,P6NtRc[1].js	
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2081
Entropy (8bit):	5.246848847039735
Encrypted:	false
SSDEEP:	48:+yZIuAyxyktjedg21DUpcvGRt6QsnUTsql2:+yZPAyLjejWZOnuY
MD5:	A1C73E663E765B556B5029C4F667A1F8
SHA1:	03232D15ECBA819CB34497E2D66BA6BB51523D6F
SHA-256:	39E5A418EEDDA78D5CC8858696E83E9EF59E755DB1E6C369595132C36AF1E348
SHA-512:	98CEE64C9A58E2186D2AD5FC15FE3B52E84516A1291AFC7DC3235B032EADDE85F4E045D45BF8DF3E7C4C8910FB0C998E89A447343B33F83E20CF091E06FA16 2
Malicious:	false
Reputation:	low
Preview:	this._D=this._D||{};(function(_){var window=this;.try{._.t("syxb");.._.w();..}catch(e){_._DumpException(e)}.try{._.t("sy1gg");.var QJg=function(a,b,c,d){d=void 0===d?new _.Uo(!0):d;_.P.call(this);var e=this;this.Da=a;this.W=b;this.ha=c;this.V=null;this.Li=_.me.getService(a);var f=new _.Io(!0),h=a.get(_.Xq);h.aW().then(function(){e.V=h.cO(b);_.xo(f,e.V)}).then(null,_.Wb(a,481));this.enabled=new _.gy([d,new _.my(f)]);_.N(QJg,_.P);QJg.prototype.qK=function(){return this.W};QJg.prototype.isEnabled=function(){return this.enabled.get()};QJg.prototype.Lp=function(){return this.enabled};QJg.prototype.Fu=function(){return this.ha};._.K7=function(a,b,c,d){QJg.call(this,a,b,c);var e=this;this.ve=null;this.visible=!1;this.content="";this.direction=2;this.title="";this.H=a.get(_.Yq).get(d);this.H.listen(function(){RJg(e)},this);this.Lp().listen(function(){RJg(e)},this)};_.N(_.K7,QJg);_.K7.prototype.setTitle=function(a){this.title=a};_.K7.prototype.setContent=function(a){this.content=a};_.K7.protot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\m=syxf,BDbGue,WCIEHd,vCpxhb,dS9ppc,syr8,sy15s,account,uflob,wEobMe,vkwSxb,kmCYTd[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	14918
Entropy (8bit):	5.383732935102864
Encrypted:	false
SSDEEP:	384:NeNzptefLUSogOlrMiA6MfgUxz8kRlsSDK0gdhb:NePteITJMiAe8YkRlsSDK0ab
MD5:	678AFE6326E9F1D2CD2A07EAA0558C7A
SHA1:	D0405E1935ED377631C1CB0FA4D329B97C9CDD74
SHA-256:	7EAE6CBE41A17A8BDB1827A0059E5805CF9B0A9F3A6551B9EF24BD0BA2EB6686
SHA-512:	B0A281EF3EA54F6588F2234B4279D8B9AE8620A026A98874302A77B8E6522EE784C4516DFEDE19803438C15E28A7E12EE0AF925EF5B100B4BA84FCBB7564F9FD
Malicious:	false
Reputation:	low
Preview:	this._D=this._D||{};(function(_){var window=this;.try{._.t("syxf");.._.w();..}catch(e){_._DumpException(e)}.try{._.t("BDbGue");.var s9=function(a){var b=a.Da;_.BD.call(this,a.hb);this.config=b.config};_.N(s9,_.BD);s9.Nb=_.BD.Nb;s9.Ta=function(){return{Da:{config:_.Pl}}};s9.prototype.Dv=function(){var a=_.Rpa.Ib().setConfig(this.config);return Promise.resolve(a)};s9.prototype.Gn=function(){return null};s9.prototype.nextPage=function(){return Promise.resolve()};s9.prototype.yj=function(){};_.CD(_.Sua,s9);.._.w();..}catch(e){_._DumpException(e)}.try{._.t("WCIEHd");.var Yah=function(a){_.BD.call(this,a.hb);var b=a.Da;a=a.service;this.Wc=b.Wc;this.Wc.Zd().observe(this.P2a,this);this.Or=b.Or;this.Fp=a.NJ;b=new _.ke(this);this.Oa(b);b.listen(this.Or,"h",this.P2a)};_.N(Yah,_.BD);Yah.Nb=_.BD.Nb;Yah.Ta=function(){return{Da:{Wc:_.vd,Or:_.ao},service:{NJ:_.VF}}};_.g=Yah.prototype;_.g.Dv=function(){return _.$h(this.IJ())};_.g.P2a=function(){var a=this.IJ();_.mQb(this.Fp,a).then(null,_.Wb(this.La(),

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\main.min[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1240954
Entropy (8bit):	5.102345867480097
Encrypted:	false
SSDEEP:	12288:SbQRQ6kfXD2o/xRGQwnxbyKwAUikpUdiPk6mSWnnT4tWpJdVdDxYUq5N/KtF/SCm:SbQRQ6k1wnxbyKwAUik1k6+nTwxUCd
MD5:	98ACB4F02138899EB3E370A653C04325
SHA1:	D90622E68ED13CC76C397A10F6DEBBBB9AC05571
SHA-256:	46566A36BEC6B683C16034B1D27B48FD7460A2721F717139F4C560102B3A74E3
SHA-512:	C725624DFEBF7084D4D7AB3CEC443BAB7612B63FCD13696BE52FFF738F938C9D0AEF45E82B92C7F3291CD4F522F21E859AC78D1337EC7010B7F3F30E0BCC73 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://about.google/assets-products/css/main.min.css?cache=d90622e
Preview:	@charset "UTF-8";.h-google-red-50{color:#fbe9e7}.h-bg-google-red-50{background-color:#fbe9e7}.h-google-red-100{color:#f4c7c3}.h-bg-google-red-100{background-color:#f4c7c3}.h-google-red-200{color:#eda29b}.h-bg-google-red-200{background-color:#eda29b}.h-google-red-300{color:#e67c73}.h-bg-google-red-300{background-color:#e67c73}.h-google-red-400{color:#e06055}.h-bg-google-red-400{background-color:#e06055}.h-google-red-500{color:#db4437}.h-bg-google-red-500{background-color:#db4437}.h-google-red-600{color:#d23f31}.h-bg-google-red-600{background-color:#d23f31}.h-google-red-700{color:#c53929}.h-bg-google-red-700{background-color:#c53929}.h-google-red-800{color:#b93221}.h-bg-google-red-800{background-color:#b93221}.h-google-red-900{color:#a52714}.h-bg-google-red-900{background-color:#a52714}.h-pink-50{color:#fce4ec}.h-bg-pink-50{background-color:#fce4ec}.h-pink-100{color:#f8bbd0}.h-bg-pink-100{background-color:#f8bbd0}.h-pink-200{color:#f48fb1}.h-bg-pink-200{background-color:#f48fb1}.h-pink-3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\menu[1].png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\menu[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	200
Entropy (8bit):	5.949275070710723
Encrypted:	false
SSDEEP:	3:yionv//thPl5lGAg9RthwkBDsTBZtPdyk0lTpD8SvUWf+Gv1DA5s6t1Q/9J1lNmt:6v/lhP8FjnDspP/SvwsSpt1QXNm7Gop
MD5:	B89018A9ABAD5E652C6563A79B8AAE8B
SHA1:	38C6AED7B680343CE4CB5219AA4477E626247765
SHA-256:	99CF21268D1BF62829F18FAD71CF7D17C8EAACC5B89889B98B11CD2950F3711C
SHA-512:	E7ACFDFCF277DEE6BFAB177CEB4C52B49D607DC553C72E324BD52420E9C29AF4C1FBFD94E1627F6412A80C0A5CE23F0CAE006D35662D958860D36D9F4457B BF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://about.google/assets-products/img/menu.png?cache=38c6aed
Preview:	.PNG.....IHDR...0...0.....W.....tEXtSoftware.Adobe ImageReadyq.e<...jIDATx..... ..@..t*H.....c$.{.cl.....9..2s.KRU...xs..._...`.)....M.....&..F.k..F.....c.%.....e..nn....I END.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\operatorParams[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1317
Entropy (8bit):	4.852778081210115
Encrypted:	false
SSDEEP:	24:D76bBSCr2FvVdG4xp9kLk/rgk4oV4SRv/4QBEwrlcKmlQFHMhfY0ypgkvVlXdR/Z:H8vKNA4xpKLw8Pe4A34EE6cfAsG42hfZ
MD5:	C0CCDCF863ED9C144E29F1CF9BE8ABC8
SHA1:	5D1C2A1F4B29AD71A5AC7CF4B24DA2398B44680B
SHA-256:	E50D4D5D041A225BD7DAC643604C3E9B438BCEB3AF0F41DA5E4516C73D9FA05C
SHA-512:	86B731653B2C0046110BF34357F21A57BF4CABCC4C54700ED18EE7218F3A41DD52B87515FF2BBECB2D2756E08E8679634715DB35A7388A81612A62A8F848D770
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/support/realtime/operatorParams
Preview:	{. "operatorDeferredUrl": "https://ssl.gstatic.com/support/realtime/operator/1613552499959/operatordeferred_bin_base.js",. "eagerLoadHostnamePattern": "((https://www\\. google\\.com/express)|((adwords|campaignmanager|support|support-content-staging.sandbox|business|fi|.+\\.corp)\\.google\\.))",. "eagerLoadHostnameFlags": "i",. "cbfVersion": 1613552499959,. "experiments": {. "attachment_upload_url": "https://support.google.com/chat-upload/support-cases/resumable",. "enable_cha t_attachment": true,. "enable_desktop_screenshare_email_fallback": false,. "enable_emojis": true,. "enable_youtube_specific_endpoints": true,. "mole_show_surv ey_url_percentage": 100,. "mole_skin_version": 2,. "operatordeferred_report_rpc_events_percentage": 10,. "screenshare_skin_version": 3. },. "settings": {. "attachment_upload_url": "https://support.google.com/chat-upload/support-cases/resumable",. "enable_chat_attachment": true,. "enable_customer_can_end_chat": tr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\pixi.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	436708
Entropy (8bit):	5.388297977345394
Encrypted:	false
SSDEEP:	6144:7A3O570aEMxkhLqO/Q8628egXjBcNARqj+qL8+OklpOvpZWUiRUf7Uq3lvEiPjjC:k3O5rE3KegXpRcOklpOvGNqRS
MD5:	963D9AA530A76C5A0ABAA0D904DF6F42
SHA1:	A4AE3EFD4E53FC1EA04C888132690A78867F2062
SHA-256:	EEECF50C486DC0C755EBDC35126D9B9AB73E46CE5AA412666B70335D6C6E5A41
SHA-512:	B1CB49A18BEE434FAA7A7A8DA10E6BF39D14829FECFC98E596628F0BAFBC3F374CAA59227081BEF5A8AC058ECB3F4353C523BE0358C25242A2700E720EE988 23
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/external_hosted/pixi/pixi.min.js
Preview:	/**. * @license. * Copyright 2013-2017 Mathew Groves, Chad Engler. * SPDX-License-Identifier: MIT. * ----------. * earcut. * Copyright (c) 2016, Mapbox. * SPDX-License-Identifier: ISC. * ----------. * es6-promise-polyfill. * Copyright (c) 2014 Roman Dvornov. * SPDX-License-Identifier: MIT. * ----------. * eventemitter3. * Copyright (c) 2014 Arnout Kazemier. * SPDX-License-Identifier: MIT. * ----------. * ismobilejs. * Copyright (c) 2019 Kai Mallea. * SPDX-License-Identifier: MIT. * ----------. * mini-signals. * Copyright (c) 2015 Jayson Harshbarger. * SPDX-License-Identifier: MIT. * ----------. *

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\png[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\png[1].png	
File Type:	PNG image data, 128 x 128, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	796
Entropy (8bit):	7.286495708720538
Encrypted:	false
SSDEEP:	12:6v/7BK1rWvIJAsI81inAJvKPs57fcril/vqompRzkSZpHtWhcF3+VUvG7:uKYvIJAsI8k8BQml/vqbvZpHhVbG7
MD5:	6433D04695BF8810F712AC9DFAF188EC
SHA1:	19738D0F653BD3DFF15080C0C476334730B21E68
SHA-256:	76E8FCC4D2F997CD56A48927D13A0C6890254796320537897196 32B4ED0A583B
SHA-512:	71D009172040991D874FEEEEBA85A19644B6B88B9AC4799261B1821432B551154901A0639AF3B17DC7F0BEC53C40CB30004066E99885CC21E8A74452B796323B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://drive-thirdparty.googleusercontent.com/128/type/image/png
Preview:	.PNG.....IHDR.....PLTE....0$.0&.0%.0%.0%.0$.0%.0%.0%.0(.0%.0 .0%.0%..WM.....=2.J@.....qi..J@....~w....WN.....c\.d[..qi.0$.0%.0%.0$...%...,tRN S.@.....0.` . 0.....+.....IDATx.....0.D.QvG>.....c...r.W..}"=EF_...S.....S.....n.r....."y..p.....B....].+\*...r1.... @..... @..... @.....*.a...[.*]c....+...H....2r'....._... rO.BUKG...gj?.....x..}#.}...A."PT.I.!P...N....N.....O..a...Y.....q.6....DU...%.#..o....A. @y...@.....!.`3. 0.OF.@.....f.@.....~'..a. .y..~...e .@.....@.N..q..%....F.@...@..P.f..t...p. `... ....@.N....q.$0.g..D....=....(..d.a.....j\ C...@.g...7...@.Xp.....x_cg .@.3.. y....<...J.....,W.Y...n.Z.V.'..|./:m..z...\....R...\..>....W.k.w.....w.....X..7M].....m.<...(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\png[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	208
Entropy (8bit):	6.3894741306138725
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lmeQj6ifbRFaJEmaS26ZY/nKzC3BGlF+bwE9UIkIY1PBa/Vp:6v/lhP27RfNtStmyzuwZR0dp
MD5:	64014ED0F78C6095E4019B598FAF5A90
SHA1:	4823CD4A152E94EC526D222A355F5D73907D4928
SHA-256:	694873A039B03CD65FD0AFDC56AE6901F2049DB7CA6EA131113098E076717E7A
SHA-512:	FACD49C807EFBA688581788D5C33EEE4D318CE81D05C67EC6DABAF63A389A2009F9C4CD897EDA345FBD44C5361E670EB6738A9961C3F5C0D60E6AFD27A6B0 6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://drive-thirdparty.googleusercontent.com/16/type/image/png
Preview:	.PNG.....IHDR.....a....IDATx.c.e....@.=..'..0P/`.1(..)5.?...5.....K..g....w..P4.~..?.<.-.g.B.....5..}..?.....d8n.~.5....k...>.?....a.B1a.....@...?.+#..\.7.=E.x.@.....I.gE.. %.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\postmessageRelay[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1134
Entropy (8bit):	5.2454521727986645
Encrypted:	false
SSDEEP:	24:haJspVkO9saAW3wFAItaSgaJspVkO9stZw3wQZ0aSI:5pVLs3W3nIoppVLsta39bX
MD5:	44446BAFF22D4BF9E63702DE47E75F0C
SHA1:	CA88789006B00D14117974D3DE226B7190CA06B7
SHA-256:	ABDD20D1F331B04B0A43D06C6ADB0F1F7C1A4DD1E13502B433665AB5591D6B08
SHA-512:	A994FF7E0392FB3CEFE2A2FC36EDBA1D1E7355F1C814727358A3ACC9869789F11BBD1B2C3246514F2C81A420A3A84550CC3007E76B03D21123DA0D99EBBD35 3
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html><html><head><title></title><meta http-equiv="content-type" content="text/html; charset=utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge "><meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1, maximum-scale=1, user-scalable=0"><script nonce="IyPP0hXuMfiFTk 8PfwlsBg" src='https://ssl.gstatic.com/accounts/o/2038943760-postmessagerelay.js'></script></head><body ><script nonce="IyPP0hXuMfiFTk8PfwlsBg" type="text/javas cript" src="https://apis.google.com/js/rpc:shindig_random.js?onload=init"></script></body></html><!DOCTYPE html><html><head><title></title><meta http-equiv="con tent-type" content="text/html; charset=utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-sc ale=1, minimum-scale=1, maximum-scale=1, user-scalable=0"><script nonce="1PQc4QdA0KkBlUrfu0HO3Q" src='https://ssl.gstatic.com/accounts/o/2038943760-po stmessagerelay.js'></script></head><body ><script nonce="1PQ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\products[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.264368684164877

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\products[1].htm	
Encrypted:	false
SSDEEP:	6:wRkrQWR0iYBtqWt2aSyu7ZWlpz4iRWuNJToP:ekrY1tdky+WXzRwGU
MD5:	39D153C02077812830B1179ACD18A322
SHA1:	0DFED5CCF0D78F801BBE7B180A2436269D946CBE
SHA-256:	1FEADEB269D052522A47B766846E61782CA730858D58CC0EBBBC2A0A157545B1
SHA-512:	CD3D57AAC09690B05983E0E4EFE1831D68F1CA70FE54AD92F76E98253F98C156BC8B96922E348663BC65C7BFFFA85A209BBABA701E5E2ADDE6C00207EF089E83
Malicious:	false
Reputation:	low
Preview:	<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">.<TITLE>301 Moved</TITLE></HEAD><BODY>.<H1>301 Moved</H1>.The document has moved.<A HREF="https://about.google/intl/en-GB/products/?tab=oh">here</A>...</BODY></HTML>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\proxy[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	436
Entropy (8bit):	5.318180426518943
Encrypted:	false
SSDEEP:	12:hYA0HqJmqGga2S79hLFBkAAqJmPm/esHb8a2J4Nbx4IQL:hYPcB22cBvPz7r2J4NW
MD5:	3444D0F9626854200FBE43D992DD7610
SHA1:	B5F7507666D3DEC70E668BEC7DE5B237AF81C1C1
SHA-256:	77BA9B077CA4051A56C4C500D66344182F4113CAA13C9B88FD2018CCA024C54D
SHA-512:	25DF90A24246A94046408F9921B1B615A26ADE02982989EF7E7D310C9EB2502C155E81BFDDE660CC3005DB8F20F64B4A29AF151E82EC76D3F29C6845978EADF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://scone-pa.clients6.google.com/static/proxy.html?usegapi=1&jsh=m%3B%2F_%2Fscs%2Fapps-static%2F_%2Fjs%2Fk%3Doz.gapi.en_US.3k1wIje1lec.O%2Fam%3DwQE%2Fd%3D1%2Fct%3Dzgms%2Frs%3DAGLTcCNT4ir0QEJ6sXXAMZvqjav9vQSaLw%2Fm%3D__features__
Preview:	<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script type="text/javascript" nonce="rWTxbbBARIJhJ4bJzbK28g==">. window['startup'] = function() {. googleapis.server.init();. };.</script>.<script type="text/javascript". src="https://apis.google.com/js/googleapis.proxy.js?onload=startup" async. defer nonce="rWTxbbBARIJhJ4bJzbK28g==">.</script>.</head>.<body>.</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\proxy[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	872
Entropy (8bit):	5.3290142047344595
Encrypted:	false
SSDEEP:	24:hYPcBafBvPz7RC4NiYPcB/swBvPz7wsd4NW:Tar7HNaBr7SNW
MD5:	004824C2FEF5D3A97E11BABE1A591857
SHA1:	3DB85D3B02891DB6053EB4A38B0B91164D9C7F51
SHA-256:	228FA34B4A502021F3EDB5B2B41B1658788E1E2F8EB5582B1982F3F57498CFDD
SHA-512:	82074D2773315C17F4A18F118431392E7C763A2910428499371FCB08CE361B15736A7E807D0E849E4263A12F6AD1FA82ABC6D99828F4E634A7983EC672ACDED6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://realtimesupport.clients6.google.com/static/proxy.html?usegapi=1&jsh=m%3B%2F_%2Fscs%2Fabc-static%2F_%2Fjs%2Fk%3Dgapi.gapi.en.L7mys-cL6BM.O%2Fd%3D1%2Fct%3Dzgms%2Frs%3DAHpOoo8QoBZWYtEZfsgOGqh_X1WKvJV7Wg%2Fm%3D__features__
Preview:	<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script type="text/javascript" nonce="e/N2oEg3SpG8ykDC05IB7Q==">. window['startup'] = function() {. googleapis.server.init();. };.</script>.<script type="text/javascript". src="https://apis.google.com/js/googleapis.proxy.js?onload=startup" async. defer nonce="e/N2oEg3SpG8ykDC05IB7Q==">.</script>.</head>.<body>.</body>.</html>.<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script type="text/javascript" nonce="zcJcIDxUEg7qpS2U/CjCnw==">. window['startup'] = function() {. googleapis.server.init();. };.</script>.<script type="text/javascript". src="https://apis.google.com/js/googleapis.proxy.js?onload=startup" async. defer nonce="zcJcIDxUEg7qpS2U/CjCnw==">.</script>.</head>.<body>.</body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AFB8gsydGaiBWsT_kkVS3XJyabNw-tlKUQ[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1160770
Entropy (8bit):	5.493280600767346
Encrypted:	false
SSDEEP:	12288:qHlPl1aVQd9fHdXemKv8BQ2X5wYtDlSQuzPY9tiGL2Mkt6dr/dXZ:o1aVQd9/sv8p5wYtDlSQuzPEkGh9
MD5:	E89195F81A66B01E98ACAE9FF559669F
SHA1:	672CC5D68FE8DB62013AE02617C372CAA315711F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\rs=AFB8gsydGaiBWsT_kkVS3XJyabNw-tlKUQ[1].css	
SHA-256:	DFAE76DD1D0D0E76E1ADF012AAA0BEBA21D154D3700EB591001A9CEB7C63242B
SHA-512:	7FA587E74262E9610D46B630E67FDEFF0AACCDFDE38C1955BAABFF586A4B0D09F0ED8A0689D0ADD7ECC400518D9836610E000D5DD58CFF64E2F57791148932A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://drive.google.com/_/drive_fe/_/ss/k=drive_fe.main.ZMY3bwZ-a2s.L.I11.O/am=9REAJjCYIVFXBSlRIBA/d=0/ct=zgms/rs=AFB8gsydGaiBWsT_kkVS3XJyabNw-tlKUQ
Preview:	.h-sb-Ic{position:relative;display:-moz-inline-box;display:inline-block}* html .h-sb-Ic,:first-child+html .h-sb-Ic{display:inline}.y-Ak,.y-Ak-hi-S{height:100%}.y-E-j{background-color:#fff;font-family:Roboto,arial,sans-serif;font-size:13px;height:100%;position:relative}.y-E{box-sizing:border-box;height:100%;overflow-y:scroll;position:relative;z-index:0}.y-xm-D{box-sizing:border-box;background-color:#fafafa;height:0;overflow:hidden;padding-right:16px;position:absolute;top:0;width:100%;z-index:2}.y-xm-D .h-sb-Ic.h-R-d{border-radius:3px;box-shadow:0 1px 1px rgba(0,0,0,0.1);box-sizing:border-box;background-color:white;color:#15c;cursor:pointer;height:35px;line-height:35px;text-align:center;width:100%}.y-E-gh-D{box-sizing:border-box;left:0;overflow:hidden;padding-bottom:12px;position:absolute;right:16px;top:0;width:auto;z-index:1}.y-E-wa{font-size:14px;font-weight:normal;margin-top:16px;text-align:center;width:100%}.y-E-wa .a-Ra-Jb{display:none}.y-E-wa-Ma.y-E-wa{font-size:12px;font-weight:no

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\so[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47193
Entropy (8bit):	5.736535507904976
Encrypted:	false
SSDEEP:	768:6g/d9SvRuj45M0G2kknoVSPlMzpQPFJ/N4BFx+Yq:BeMAnoQPuzI1gz+Yq
MD5:	A067BD7C48F3D195A5B6A49491FDAB43
SHA1:	8942BA3DA23F2CBB01B26AF8F9232FAF6F60588B
SHA-256:	BD13953112025A990D1827B52E000BEA8CD85497AC0A011B26FB935C25E5DBA4
SHA-512:	34BEAFF4E6FD993979A60EA4EE42FF2307BDDD204F38EE1B1371308C695CF64D8C4333ED2F957A063EA18782AB10B7B9E7142F15E20C6007BAB3AE068A9674AC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ogs.google.com/widget/app/so?origin=https%3A%2F%2Fdrive.google.com&cn=app&pid=49&spid=49&hl=en-GB
Preview:	<!doctype html><html lang="en" dir="ltr"><head><base href="https://ogs.google.com/"><meta name="referrer" content="origin"><link rel="canonical" href="https://ogs.google.com/widget/app/so"><link rel="preconnect" href="https://www.gstatic.com"><link rel="preconnect" href="https://ssl.gstatic.com"><link rel="preconnect" href="https://apis.google.com"><link rel="prefetch" href="https://apis.google.com/js/api.js"><script data-id="_gd" nonce="zrTHjC+lwxBU6OUUf27XFg">window.WIZ_global_data = {"DpimGf":false,"EP1ykd":["/_/*"],"FdrFJe":"4723212063367194 9","Im6cmf":"/_/OneGoogleWidgetUi","LVIXXb":1,"LoQv7e":true,"MT7f9b":[],"NrSucd":false,"OwAJ6e":false,"QrtxK":"","S06Grb":"","S1NZmd":false,"Yllh3e":"%.@.1614048691079128,173058767,2516611167]\n","ZwjLXe":49,"cfb2h":"boq_onegooglehttpserver_20210216.01_p0","eptZe":"/_/OneGoogleWidgetUi/","fPDxwd":[1763433,1772879,1782333],"gGcLoe":false,"ikfjnc":["https://drive.google.com"],"nQyAE":{"wcLcde":"false","tBSlob":"false"},"qwAQke":"OneGoogleWidgetUi"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed0VDNJ161.jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 960x640, frames 3
Category:	downloaded
Size (bytes):	92301
Entropy (8bit):	7.976718791180535
Encrypted:	false
SSDEEP:	1536:3PDrZo1sYV9OrYJfCiunrzZBcU7EOg2mFpgYM0sIcJtvIh3hzJiN:33C6YV93unrNBXc00sIcJtEMN
MD5:	B430385D049983793E523E4AA429D358
SHA1:	01667FAC2B16289CFA10417BCB9B414089446CCF
SHA-256:	32BA351E2221C0678271DABFF624519FE92AD0FE477A071F7862E523BDDCADA3
SHA-512:	A5824F352CADEAA3C359226008F1A229F0824E61EF03C7D92FAEFBB702F97F6B3675BFDE54D143BE3C12BB48DECC255CD59CB63A6B0CF4A4A75E3D18047043E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/k88BuFWA8lUWM6U0cZ4J3C8afW-a1CbiAn9StagRWO3vSbGTYBSwVICxE-WN-58bVjb5A3yWDcTBP_ud4OTxbe-KoxU7iumBkirlgg=w960-l80-sg-rj-c0xffffff
Preview:	......JFIF..... ....!%!.%.....".....J.....!1A.."Qaq2...B....#Rb..3r...C..$Sc.....4s...t.....8.....!1.A.."Qaq..2.....B..#R$3r..4b.....?...p...W...)....B..).D...N.....*p.D.C..E(.E..)...@.:..)...DQ..)...*p...(.S.!D..B.!F..S.*1@.Q...E...B...D.QF...J.P..Th.C..4...Q.F(.R.F(..*"...".*4.T...b...(...F....1J....(.(.`.1J(. Q..h.)Q.T.(.4..P4h...QF)E ..J)E..4b...TiP..J)P..F)P..(..B.B..*T....R.R.B....T...F....B...:.0.*T...4.P....Ch.@.....)Q.@...B...i...B..@.4....)Q.@..N....j`.(...@.).@.p..i..H.F..E..8...(...J.H...)E8....HQ.....E...).".....1@...@S..Q..@..J...QJ..H.F(.1@...Th..".....b.....(.F.R.E.QD...h.....(....iQ..(.....F.R....Q..T...J.*..F(.@.Th...F...B.....`.4b.P..F...R....)E....(.@...T..B.i..T.Q..T.E.@*T....R.J.....B..B.@.`6).4..)R.L.B.*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed2WZK0TN7.jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, software=Picasa], baseline, precision 8, 960x640, frames 3
Category:	downloaded
Size (bytes):	53095
Entropy (8bit):	7.970769631877502
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed2WZK0TN7.jpg	
SSDEEP:	1536:HadjZlUY7ghCy0wuviFptalddHeC/aoYL:Hyw79pYdX/azL
MD5:	BFCEFEF114DCCA2A1B67960AD17ACE09
SHA1:	817C760E2F4B685937EB02A2F56549E02121D394
SHA-256:	43BE61B18B74A9677A87B1F441C3D8E851736E41AC120844D6C00D85F74310DF
SHA-512:	5C565B6FF133E1939026BBE9DE9C346561C8AE91DA16538BDFCB863909CE7F408E945A16C8AE98C971731856AA8BCA9C81BFF60B4EF1439361FF708A87A34EEA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/vG-LoMt3vmMg1CaIS_rNs0LNomed4_E3yPUtvue8Np5O8n8gUoBpWsdLQhlKdhuh49ULXYRN0CTRoz0nO8cFjWvfP11ApKbpVVEu=w960-l80-sg-rj-c0xffffff
Preview:	......JFIF............*Exif..II*.......1...............Picasa.....@ICC_PROFILE......0ADBE....mntrRGB XYZ ....3.;acspAPPL....none..........................-ADBE................................. ....cprt.......2desc...0...kwtpt........bkpt........rTRC........gTRC........bTRC........rXYZ........gXYZ........bXYZ........text....Copyright 2000 Adobe Systems Incorporated...desc ....Adobe RGB (1998)...XYZ ....Q........XYZ ....curv.........3..curv.........3..curv.........3..XYZ ....O.....XYZ .... ..4....,....XYZ ......&1../... ....!$!.$..".......................................O.......................!1..AQ .."aq...2R..B....#3Sbr...C...$4T..csD......dt...............................0.......................!1..AQ."2a..BqR...3.#.............?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamedE2HB8ZZ2.jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 262x262, frames 3
Category:	downloaded
Size (bytes):	9930
Entropy (8bit):	7.904934976752398
Encrypted:	false
SSDEEP:	192:pDCVPVRausubE8Q3f+selmM1S/8LpRFOH2Rxo1YMvhdrr:dqjsLHFedo0FjPo1YMvhF
MD5:	65C82F3AAD9E1DAF1FA9B35DF1F232A0
SHA1:	9CEE679ED7375132A7BC81B1D07F31F49B5E8451
SHA-256:	2E4BE8158D158D5E2F6471AC8AC685D771B8344A024AAFCC3FF53221EC93C63C
SHA-512:	480926B662954C59B7E305D53CA0FB95195FDD36DFD59CA1280FB0ED657697B55124CF0864AB9C05C528FE8A7D4E57E20FBA15ED61FAE558045EEBA97D6166
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://lh3.googleusercontent.com/DaeHJ1cE8YmvDBsBfBOxacn27nsLy35yHgxW41xMHbQbgmCrEd6GAMYWBY9ucReiZDyh6hHJOFQ6RDFx3ByAX0G40D56DDMsDzlZLQ=w262-l90-sg-rj
Preview:	......JFIF..."...O...........................!..."12AQ.#aq. ...3BR..$CSTbr....4D.......%ctu..................................%.....................1.!A."..2Qaq.............?..)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.)J.A..zhb.hE.2.,. .9...B.G..) ...1.. MZ...9$8.#9.A.R.'..C.....#...#(go...;.X...".$. /.(7.Q.g....Rz 2lVo.y..@.'...z..{...7...?.....s.....J.k(f.y..;...U....&.Y.&L..B..8...9.....?..(6[.zm?.........~kC.l.e.d....k\...k..... .^...Z#..>..~...{.Y....2..<.s.......l..F...........q.!..a.H.f.zK.@...l.....^ .....n..r....%...1..B.RE.p.9..`s0..1...wvmo.3J....fR'.....&.k...m...C.t.(..(..(..(..(..(..(..(..(..(..(..(..(..(0>.O.5q.l.....o.[y#.... O.Z..wr.X...!.Q./L..V.w..ag..\...F-..*.Y7.@..3*.c,...#R...gH.n...4>...)A-.f.V1."..6......\.=:.=.>.V......Z.}.{.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamedMK3OZSV8.jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, software=Picasa], baseline, precision 8, 960x640, frames 3
Category:	downloaded
Size (bytes):	107599
Entropy (8bit):	7.966756052290182
Encrypted:	false
SSDEEP:	3072:H/MPf/bsmwMI2sitefa8CvGxJxyINtjgJGs9l/olPYKIw35PnlY:HGtwMdEfa9GxHdjgJDl/olPYKIwpPnK
MD5:	38C71AB6B4B4A5BC3B28D407424E052E
SHA1:	5556D7194BDF7EE5DB70E4E7B475D4749C8F4082
SHA-256:	2B9FF4FB30075E67A4257F4F6BDCFB6DBCCFCF7124CA02A1AA63C6D3D8260B8A
SHA-512:	288A67E5CCFD4FE5AE1108AB737445534C13A21C967777F5C5EF3AB572BFA747C3CB5F66552752632E051AEBA5562C1CB7F6A41285E179972EED8A25B869D6C
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://lh3.googleusercontent.com/n640xXBcj9ILRScUTjoU81UBKa8GZHVTNoFTpHRqG8tyBzUZ4czen8DBalMvNs0xR6BoHXhdFnZxPLux22_e46aUkUkGoFZz_asQIg=w960-l80-sg-rj-c0xffffff
Preview:	......JFIF............*Exif..II*.......1...............Picasa.....@ICC_PROFILE......0ADBE....mntrRGB XYZ ....3.;acspAPPL....none..........................-ADBE................................. ....cprt.......2desc...0...kwtpt........bkpt........rTRC........gTRC........bTRC........rXYZ........gXYZ........bXYZ........text....Copyright 2000 Adobe Systems Incorporated...desc ....Adobe RGB (1998)...XYZ ....Q........XYZ ....curv.........3..curv.........3..curv.........3..XYZ ....O.....XYZ .... ..4....,....XYZ ......&1../... ....!%!.%.."......................................G.....................!1..AQ.aq ."....2...B...Rb.#r.3.....$CS...cs................................6.....................!.1AQ..a"2q...BR..#b.....3Cr.............?..+..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamedMY7UJEBU.jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 262x157, frames 3
Category:	downloaded
Size (bytes):	10000

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamedMY7UJEBU.jpg	
Entropy (8bit):	7.952157340986992
Encrypted:	false
SSDEEP:	192:faZGBxujI5pnpYGI+rd9gBA4P6QTL/RS836LEh1rnkNJK4Y2cGD:fZ75aGdwBA4P1/883ci1rnp/M
MD5:	03955D06C70538C34D7430371C9E6EA8
SHA1:	9DE9AF6A32E735F1139D10164949F072A53D5182
SHA-256:	E58256ACEA26B1BDC0F384A42FD0BC69348A5A745078D79FD2FFEB0C8BD83EAB
SHA-512:	5428C8A6B243E7FCF00E667B8CE0204C9DC6EEF3C06A5C717BD0632E4900C53CEDD5846D18674A6927B3FF52FE94BF0E2C20E1951ED121C33F61D081B1F7F0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/inMunrmxQKU2dsDv0PT1JaELzFlTn5ASRr_dBzGbAZj5Kcqk7TqXJZiP7duVgQFUVx3vBUAgfv1WP3YXj0GD9ATuYhvBMwe1FDXRyA=w262-l90-sg-rj
Preview:	......JFIF.....".....Q.....!."1AQS....#R Taq.....2B.....$3rt...bsC....%&7D.....7.....!1.AQR...aq.."S....2.$Br.Cb.#.....?..Q^.K..&..-M.s....Z...).Rb..j.Jwm...Z....(..'..(....\.Sx...&(..... Z....`R.jo.b...\.SX..9.1E.7.Js.6.....m....Y..-.....3....$#.U\.{6W*.....q.0<O..).i.A.1W.....a3.....w&@..\5.R.O...Q....A.....n.m%.....e.H.Kz&)t.#'):.....b...6...4....h<...N..O.U. ..."d...oc..[=..&i.....Zh.R.d...(.W.1.a.k|..Y.v....[...V...9X*]lM....M$K...Sn*.....7e...-R4.....X...(.Y.b.4h.t.....q}....6.|..<.Nd.h|'W.....(.]2T...{g\...}...J0..E$6..X2.;U....Vf)...M?.b~.~3.... ..&.K^...7,P..F.wm(Z.z.jgm.i.m.rV.....Nu6.-.M@...@..m.m.....o.j=.x..\<B..F...m...:.|..'.O.o0..X.h.Y....F..B../.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[10].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, software=Picasa], baseline, precision 8, 262x280, frames 3
Category:	downloaded
Size (bytes):	24763
Entropy (8bit):	7.920687051349615
Encrypted:	false
SSDEEP:	384:eYNg71fDG/EAVRMMDs+csahQU70LwdCstvVH5AoFpp6y5vwdCnKMcMN:eYyaVHDs+/a6U708dCYdZ1/r5vGGcy
MD5:	D4F98A8D07E2F9EE0DE2D2BA9DB1E134
SHA1:	992780412740CFE75F416C49D76DC8EB8D6646E5
SHA-256:	D0A60FA75E7D8ACCB7A3258F554F700CEA985B0EBA6892A2031D7AD5F2902971
SHA-512:	E4B580235A0B5A21B734DBC5284B8B98D7111E17F978ACCA1C1BDD4A7598F5892D48D55A594983FBD3C8A8EC206622BC509D307A6D4FA777FC2963265438738
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/wuqE_umq1VzK_9RN9JaoQLTrroj3_nhfVl81TuSBkR7xDiLR4Wh33mJxodjfK5gnOtjEHlC-k0vPCDOlcjj-8QyJw11kdp_yqzPDnMw=w262-l90-sg-rj
Preview:	......JFIF.....*Exif..II*.....1.....Picasa.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP ....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...< ....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1..... ....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch..... .....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Referen

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 512x243, frames 3
Category:	downloaded
Size (bytes):	20796
Entropy (8bit):	7.932897112275553
Encrypted:	false
SSDEEP:	384:F/DDDDEiKS/BE9wxLtWCTxAVjsTHX9f1xNO5+K0W5OlChdj/wlxgLp37:F/DDDDn//wMLtWAijkXTg+KpoGyxg9
MD5:	4DAA04CDC0D6D483AEE9B1ABCBD71DFA
SHA1:	02B60EB25527614565B796BD81E4E2ABCF6DAB59
SHA-256:	5BD89B199830FA702E0698A0F1709D234B200E4BEA678618F54FE45FFE4780DB
SHA-512:	A38967F34CA2E69F642C381468D90B44519E6482DC993AA839866C5A19BC4FF25A4465021C9CB87EC148DB3CE5FBFD7250DA3DC324F75F6B646CD0E1A674CCD
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/aUU5FrBysAKYHEkylRE8feg9H2qn9YAifUBlrqHPeb26Pw4dqKFqneHHoC6i-dH8o4ur-b9tR5RHRbfM2BooPDGkELxnSgXI1JDT
Preview:	......JFIF.....K.....!...1QRb.."Aa... #2Tqr.....4Bs..3...$C...%U.....A.....!....1RS..AQ."45aqrs.2....t.#b..BDd.....?...R9H.I^.]..6(J..#..%.....N8.>T...m.h..v-.Rtv}.N...3[.^. ...1h.m.Z..h..of".7...KOJ....E.-..D.DD..133.....'.I=gy.5kM.mi.....3<e.b"8G.*.(.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.....q..:..x..kRb.Lq.....a..1...>M .H.9R....F.....6.!....$.#..;..m...k...I.....u....{N)1y..i.....Wwvb.K.:.KSJ..5.jR&...E.;.b8g.....t.;.I;.8..5..i..9.....g..IF#...U.P(.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.....@.P(.. ...@.P(....Q. ...A...m5..g.....TLf1=.Q%..@.B..d)..B..d)..B..d)..B..d)..B..d)..B..d)..B..d)..B..d)..B..d)..B..d)..B..d)..P(=.."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 512 x 269, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[1].png	
Category:	downloaded
Size (bytes):	81108
Entropy (8bit):	7.987395113593556
Encrypted:	false
SSDEEP:	1536:euZ1C5vCt0QES6BMvYeQ+bMpIJZrASUUduyZcUaPTEFdd1hVxfRUCLpu8h/8UyXp:hZ1C5vCMIYeNIsuSflZcUETE/VffGPuw
MD5:	62EF2F30B12BCC3542E32C84BC6E0555
SHA1:	5BA2255545186293E91A38DAB3570A726682BD40
SHA-256:	7F8E933A41E72509DA2F4D72004F6301CE2EB2CFC0273460D098A57D7E1A296B
SHA-512:	F5BC462ED89C88EC8BAE546E69B812CC60FCB31E193D40EB6A99C558BEC0897D3B3828A0551EA0DA768FB4722A358E3C384E42A927FF630F5A97E1C32E34708 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/gxcsIvf4xu52xUtJRZN3xyjHaFjCj8WA7tCVhueEtR7J7g7nbJ07UEE0K8_XPbOfbUTVdmxaaHQcOjP8oez4K41_rF5zLMdnr8el
Preview:	.PNG.....IHDR.....lJ....EiCCPicc..H..W.XS...[RIh.P...D...H..E..*.JH..%..bg..\....].Qt-...u..bw-....uq..*oR`]}.{....?g...df...z5|.,....@Z(O..e.KKg.....@...._..q..c....?.....W.U\. ..W1.....x....A.....K.2y!.D6..M-..p..Fr. .2....R....*.MR...]..i|.<...f.g..r ..-.=.B...=2.A.1_.q..C..&.0...Y_....3k.....\.B..(d....g9....+.|8.F...T9.....4...Y.q..B.N"T.C.R..d.=j!Ppa...b.!? ,.b..#...1Z}V.$..1.!.4I!/I;v.H....ON....r.G;../W.U.R.%s...".....bqR*.T.0j.$%.b]...y.....X....+.T..C..I#C5.XF.<"Ak/+P...%.X-.*.'Ei.....B.(.r..xD.q1...Ea..6.4Y./v_V.....#....dQ~.Jo.... (Q;..U.'.....'i..3s...5..E .pA.`.%lY`2.....n.K....@.r...k5.#R.=R.L.....D@18.T.+.EP.iP.y..luo.zD.x.q.....R=J:.-.<...7..0.|.T}..8P...(.xYz...pb.1..At... <.....<q6.7.....'.v.C.uB...$l...X .....8..qG....2.L....#.....={C-W..*w..s0./j...xPP..%....H]W].A.UE...&...r.{.....B.....[....`.s.a....cX3v.;..s.z..xKP..y$...k}.*.....i...p'..%9.B....".O*.6.....;..^1....y.o].k.....5}` >\.O..9.....g+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 512x242, frames 3
Category:	downloaded
Size (bytes):	15478
Entropy (8bit):	7.571067785973808
Encrypted:	false
SSDEEP:	384:eb1iSbis6ybRo6XP1bKebgLTmk0oEN9sW:eMob66XPh1bgLTmaod
MD5:	8C57D9BCFCC30305F1912FE34936AA3A
SHA1:	D89157C243CDC2070B29CFD195107EEB745D5C49
SHA-256:	9920F68AB38EA24BBD7749F8BA43C710BF7DD1599FFF0B09B9639A8B962DBD1D
SHA-512:	0D52CE73E7FE83AF519F1D2B15BAD718E8357A72680A33746101AEA69940ED198E2B3F6E610F8D8EC0E0365D3BDB370028561561D30CD4311B9AC9CE95F74CC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/X2U4aJ0BTM8vVGC3Z9AfZtkT2yEbm9f0KibL6jN8FQUlXP4BK-ML-j78wwCs5k_UjcL7AxgadJSKyNCkX2l_sEqETA9vpYhoMw3f0A
Preview:	......JFIF.....M.....!1AQ...aq..."2....#B.RT.....Sbr..3s....%45t.....I.....!1.A.."Qaq..2..#B.....RSbr....3T.$c.....Cs..%.....?..?..[m'd.....I.....6.Sr.....(mo[m.b..r..v..... *..F.s..r.m....^.:.u*<.\..6.#.....e..+...O..n=.~...../...m,.^..e..5..t3[%Kw.~...^M...1.z..Nk...../S..k~....-\-IR....t...>Mh..xW..M.E.....Z.....@.....S.0@.....\...c. i7t..2O..H..... .....F.0.3..q.:L.-}..j.Z..S....'S.M8e.T.:p...i?D....?I'+..jO.WK..~&.[..#.WX?...*j.eV.x..*..<.....q.sd.....x.....ML...}]...7.w.'...n.Q.....9..yg..^...m.8.....,\.H..T...R.:. <})S...N1.9..A].....i.tg.....8.r...J/=.....5...)...nQn)...Yn..[NG.c_.d.p..I....z._.UY.Vm.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	8389
Entropy (8bit):	7.917300776772861
Encrypted:	false
SSDEEP:	192:xIIHUCD4wavWUxq5qR2i2XT+RBSfzAeYw:n0wCq5qkxXbzjr
MD5:	939A093F38C31C1E1FADFD51983716BB
SHA1:	6BEB74F5A2876A89F9558ACCC15E48C7EF9BCB78
SHA-256:	F86B21F4B4FC02920B856A75B701275EC57CE6A185848F468F40D23327B3D3C8
SHA-512:	A241ED629788B1D2F2584C9A3842CEF529D03EE3801359D852D6CF619D7A0008F7259ADEA0FA2BFC4AF1120B8100D93309FFEDECEDEB7DA822C310C5FF073C 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/8bC8ZC9RQ_cJj5lSa8LjCfRClGeSyp4SkN72C0tMSUIqGPVjEpHeUDfAScLNKy82MiXWLBlkpMl4FhJGrGRDhzHxOoXq5v-QSt-rvg=h128
Preview:	.PNG.....IHDR.....>a....CiCCPICC profile..x.SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH.....H.. ....g.....yx~t.?...o...p ..$.....P&W. ..."....R...T.....S.d.....ly\|B"....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.).f.."...#.H..L.....8?.....f.l....k.o ">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....l.~.....X.v.@~.-.....g42y .....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@.....s.t4.]...k....=....K.ut.}.. c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m..... .....O.....:..L..$R...J5e?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[3].jpg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 512x243, frames 3
Category:	downloaded
Size (bytes):	13842
Entropy (8bit):	7.585076465045905
Encrypted:	false
SSDEEP:	192:VmX44dUDZg2XM1aCSOtc+/hklAHHSFd9x+87cIli9xYfCeSWJXu/k6bvOurn:8ZiNg2XTPW/pEAERlBli9x/WJAvrn
MD5:	F80F8779D7DB0B6D53F13590F12DAB66
SHA1:	2AC503F0B79C928601B6FAEF2971E240CDF11B0E
SHA-256:	3D863197361448BB014AD7749C7ADA3754D6157F91D8E91AD60E5E9FE9995CC2
SHA-512:	8CB1732A316F1D466B18A114ABD587EC2E41119833B8D928A330AE140CBCA04F0ED56280C6B549DE03128E509079A6EC9B5864981B37066DC941C37FC6343DC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/7Rt8jZhq2EoBXhnDnXizU8KvjVPJpbUZXjd7fCS2ZBlytMGqLZ3UB4sovW5Rkgnaynr_m644LgC65jXRWAh3ummVbtjwuqCNbm4F
Preview:	......JFIF.....I.....!1...AQq.".Ba.2R ..#b....$3U.Cc.....%4Sr.....C.....!1AQa.."2q.B..R.....#Tbr.....CDS....34.....?..6.}.1.....!.~.....G..q....~.....G..q....~.....G. .q....~.....G..q....~.....G..q....~.....G..q....~.....G..q....~.....G..q....~.....G..q....~.....G..q....~.....G..q....~.....G..q....~..jn.dH..$D.....@... .....}W..gW..I.....+.)..#v.y...|?../yyy.FVcaB..$.x...R.RP..i...t"2d..C.HX.....L!.'..P..G.+.Jzk.+...T.o..=ynk....h^_N.\.'.7.:.....h.Srx.Ud.9B+zU.BzsJI6 ..>?X:Kc.f..<.....@..... ,..@. .....2&v.....y6Q,...eV.*..Y8.zS.....i.%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[3].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3455
Entropy (8bit):	7.723315830615501
Encrypted:	false
SSDEEP:	96:924aQnKiPOIJFNOQBr1RQpjugSt9cRWOBF:WkK8PJFJr1RQccRW2
MD5:	5499503313D1C9B3BA932AE65707365E
SHA1:	3F05538E4A24B2350FF5185E896C5D378FC11AF3
SHA-256:	0C7BD76817726621DBBC8E1E032C1159A6D1161AEB2D0D3F0FAAE7092063733E
SHA-512:	C80586D8CB99CD654B9E31D53919FD9D0E8C9DA9D772D291B905471B22036435BCB30EB3E25AAEB8B4937986B7AF84F74FE683120D224887469B5D3DE315188
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/Q4UDu0hKQgAyUzO0RpJTpTKc2DyaZbU-K96JCJjqKd9_ABetMMpS6LxO6Y7Ypm2CVhCro4n4n9PTF97SlwrSjmJFaHdV-_yDr8MpX1M=h128
Preview:	.PNG.....IHDR.....>a.....tEXtSoftware.Adobe ImageReadyq.e<...%iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c002 79.164460, 2020/05/12-16:04:17 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop 21.2 (Macintosh)" xmpMM:InstanceID="xmp.iid:4D93FB6F206D11EB9DACD75CA1E8539C" xmpMM:DocumentID="xmp.did:4D93FB70206D11EB9DACD75CA1E8539C"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4D93FB6D206D11EB9DACD75CA1E8539C" stRef:documentID="xmp.did:4D93FB6E206D11EB9DACD75CA1E8539C"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.%q,....IDATx..{.TW .....n.u....R.....V..1U...k.k....MS....j..5.Hj...b4U.E.I.M..V..Z....e.d_....{...e.d.{...;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 512x242, frames 3
Category:	downloaded
Size (bytes):	20984
Entropy (8bit):	7.9024862601957935
Encrypted:	false
SSDEEP:	384:ZENLI0lHtMb4M63o03wG0ZjkXHWvMSaUshEHS9lvlvlvlvlvlvlsTlskgZJZJZJA:ZEN5Hi63o20NkgMSuTKOkaXXXm
MD5:	673298049EB23E307520A2DDFCD9711D
SHA1:	B4475302E875C7EA49B0BFDD15F7635255924018
SHA-256:	CFB90166D5AFC4D7DFB156BAD1F43BDA3DE659B584FC4013347EC1BC201873FF
SHA-512:	C2E2DEECE61D11CC9D7A35CC083EC6ECCF6460625ECA7FA21ACC3B2173A578FEDCEEF661F7496CDDE6E0941E1DE2F9525FAB44CE1A385C588AA59E9A3F02 1E48
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/vcggGGHCBGfDfzLo3wVBsORCiQDAMetdIP2F5HkhSXkp8VriiHrfm5-_BAChoX5rL5F4VuJx_Xdy9gbT3-oJ03wS4Z3w9izEvqjkyyk
Preview:	......JFIF.....U.....QR.....!1S....."2 AUaq....3t.....4Bs..#$Tr...5Cb.....cd.....C.....!..1R.....AQ."2Saq....3r....#Bs.45Tb...C.....?..;.....f....R..D.D...../s.....Z.....n.7.1v.'&....w ..};.....p....].9,..j).$....t..K)q%.y.$..'.....\|Km....P.. ....QJZAi .b..{.....N.....W.LT...zY...\^.$y..5...5.s.h8.....@....sx.'l.qof{m}..^.....J. (W..9....(I....qn..uk4.:Y..$.I$.$....R.6.|Km.....@....@....@....@....@....@....@....@....@....@....@....@....@....@....@.....A.A...(..%6.kj.|Q.....W....f.....y.m.b.....L4z.W. [^.....B...c.I|.h.;...._..{.}R.....G...>Pw.iz:....i.U..)...=..'.W.....Ot..]....#..|..'Z^...u=.j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[4].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[4].png	
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4488
Entropy (8bit):	7.9295065176531345
Encrypted:	false
SSDEEP:	96:FTSd7aVqzexR58bFZ9+A4qGqQ2Wt2jAAj5NUZxF4cv3S:F3KbNB4i/Wt2LUZ37v3S
MD5:	219ECE9706D651F71C203671F0AE3C1D
SHA1:	C0B58EB1DB07DFECA0E6569B4B4B307C01CC56E6
SHA-256:	9883B490936F31AC90963F476C2164C5EB72711F975EEA5EFACC7573280950EB
SHA-512:	81E657B3312C4D7355C887287AA95E698E660B7AF2D311390DFAC8D47D35E1F04410F0C78C01043D0FFBCD4CC1C014D4A912CE92956631327713077 8F49384B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/BAwQk6jAMu2s_7Jh-8-_CsvSwEAaeLsVhL8z82VOoEkoaujxll1kYL3Pz4jkYpLbRpUA2fOZTtlppG2gXpsDoijSo1a1M5uPvke3=h128
Preview:	.PNG.....IHDR.....>a.....sBIT....|.d...._zTXtRaw profile type APP1.....JO.K-.LV((.O..I.R..c...K.K.D.....04006..F@.9T(.....Y.....1....H...:.C2....IDATx..y...y....K+-.1...0gb..)n..Z$s...)L0...b..I+..B@..;N8l0.D...@X.]a.....8.e@....d$.....G.fz.~....Um.....o^....^CBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB..o..3g....}Q...d..0.}4o....m....3.....wz.x..E....%.....u.A..1.....X.P...s.k..d;.c.9.'5l....D..|.5J...W.Q.`..C1.g.y..A.....;d..l....8....q.1.....J.....Uw..0{.A...r....W@9._qh9...]s;U0.\..4....p..i..+...Q.....=...~!. ....6^&+...j.ks.....M....j..8i.K.25.s}'n.Y..8....m...._.`.f..s.!..:....'`....d.....T..[.\.....Q...KHs;5L>.q..wd....#....,.u'.uu.r.`0l...Y...Jb....f..mz.....9n...a.....o.....,.&.X..u.uM.>..$"....&V..n(LBq.~-....K..bf.'..jz.%)v.....|#.M..f..D.e....0..U.Pe..cnB.4....A...>O.n.j.....i..s..?B..E...:.....EG.....n.....OY..I.....j.....w.Pj;...*{....;.....,.....m.f.v...F..y..Z.J...@6.7e.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[5].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	3828
Entropy (8bit):	7.886429114351116
Encrypted:	false
SSDEEP:	96:RnhZaPV9NF7YtTdscu0Hl/SuiXyrj3MZpZ3:RhZ4Nnki0j8HJ
MD5:	5502A4B973FDDD54F1303482A8B3B013
SHA1:	78F054AF9A3740DCC0DEE74108978B34F5CD82BF
SHA-256:	30B09BBCDDDE3D3799D874E77B3682E7D5483920C1F694FEE7ACB8CB1B7FFEBF
SHA-512:	48D5EF286BB727557F5AE7F7430D83A46071A8BC75D6FCD11CAC2DB500DFDBB90E0F04C8F025B21F4CBF73D3D33EC912B7E0ED119B84AC3A8230FFFB06972E 18
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/RwVe2Cm1EjeDmYhdTzr179G0ovq_PCxgPzQ92PO-YxTBEFTHWh0L6Ev8FFDWRgRGrE81vwn95tyg9Ey189OO4kllhhpLAMIsGFZ-UKA=h128
Preview:	.PNG.....IHDR.....>a.....sBIT....|.d.....IDATx..}.....=.wf.;dD..cdY..f.. .D.J..h. I....k.*...1%.He.&qk.[I..5...$jHY.%C..*..\P..A.....s...d`..s?...w.Wu...}.{.....sN.....#.r- ...y.#J..K\..v..@.!...4...m...d....S...?_.....A ..=.A.....L.O.x.....o...M...e.s.....y."o6..Y..Q2...u...1v..3.....4..i.}....F.....+.-.#...3.P..'n..;.u.3..P.....Rjz..i].7O..kM....H.Y#0S.k..O.:.Y..!1@.....j.....d.....H)..1s...5..... ..+..O{?s.W.o.T.Z.P$.....R.>.....H..!.....TG....."&..O..'>{....Fb.2`E@....?=.k..\Hb.2`.xDi.....I.P&..j.....S...2...e$....8..%.(#V..\|M.O..k-.$.p....Ob.2cDP.K.m.. 1..B+x..9...$.p.....L.....................]J).&.Zb....(.....D.G..au.k.....W:.Q.* x...&".....J!..+..]...d@...1&.....;...5".!..ZG..C...R.i..s.<Q@..q).....N..87.(.a.S'...!.q.t(k.....R..m..../.)%...l..tqNd...i%).....L.....V.y..@[1:].....juk..W.a+-#.{..k.@...M...`.&..."..n.j7x...S)?...y%k...."..I..j.Rf.F.@.R].|.....\....&....hR....km..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 262x224, frames 3
Category:	downloaded
Size (bytes):	4349
Entropy (8bit):	7.642387148857661
Encrypted:	false
SSDEEP:	96:n0MGbAi3GjFy1re25SOT12FZL5kaQHTBTZgJ/L9ss6CSnEQ8ICJU+o:0Yi31Sk/WxmPxZgN9sISnEWwU5
MD5:	6566E6BC8E2E4852AFA6308ED1F72FDF
SHA1:	784725C7C77466BD754FCB7AFABBE6BE7095667B
SHA-256:	4C09896220278C369ED7F7CC39D151DCA86CF8A2F4825903EC1C4FE25769AB22
SHA-512:	D13D0A909C4982CAE3C9EFD88663AD2AFEEFFFA32C9291700270C770A55FF11888EFA03D1865FDA5FFDD91B3BF02CD1B16355E9AE98A0DA7BC8B986194A33F F3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/i6R5h1krvImzjY8lWhADQUM9_SyZkEvGcTRQgIfFRFV9JjAmxdh-CKw8c6qwC9gre_boxhoYT8dp14VpPmFfyIZ8Q2oyvM_w4VeS9hY=w262-l90-sg-rj
Preview:	.....JFIF.....".....L.....!1....4aqrt.."$ 6ABQs.....#&3b....2Ru..5.....Sce.....#.....1...a.!"AQ.....?..0.....PvP...&.b.<..G..L:.uP.{.v....-.....f....=#C.:.].n...J..e.]2tF[o.ew"~&.s...7.Q.g.9d..._..m.J.....w..sV.S..=.{}.jmw.5.H..e....k.J.z2(..yM...s.i].|.t....]..".bX.....~.....!....b.g.;.TSvB..7.i.....P.....r...R.,.....;W.t.4....?h..Od."UJ...N..)...c..+yJVF...+..F..n....U..'.....,..E.)A.b[.c...V....!.M.#t+.u9.bVN..x..n.u.T..=.M|Hx..A,.#B..C..8...=....>..O.m\l...C..7..9.M..s..i...Wj..R..1...?...ys~.....M.JX..1}N..nO..u.I..O.....f..S...#(....e.5.:..R)>.]....y..=..v..9cN....cV..R._)..s.*u.v.h.p..z..lJ...j...q.y..-.n..U(..:..cmN..?.j..-.w.7:.L.p%./+.q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[6].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4617
Entropy (8bit):	7.928487625973478
Encrypted:	false
SSDEEP:	96:yWezFg84sZQTsQ38natgyOZe99J9tea4s/bmc1jw:2Jg84R8atg+94o/bmR
MD5:	58DD70D17253CB171516F70CF30C579D
SHA1:	569E4D1F43D4B4603E28588043225E08B91C9CFC
SHA-256:	96F76F6DC6E8ECEE165021A2561ADE8FFD42FD8D7BD0E767857A688546E5BBDD
SHA-512:	FE85B37C46D41ADA1E825F4D3733B9BBB3F2B54F0723E10491364D84277148841FE4A93ADB261EF6380D366BB8FA8FB834777222B2558D48EE3C5DF32A53FD61
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://lh3.googleusercontent.com/m5HIvqrNJHr2w5VXuNapBWKSx6YZTU7lIhffkIgDQU_VbpYAfkgXt2Un2ks_wzTn7vrfkyllWMLouCcOcBwfakYylBMe_9PwYm7_=h128
Preview:	.PNG.....IHDR.....>a.....sRGB.....IDATx..]{.T.....}..>a.tu.Z.B.b@)..@.E..I.i..X.<4.....G..I.M#.....BA.P..vE.....+;...9..;....w....$.{..s..}...}....G.....8.p4.h....G...n...l...!T. ....P...b...x..,.B..A>.+.\...g!....B.....8..Z\nh.rZN4...M_Ya.....'....y..6.s^.5X..^4./.8v.9.Q.(.w4..Z.c$=..@eCW-.....d#5Gya....q....6.7.....le...}.<<P.E.R.a.Z.N....*.-..y....[k.z...._. .|.....-i.!...>t.{.lS.V-ikM....r.....X....i-.Q....XW.}:P.9.d...V.....r...'8..X..n-u....1.YcM.l.. ....iRK.@....C...-x.em8...\.+.. .%.`...pt...K...#x.v.&...mm.y#....T.x.]......b..e.< .d.>g,../...../.....=.f.i... {.{...l....3..R..P....%....1./S..rU.".E..a.1F.l.....p..l_W..H..5.;_.....<..{gh.F*Uy^.Op....C.a.t.4...`_....".._.....9.....J.V.....Z.;1.....:$F.....TSQ.W.....&....._..).7.1,..];...1.z..S...o..03 .....F.#=*. .J.....6l..H...H...i..b.N.+....w...P.....%BfC.Z....,.....@h.Ax.S.kov.&..o...CM.....Z.N.O{.."}T._.V.hf.4.#..{&O+.+.C]i.3.[1.....0...'.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[7].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=1, software=Picasa], baseline, precision 8, 262x202, frames 3
Category:	downloaded
Size (bytes):	10627
Entropy (8bit):	7.732039648189364
Encrypted:	false
SSDEEP:	192:eYNMtKw+7MUVJs+R73QPK8csAoa8Jp4aRUgOVz+xvQ:eYNg7+79eu8csAr8gaRPAz+C
MD5:	2EBAE441183ADC30B06FF872D7525FBB
SHA1:	49BD88550732804E34191240C71FBF276907F086
SHA-256:	450DFF42576033A6459F154CB22B15FE1C09880C50D15E023581F362C4B29760
SHA-512:	9ECBC7EF02508650D28BBF770B70EDE4537405242546A190AF0786B82DFC2C60C242B3B18E13C13665ABCB0FFCB7058D59AF73708C390E5C272DFF652D857E4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/KFqYip3oJZGXXDArfdbTmusp-9Wxf36yOiu2r5JgBmwdW6Bpp9s9DnajbUmshJto1EcCYqLz4Hut8KSAK7YWlBA-fposK5jy0wAR=w262-l90-sg-rj
Preview:	......JFIF.....*Exif..II*.....1.....Picasa.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP ....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...< ....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1..... .....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch..... .....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Referen

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[7].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2849
Entropy (8bit):	7.902475938239269
Encrypted:	false
SSDEEP:	48:JyvUTZXZMNnTa0ue4kJkEoWDXwtsl5quLd7vjU5ppuBcGGYvFuLYcobdoPFJMW7+:i1NTse4kJboWDXzq0k5ORLvFuLtoRgM7
MD5:	526873B718B33E92AA22FA85B197D2AE
SHA1:	1C24DEA8CB86F97F653DEED45824313FBCD6F87A
SHA-256:	E561EAE5D9A60DF72C07EBC03B74D6176C866FA46F6D00539E19AFD8A1AF3D16
SHA-512:	A6D15DA8F3340604C1D4C64F8F4B9ADF8158C90486A18ECA66080FEB0E0F89ACDD6DE413FCA7A51DAE6B6BB3A0E9B874784E0E57D4FC49359A625722FF8ECE 6E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/DaaQa-Y-b3_IAhu6SBFb2vRl8PFR5iuCLwLszc16_OTlLrEFvFF9P4CS0ui-414nG9016ul3dQD1R3mHtmMx4P1bIA-zRXuPpFN4yw=h128
Preview:	.PNG.....IHDR.....>a.....sBIT....|.d.....IDATx..{.....}.....D...x....F..D.R)Q...T.QS.b.....X.GJ..E4..Dc.G..1T 1>P..(.8A.P..qp....3..c.c=.7.....W.uuW;}.._.....`0.....`0. ....`0...E.*.....$.4!..B.j@.*m.#..t..].c...\..b..jM{F/k{v..Z_....~.m...A...[.....Hg.4..-e....!.n^+....O.t.W....g...e5Ik..vB.....t&..;?..]).....kJ..f....|Y ...c..x.A9.!#UU..s.p.=.....h...wC. ..).....'...i..!h....r.....z..^..$@UTL.VT.f.....b...=. ,&..~.B"..r.7.`.....A..#.v.M._ih.LJ1(5..#@.1...#@.1...#@.1...#@.1...#@.1...#@.1.....'..;.....GK..v....dQh.B..n...3.._..:....R. ...y...*}.B.*.3...c+N...:..FY.>..R.C..(DJ.....o.V..@pj~7....P.....j..~.....#@.1...#@.1...#@.1...#@.. /.....l.B...E.....,&.[$b%....c.E.R....{.....,s.th.j...,4m.X..Z.<-B0.<.k/.2..o"..v../.a. {..k..]W.K.....[4#bP..r.V.....uxrF.sN.}.[3._...6.....>.q.....4..6..fd...w.jpt.g'B..(..p.....'.mq..4.....X...[..._..wa....9Hv.i.v..vH.P..D...nemK85.g/...z...4.[.e...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[8].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 262x185, frames 3
Category:	downloaded
Size (bytes):	6191
Entropy (8bit):	7.896384819428468
Encrypted:	false
SSDEEP:	96:i4dwB0Cl1q8ipwzlKpm0bEMcaz0Hu2JntNcANi56vGHT/YIGz8q+OgPxxCiY7FPs:O0CLeCIga0Hu2JzcANG6XIf7OsEPXTm/
MD5:	2A162F84CF92A1C7B77FF903D71A9218
SHA1:	F4748E612C26E687B0241FCDF76F9AE7AEFBDEEA
SHA-256:	8B94455C23C1613736D03674024BE2AB8DF18921508CDEFDD44C22D91B0DF3F5
SHA-512:	AD49A73F0C59EAACB201F015A4C5E6079E50A11B3BF0156EEC2E92A20FE76D0200C1546DF4652E4F804469863533F96C71EA7674D7576326BA137E0A182D6E62
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/biI2ynlt7xlxX36wWQanaayWtQO0xIOz7esQZ9xi2WLBcJ3zS26aniFHgi9TvAAYH2hJ5SZRWmiw3-fMKeRnCH6ettKRc77ZTgFwAio=w262-l90-sg-rj
Preview:	......JFIF.....".....S.....!.1A...Qaq."2r.. ....#BR..Db.....3CET.....$4Sct.....1.....Q.!1Aa....."B....q.....?...K..(.L..t.9.*.T...s..L..gL.9R..fL.6D..u.@B.u.@A.Q.DD....D@...DD... .D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@...DD....D@....)q..mV!#s...#..!^..~....nx,.|....KQa..>5enr..,-...Y...2...Siy.c...S.O.bH..tQ0pkX.h7].q.J...~.7v-Y .}.k..O..s..Q...*.z.....WK..3K.,.6nx{F7b._?r.w=.f.Z.Kbw.1.8...GkI.h..2.@.x.....4..K.K~...'.1..f.....h..U#.".Z..K..Q}..I.9.....?e.....tNs.....!....Y.`..3[.S1...S..%.b5K.%.Z....}%'. .S.....M....:.....7...;..:.j.ue.y..{.#...]g.|.K.....<u<.OS.....t.q..d.y.....8I...P..nj.7.iG....'.N...3..>...?.U.u..:...rH.2.\7.....X.\.....aZj9...@*

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[8].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 128 x 128, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1705
Entropy (8bit):	7.726090618507379
Encrypted:	false
SSDEEP:	48:JvjQzSeYrtE72UeyG1FJs2Z9phkO3WztxvygMlHMdhs/:VbPreafJrW0PhkdLyrNMdG/
MD5:	364DB2462936493347EB20FEFB249CEA
SHA1:	A021640951371B9763F848885D88A03C869B393B
SHA-256:	B90DCC31B9AD7210BBFF4C2251BD82958BAA2D7E3E7BA4C4CBB5A6B185FFAD86
SHA-512:	04495870F49BD0FA40410D4A6C60A664123563AD00FB483796A8583998F483E96A827A53747B6A8E58A73DD07781299EE44D5D380EA210608EBB8BF15255986A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/9TzWtxtT-9VrIwa8SXTSKhfl91Ndy4hU-1uLE9-hFsVSHARAOlFEdFExVR4QCegJ-KUBTSlJm3DZY6g31sbVrUT_HfxQvX_7WgLp=h128
Preview:	.PNG.....IHDR.....>a.....sBIT....|.d....`IDATx..Ol.U...ov.PIZ..j...DK)jL !.%.....E.....p0.$".H .....M=...".4...D ..a.<...$...y.....M6.....og.. .. ....*.Dz.K)....h.Q.r'L...P.x.v!I`^. ....`&.rT..%.N...]........=<K#..hr~.W..0...B.....Gd,.....2~l.[)....M|n..z0&.....(P1.!.\....Ml.]J...@.e9...MD..% O....9..XH!.o..)..z\..L..]^...=.).Z.k.F..=....=.S?.....C=..`.Gz...$...".i2 ....i..@.H...."@.d.'...&c=..`....".-2....6.@O ...rO .d..=.....,."@.....Y#.@..").."@VI.'..jA.....{...n.O...fz..*&&...cE.-@k.9#.....E.Z.....<+...G.... pD.....G.... p.:.p...[Q...!.....j..... G.0....ga.8\....p.@,A.r.)..e.An.F.....j.....}.....5q..E.S.M.....WC.8..U.0az....N\|.GWB./.....20~..?.3.....N.....\_....ka.nh\| ..MS...9<...J@.:..!fF.\..m.W..!@....t.7..c=LZ..p...hz.:?N/.0.i/.....ck}..X...c3><..m.*..w..3..-.0.m.%p[..0c...;...+..Z.....jhn....{.w...m....\..0...=e.....:.h...]....O.qt.pS....P..L..0.%.U...h..q2sy.G...:.....$....j.].*.+....f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\unnamed[9].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 262x262, frames 3
Category:	downloaded
Size (bytes):	3232
Entropy (8bit):	7.439499386210749
Encrypted:	false
SSDEEP:	48:CQ9nBl8yOqm6PnlyvgKofuihd0RUcbp2g2MDiqvHFP4IBwgQLqVRbuvy9Itju99h:5pDU6PlyIKoWMIx2uie4ojIqXu69J7h
MD5:	5E3DCB91F7479C4DDDD97A70EA737F93
SHA1:	44BB1782FB7C9D19D5722ED8A659A2B67BE02535
SHA-256:	C20147F07ACD80954520F926614960F6CB29B70AF9432102546809668ABC1CD3
SHA-512:	E58769D5704875A7A3B36C81DA03AD7F2C6200B9A2164CBC23DE88EA898951C1ECED2E5AF9E34112694D78BF6581E7D52A7DCC0F8A950E6B3F429903D72C12A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/q6qMZrrMLLqdCto6icsSvaZVetRFFAcTw2YjAAQnA_M5eEyQhBomDBuEYo8h0utfCNGBhKfBwuoP07UqZFWTwK08Rty2Y462jYP-tw=w262-l90-sg-rj
Preview:	......JFIF.....".....E.....!.1A.."Qaq..2Rr... ..#3b...4Bs.....$Cc.....?.....R0.\\.....d.&.H...2..2.....,,d.....b..@.2.....2..fn d..d..d.. .....@L.....e37".....X.\\..W."....$.D..e.w..v.....;.G...e-.....5.L...:..O..=..F^..e.....~+..=...i..X...q...BKo/F^.....|..8.Kt...O7%.Jf...O%....2...{..p.J5#./.K._S.>n.71p&.\\.....=...n.....=..e~.|5<U..m.....k.e.j.%H.d]..C."....3..R.\..kN....*L....+..MSOer.....BMF..n.....\.j..{....g.Fo|.....|.....u..e....s._ll.....#F.....x....QL..5.K.8..>..s. j...."/nS..G.c..q...[r...?+.[j....#.....i...W..Wvg....BXp%M.FF..a.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\2038943760-postmessagerelay[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	9875
Entropy (8bit):	5.579490775730224
Encrypted:	false
SSDEEP:	192:1TyJwMuoQ7zm1EeeFWLuivp3YilJ1MfWXxPKPo5ulhIEkvwt:1TowMuoQ7zm1gC3ZlJvBiPKWaot
MD5:	7800A27DF1F2A78F5B6D6AAA9644802C
SHA1:	FE6DC96D677C9EEB610DB2B16B86B7C1C63C249C
SHA-256:	5BD9CA2F57B6C388332DD095D8C9BE87DC71C2E1B78B843515AE758FE05A1223
SHA-512:	EEC57D75897B295CD37E3588BA3ED4EEB2957B6F339979E9958DE7AA88B7ACAACF04E16B865F075C6307AC7EE0BBA683A44C9074624A8650A59AC7D4586055(8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/accounts/o/2038943760-postmessagerelay.js
Preview:	/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var m=this||self,w=function(a,b){a=a.split(".");var c=m;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var e;a.length&&(e=a.shift());)a.length||void 0===b?c=c[e]&&c[e]!==Object.prototype[e]?c[e]:c[e]={}:c[e]=b},x=function(a,b){fu nction c(){}c.prototype=b.prototype;a.A=b.prototype;a.prototype=new c;a.prototype.constructor=a;a.v=function(e,d,h){for(var l=Array(arguments.length-2),n=2;n<ar guments.length;n++)l[n-2]=arguments[n];return b.prototype[d].apply(e,l)}};function y(a){if(Error.captureStackTrace)Error.captureStackTrace(this,y);else{var b=Error().stac k;b&&(this.stack=b)}a&&(this.message=String(a))}x(y,Error);y.prototype.name="CustomError";var z=function(a,b){a=a.split("%s");for(var c="",e=a.length-1,d=0;d<e; d++)c+=a[d]+(d<b.length?b[d]:"%s");y.call(this,c+a[e])};x(z,y);z.prototype.name="AssertionError";var B=function(a,b,c){if(!a){var e="Assertion failed";if(b){e+=": "+b;var

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4UaGrENHsxJlGDuGo1OIlI3K[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 82300, version 1.1
Category:	downloaded
Size (bytes):	82300
Entropy (8bit):	**7.993868899885629**
Encrypted:	**true**
SSDEEP:	1536:nG4K6l+BuoexS2Sv1TEThLUb2AQ3i/U7sCV30lbRS5NA7UFloGIN46:nGxkBxS2YEThIb2v3iIsCV2H7UFl9Z6
MD5:	78F084CD32CB85327C04655BD20D7135
SHA1:	BA8CD3AC9F80EC121C20A4423987BE8B3A706D55
SHA-256:	DC662D2DD599D356BAF970A6AE9AACB4477FCC84E39159FE4B49ED82D2ACB4B7
SHA-512:	06CF2D6AD91ABF5B8DF8AC54D4345E6560A43C59D013B2170454BA00FBF255B1D5060BD89F34640E0DFFBCB6323B7C4A94AEBEE9A4125286997E17E3606BB5(0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UaGrENHsxJlGDuGo1OIlI3K.woff
Preview:	wOFF.....A|.....GDEF.....<e.e.GPOS...D..;.....Qr.'GSUB..=\...<..#X....OS/2..O....U...`kr[.cmap..O.....@Y..Dcvt ..V....y.....fpgm..V.....uo..gasp..^ H.....glyf..^T...a..x..head.....6...6..'.hhea..... ...$.0..hmtx.....H.v4loca.."....&O..^maxp..+.... ... .name..+....e...m...+post...D.....*N....prep..@....p..... ..x.U..F.q... s.G.....jiZ ...DCB...H...BO....ao.....{.^.....lb>..zCz.....O...i..k.....$9-S.m.$..S<. .x.|...}..e.V2Z..g4\p..{.5.....~[}_.X}^.#.`..S..U.T.....;... {....l...._../.....?."-=x..Y.p...}.z.$... ....f4.*.w..9.J.033...'.0.p.....^.....:.T...AS.;...^.l.m...@..jD;...h{.C...'....9c.. ...a..(.7v(BY.1Q.rT.{.{'T.....34A.B?.gE..B.*Q5...C0....c...Y?.....+~\...IR`.'.4)B...(.R....7..0...w.>>. ..O.....w.x^Xi.r..:...p8R#..."....t-..p[.].-..v..E.K..5..=y8.. ..9...p._.{.;.3a..,c...6..mw;..5|...5..78.S.&.)v.gr6.p..s!.q1.p9..j.....:Yg.....I.`.m.=c..{...9*..Ud..d.Rp|....LI.'\)Y%Y...].O..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4UabrENHsxJlGDuGo1OIlLU94YtzCwA[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26412, version 1.1
Category:	downloaded
Size (bytes):	26412
Entropy (8bit):	7.982191465892414
Encrypted:	false
SSDEEP:	768:BXFxTA19K8CdHMT6KHQO8LWhHCWN1ekhzLS:9f29ZYMTwO8qh1nm
MD5:	142CAD8531B3C073B7A3CA9C5D6A1422
SHA1:	A33B906ECF28D62EFE4941521FDA567C2B417E4E
SHA-256:	F8F2046A2847F22383616CF8A53620E6CECDD29CF2B6044A72688C11370B2FF8
SHA-512:	ED9C3EEBE1807447529B7E45B4ACE3F0890C45695BA04CCCB8A83C3063C033B4B52FA62B0621C06EA781BBEA20BC004E83D82C42F04BB68FD6314945339DF2 A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff
Preview:	wOFF.....g,.....GDEF.....q.....GPOS.....%..+...RGSUB.....y.....m.OS/2.....U...`i`..cmap.....~n...cvt .....fpgm...@.....uo..gasp..... ..glyf.....>F..m>Q..head..[\...6...6..'.hhea..[.... ...$...3hmtx..[.....<'3loca..^l...{...._.{.maxp..`.... ... ....name..a.....V..4.post..a.....i]\prep..et.....^....x.D...Q...3..IX=D.@ @....@....."...}.....`.%.....x.....umW...g.WwO.....J..^?.Jci^N{.Nr..Jw@.n(.....t4....g...x.....6.E..8.....affff.0.B..&.L...B.Nzy..n.T.t~w&..%[.dYzzz.Oe" ..lE.....m..7[s}...[l..)..)... (H.A.@q.57..S.@.._..].*.j.-^N.R...'...]v.0..2n.6...~....X..xN.DN.T..b..*Q5.E.).,Ql.....M....6.P."..\|..*.tl5.....t..r.(...{M..T}..@.kbNP.l*.9-...=E.U'.{.....p\|.t..qJE.9...'...*...z...L./.....r nXQ.6.\|.....n.V.....K.?.G...<..<..Q.....C..K(s.PR.x\(..P@.P..z.DL.1.$*../.8A.8Q.r.Pr[e.Rt+~.}9.)E.'.U..z.G..G..OH/H...L.../..{S...EP.%.....o.....uN...'.}%..9.F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\4UabrENHsxJlGDuGo1OIlLU94bt3[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 82716, version 1.1
Category:	downloaded
Size (bytes):	82716
Entropy (8bit):	**7.993713530548**
Encrypted:	**true**
SSDEEP:	1536:hijC7nihKxAiyoVOuS+VhAhFO22tkZWEleJ/oItoGIN9:gIgKThK+XPkZ7It9k
MD5:	6108B8DFDDDD5F9D46A75347D4D803BE
SHA1:	E6A27CF8C983E886B7FBFE3BC8D51E7C797D2F89
SHA-256:	F811A1FE35E8D890E072467515DF338DB4CE562E1CEFDCAC5CB8F76E505AE89B
SHA-512:	52D04EFDC8F3A9F52F7227CEA3E5E5808C3B8E1C12D9D98EB5BABFE2E7953162FA2E13639CD850D595B15214357FB42340B4494E300EC9E4D25C00A2F577BDE7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/googlesans/v14/4UabrENHsxJlGDuGo1OIlLU94bt3.woff
Preview:	wOFF.....C.....GDEF.....XkvkWGPOS...X..;.....GSUB..=....<..#X....OS/2..P8...U...`k.\.cmap..P.....@Y..Dcvt ..V.....fpgm..W8.....uo..gasp.._.....glyf.._.....u.ua.8head.....6...6..'.hhea...T... ...$....hmtx...t.....H.Nq(loca..$.....&..8.maxp..-.... ... ....name..-,...m.....H.post../.....*N....prep..Ad.....^....x.EO%T@.....{...i..4.4\...t.z...7..mgi....`RR.H.....9...C.I.....)..._.h.^C.g...|@,.r.....8d.q.....lp.x....p\Lc.sX`...}.p...T...H.DW..N...Q.x.....B..H..zI....A..&%P+.R8Vf..UVE]mu.k`O..).9.57h....1tx..Y.t.G...kv%.....1.....0..%v....h..!l.7....1..N.....f.~US]..F... ..\5...>.X.=.wC....!g..>.O.p0.#...a..(m0w(BY.9Q.rT...qh'T.}.a..`34A..)gEAN.....p.....|.C.....k>....R....i@T.b.QM.ZYu..7..r...;...:~.a....N<!.4B..I....8...P.....3.w-.tw{.....r3...>.I.....<..q ....p".....2a..-c...v...P;..5..i.....Y...8G..8....K....+..k...(..:XG.d...{..gm.M.I...h....?.R..!..YH.q..K

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Abobe_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	314601
Entropy (8bit):	5.554452464123459
Encrypted:	false
SSDEEP:	6144:Qth+qx9thCdBEu5E8KJK4Q+MRAdlTByYunleg9zM39pkV:aOX9E84Q+MRAnYegNW9pkV
MD5:	F335602886273EAAEDFCF7FDA09205A5
SHA1:	431E043485C43B6F8319B02B314BB06B3007FDA9
SHA-256:	104F50B16888AA6516511BA1C857251A670DCE68468F22B0843D2BD8E8F443CF
SHA-512:	F56CDC4FE916918F25417CC949EC00CF65716F1AAAE49AABDD0B080CB8850ADF4C0111F0024153DC3ED54CBFCD490D988F722404C2497130848ADA94230C89
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kstatic.googleusercontent.com/files/667fa0a2a1aa16fb1a877a3b3f2725cc03b156c36f458422c4279744e3cdd67fa75470b541ba1018ca6628e1126131a49c24e918f919a4e4ee10923f1d48ca8c
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="200px" height="102px" viewBox="0 0 200 102" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 64 (93537) - https://sketch.com -->. <title>Group 98</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01" transform="translate(-80.000000, -5938.000000)">. <g id="09_Drive-integrates" transform="translate(80.000000, 5668.000000)">. <g id="Group-27" transform="translate(0.000000, 100.000000)">. <g id="Group-22" transform="translate(0.000000, 170.000000)">. <g id="Group-71">. <g id="Group-70">. <g id="Group-98">. <rect id="Rectangle" fill="#FFFFFF" x="0" y="0" width="200" height="102"></rect>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Atlassian_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	54219
Entropy (8bit):	6.021136570555999
Encrypted:	false
SSDEEP:	1536:gGPmBjUE88WUClBXU+An8uOal2Hb1KdLqT:gcOb88+BXOVT2HbgdLqT
MD5:	47584606A5C47F8D3FC084ECE3D87506
SHA1:	24E860209289FAB401C23BD28DD80F0A3B49338F
SHA-256:	85D1D8AEDF16A12488385249EB02898BE10546AA3008E31BA7C576209000FFD7
SHA-512:	4300FED05FA886019B1B4A5D06FD94A6A96F6B079030E21EF6A5D3C360C895830FBAA91B3766E5E326F6CB587B09E7931DD4E05EA72247B6C1FCD77142D4782
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kstatic.googleusercontent.com/files/686902a5a73584f00448ecb41b20642e6a67bb8a30856e62f31cec5a5658f0c230d7e4d985e6bb735be91b7bc43026e1dfc5a17abf22f20aebbfe39527b620c7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Atlassian_01[1].svg	
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="200px" height="102px" viewBox="0 0 200 102" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 64 (93537) - https://sketch.com -->. <title>Group 99</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01" transform="translate(-296.000000, -5938.000000)">. <g id="09_Drive-integrates" transform="translate(80.000000, 5668.000000)">. <g id="Group-27" transform="translate(0.000000, 100.000000)">. <g id="Group-22" transform="translate(0.000000, 170.000000)">. <g id="Group-71">. <g id="Group-70">. <g id="Group-99" transform="translate(216.000000, 0.000000)">. <rect id="Rectangle" fill="#FFFFFF" x="0" y=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Autodesk_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	40968
Entropy (8bit):	6.054861913701004
Encrypted:	false
SSDEEP:	768:Nv9oaeJleebucIR4cpTXOJzIA9mtMXn2e57HatQGWyfFgI4cEP:Z9C8eitzOGqn2ehZkdFEP
MD5:	45151E115D6A562D0F38248BA211D7FC
SHA1:	FA628332CDB842C012E7E907B9294540FA04D05F
SHA-256:	78C45818F2E8AED0304D9055A1F0CBFECC76A0394978122F01B6F5DDBFCC4544
SHA-512:	CCC1530D0046835AE6CABDBA7544E7275719A653FBCF8520796D703A13E1AC13269123E3BAC0B55F445EE65A27A0C9C5283D7E453D97CCB1358ADD13FF5038
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://kstatic.googleusercontent.com/files/502e1e2bcf1d734194ada6a0404463ea623c3c5eb170ce7ca5a8b95febfce2be839280662ef8b350a6605e79e86a6254e1d9160a3 a1de29d2bd0b0506f46194
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="200px" height="102px" viewBox="0 0 200 102" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 64 (93537) - https://sketch.com -->. <title>Group 100</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01" transform="translate(-512.000000, -5938.000000)">. <g id="09_Drive-integrates" transform="translate(80.000000, 5668.000000)">. <g id="Group-27" transform="translate(0.000000, 100.000000)">. <g id="Group-22" transform="translate(0.000000, 170.000000)">. <g id="Group-71">. <g id="Group-70">. <g id="Group-100" transform="translate(432.000000, 0.000000)">. <rect id="Rectangle" fill="#FFFFFF" x="0"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Docusign_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	29934
Entropy (8bit):	6.050271421439555
Encrypted:	false
SSDEEP:	384:MNo/llQ77AoHu/AWinFm8rpXo5p0Tb2AoHZf2LGTTGszGsQmUwpoNiS:FllQ77AoHuIWoFt5u0n2Ao0QlzflUsod
MD5:	DE2B1A746789EAEC33C0BDC739E73EBE
SHA1:	E9BDAEF24334534465BCF684D7CCA627A8E48830
SHA-256:	9ED9D7372A34415EDCBD4DAAC357A093D12CB0DDE40706E8C86B2BF0218BC58D
SHA-512:	71433AAA9B5DE49AC6959795A46E020D9A011EE4068A15394563D9016BA8DAA2FD2BBC76499782E958F707652E1CC0E884DE716CF76512FC3DAC929A01420D1
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://kstatic.googleusercontent.com/files/7ab7238bb2adf87b4b0a5a4b51d04a8c00269e10761a786f6d025ad7f5f79c56d83a71251e9b8c650de502ad431cc3c2a5d605615 5e6f41a3a6ff5d57247649
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg width="200px" height="102px" viewBox="0 0 200 102" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 64 (93537) - https://sketch.com -->. <title>Group 101</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01" transform="translate(-728.000000, -5938.000000)">. <g id="09_Drive-integrates" transform="translate(80.000000, 5668.000000)">. <g id="Group-27" transform="translate(0.000000, 100.000000)">. <g id="Group-22" transform="translate(0.000000, 170.000000)">. <g id="Group-71">. <g id="Group-70">. <g id="Group-101" transform="translate(648.000000, 0.000000)">. <rect id="Rectangle" fill="#FFFFFF" x="0"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Drive_Product_Icon[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1283
Entropy (8bit):	4.592944231809672
Encrypted:	false
SSDEEP:	24:t/x/DuqUHchUt1kB0K6ONUkz/bR6d3HdNLUO/WW0Rpl3Xu6oIQoee9Xrb:H/M1BD4QNWx1XbVXX
MD5:	2F60F76F3DC382D0C099E8B7FB306CFB
SHA1:	ED7D8BA7A0F6B1D18E62E7977F846C5AE7CF80A1
SHA-256:	B4219E47BE77B053E4BB287EB2575CB56F950D92FFF53C9894FA618607D43A6B
SHA-512:	3EFF22A01B8547BA00A6F0CF7A7E399946F0297EFC4BD0392F6A57C1CB76BEE00BDEA5CB910C645F4A7F34E06C4E158A6C31B8747E91E9B12E1AAF7423E7289 D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Drive_Product_Icon[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http:// https://kstatic.googleusercontent.com/files/f4b4fbcc6119576da7ab3f68270196009fc1b16f1927910842d793c385115593b6dd5fbe9a1e21fe64f3cbbc509c3a02c95ebc9635f76c355282482986f1fe7d
Preview:	<svg width="94" height="94" viewBox="0 0 94 94" fill="none" xmlns="http://www.w3.org/2000/svg">.<rect width="94" height="94" fill="white"/>.<path d="M10.7219 73.2906L14.4917 79.8021C15.275 81.1729 16.401 82.25 17.7229 83.0333L31.1865 59.7292H4.25937C4.25937 61.2469 4.65104 62.7646 5.43437 64.1354L10.7219 73.2906Z" fill="#0066DA"/>.<path d="M47 32.3125L33.5365 9.00833C32.2146 9.79166 31.0885 10.8687 30.3052 12.2396L5.43437 55.3229C4.65104 56.6938 4.25937 58.2115 4.25937 59.7292H31.1865L47 32.3125Z" fill="#00AC47"/>.<path d="M47 32.3125L60.4635 9.00833C59.1416 8.22499 57.6239 7.83333 56.0573 7.83333H37.9427C36.376 7.83333 34.8583 8.27395 33.5364 9.00833L47 32.3125Z" fill="#00832D"/>.<path d="M62.8135 59.7292H31.1864L17.7229 83.0333C19.0448 83.8167 20.5625 84.2083 22.1292 84.2083H71.8708C73.4375 84.2083 74.9552 83.7677 76.2771 83.0333L62.8135 59.7292Z" fill="#2684FC"/>.<path d="M76.2771 83.0333C77.5992 82.25 78.725 81.1729 79.5083 79.8021L81.075 77.1094L88.5656 64.1354C89.3489 62.7646 89.7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\KFOkCnqEu92Fr1MmgVxIIzQ[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 19936, version 1.1
Category:	downloaded
Size (bytes):	19936
Entropy (8bit):	7.969635209849544
Encrypted:	false
SSDEEP:	384:mvNCb8Eb+tS9nAIRMeC4J4h4Il7xtUOTCBGt+GXn/TUnOPgdGRhBg9r:Y4zbwTiMedJNIhkGbXn/TUnS+2hS9r
MD5:	E9DBBE8A693DD275C16D32FEB101F1C1
SHA1:	B99D87E2F031FB4E6986A747E36679CB9BC6BD01
SHA-256:	48433679240732ED1A9B98E195A75785607795037757E3571FF91878A20A93B2
SHA-512:	D1403EF7D11C1BA08F1AE58B96579F175F8DD6A99045B1E8DB51999FB6060E0794CFDE16BFE4F73155339375AB126269BC3A835CC6788EA4C1516012B1465E75
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOkCnqEu92Fr1MmgVxIIzQ.woff
Preview:	wOFF.....M.....GDEF.....G...d....GPOS.....hGSUB.....7b..OS/2.....R...`s.#.cmap.....L....cvt .....H...H.2..fpgm.....3...._...gasp...0.....glyf...<..;...n..e..hdmx..G<...i.....head..G....6...6.G..hhea..G.....$...`hmtx..H....M.....Wd^loca..JP.....maxp..L,... ... .name..LL.....x..9.post..M ..... .m.dprep..M4.....+6.x...1..P.....PB..U.=l.@..B)..w.....Y.e.u.m.C.s...x.h.~R....R.....2.x.....[....#N..m.m.m.mfm....SP..NuM..9]..=.U..!...[.....w...|.....^p....H.....;...).....;..EoDo..E.E.D...`.0.GG.aA.H.V.Mx\xA...../..d3.Eb_.J...R.^v.....\^ob.}.z..k.x).v$f$..O)+.2..*....y}6`C6b.6cs...l.....!.....<..|.|..|..|.|....o....l%.4.L.Sl.&C.6..!`...{...c..\.J.(.2.C....V.A..?.M<nG.....v..m.;..R.C..aj.H...=..{.>.:.....}i_Y.....:....o.&k..KY.2..6k....i]..{..p}../.....VO3.o].fJ....R-TZ..;...RN..&V...C...3.?.....&..z.s&.D....r,.I...t.R..a$k..Mm..Y.U...+b.%kQ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\L4FCQBHD.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	820599
Entropy (8bit):	5.532386793624594
Encrypted:	false
SSDEEP:	24576:cQJtssMiipcx+VoAncFE0BBZHJrUvaf0zlV0U+AqVCU:9tssMiipcx+VoAncFE0BBZHJrUvzlV0v
MD5:	1414C1233406A5405379C7E8068F2214
SHA1:	5DD98C91FF1EBD7BCA5526D7D518B990869225A8
SHA-256:	3418125D467C1DBFAAE672F63DDF4DF4CE061865ECCF64C74820D6EAF5F55859
SHA-512:	8B1FAB4BA730DDAF3E9D915D3D7CC14620D9A1A335BD293C0ADA8C44CAB6426C7E0F247B31FC65BA6D8518C855E02035E3BD64A55FB5F86389F2B557429D5A6C
Malicious:	false
Reputation:	low
Preview:	this._D=this._D||{};(function(_){var window=this;.try{._.Ihf=function(a){return"cp"==a||"catd"==a||"clid"==a||"csc"==a||"iid"==a};_.t("sy1di");.._.w();..}catch(e){_._DumpException(e)}.try{._.t("sy1cw");./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/._.RY=function(a,b){_.Ci.call(this);this.hc=a;a=_.Mh(this.hc)?this.hc:this.hc?this.hc.body:null;this.ha=!!a&&_.ds(a);this.H=_.$d(this.hc,_.ch?"DOMMouseScroll":"mousewheel",this,b)};_.O(_.RY,_.Ci);._.RY.prototype.handleEvent=function(a){var b=0,c=0,d=a.Me;"mousewheel"==d.type?(a=r8e(-d.wheelDelta),void 0!==d.wheelDeltaX?(b=r8e(-d.wheelDeltaX),c=r8e(-d.wheelDeltaY)):c=a):(a=d.detail,100<a?a=3:-100>a&&(a=-3),void 0!==d.axis&&d.axis===d.HORIZONTAL_AXIS?b=a:c=a);"number"===typeof this.V&&(b=_.ih(b,-this.V,this.V));"number"===typeof this.W&&(c=_.ih(c,-this.W,this.W));this.ha&&(b=-b);b=new _.s8e(a,d,b,c);this.dispatchEvent(b)};var r8e=function(a){return _.dh&&(_.eh||_.Iha)&&0!=a%40?a:a/40};._.RY.prototype.Ya=fun

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Salesforce_01[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	19887
Entropy (8bit):	4.279635539953778
Encrypted:	false
SSDEEP:	384:aRCs/xKqHHy05fMUlmlK+ebwlyJf5mIHcccKRvMd:ab/XHlnlm/e46f5B5S
MD5:	A8E9E4B41715FF464A8AE7F15D01248A
SHA1:	C74DA4B29BAAC9A21EB8EB507E96292E58F95454
SHA-256:	E3812DE195D2E175E4DFBB47E674A1E3C68FC3792E785C40BA620E4F1102A02D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Salesforce_01[1].svg	
SHA-512:	D21DDD4D4D3524A153601699A4D151E0FF37B8C51B231A65A3E0057E2FA98A8871939113711CB6C714139D31121E7BFD4F54C3ABF37F5E0105F7D61ED7D9542A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://kstatic.googleusercontent.com/files/29a8b6c367123fbc5365cd156b12d35427fa7640e6af546d59af38dff162fe82ee529cdcb82ea31f5a4bb8687a492966528c0222706e5017d0d0ec4b7324bd31
Preview:	<?xml version="1.0" encoding="UTF-8"?><svg width="200px" height="102px" viewBox="0 0 200 102" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. Generator: Sketch 64 (93537) - https://sketch.com -->. <title>Group 102</title>. <desc>Created with Sketch.</desc>. <g id="Page-1" stroke="none" stroke-width="1" fill="none" fill-rule="evenodd">. <g id="Google_Drive_Homepage_01" transform="translate(-944.000000, -5938.000000)">. <g id="09_Drive-integrates" transform="translate(80.000000, 5668.000000)">. <g id="Group-27" transform="translate(0.000000, 100.000000)">. <g id="Group-22" transform="translate(0.000000, 170.000000)">. <g id="Group-71">. <g id="Group-70">. <g id="Group-102" transform="translate(864.000000, 0.000000)">. <rect id="Rectangle" fill="#FFFFFF" x="0"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\Screenshot (163)[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 200 x 190, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	34893
Entropy (8bit):	7.975138174092085
Encrypted:	false
SSDEEP:	768:tQY2ADmgnH9MWkXd4CcaW25Fq8hkQQwF7baIdFP7JnH4vV3uG:txm8H9UN4iHq8b7baUPFnYv3
MD5:	57F54528A679C120E4772A65E7597351
SHA1:	8E7E319A0A790D6EB1E1437EF221675D1417E539
SHA-256:	C5253DCEB20DF4383E5D151E0DD2538884E51F4F192415397C62CE6B6F42E0FF
SHA-512:	88EE4304D605D48982E6E61050492274F9BD32A62756A0321CDF2C9C78C3D2F2857F6DF53FC1B7CA0DC0F8DA78BADE9C19AF9F28C6DA6E25BC4B25B3A3B2C3EE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh3.googleusercontent.com/u/0/d/1FaBL55V0pTrlZhpmN344c0GD4ofnsTf7=w200-h190-p-k-nu-iv4
Preview:	.PNG.....IHDR.....A.....sBIT.....O... .IDATx..y.&.u.v...o{..1....`....p.h.(.%S.C.fTJ%.J.%.8.(.H...R.c.*..J,V.m..P.l....$H..2.f{...v.....q.....$@..;d...u...=.,.s.i..?...9g/..39.^c...s.....B...c-".Z....." :.....li....Zk.R..c.D`.E.9DD.t.I..A.#....&...9:[.....n.UKz...s.V@.z..s.]..K_{..f...4...K:.;S.....n.\.....|{.v..O....Z.R...../X.@+..sn..K....=x.....H../_...~....:.y.^.y!..k....s.Z..|.....l.....?..upZ..s..G..7.t.(r...\.80?...P..py.An.....?2.._.....~z}.....|._>.6p..z..s.....O=.....g.....pGo...../].....4.;ys...|..7..&c{..:.. ...~.;.?....|q..[.....K.sO.....3/.q..1../.:z...^8u8>.!._x~nv.....8..... .../_D.N{9.....0...O..._j..';.*.....o../..W...C+..$..<.J....9|py.2.....Z.c.N..$.(.,.(P....9.....o.A...nl....S.z..:m.....^K.;..f=3..s..3.d....1F.g.C?..w...li..H+B.`...."t.(..`Ha.*..D..."'.-f.D..D,...Ta.. b./.{....P~....z.H.a...T}E.....j...T.....4..V..b.....@.

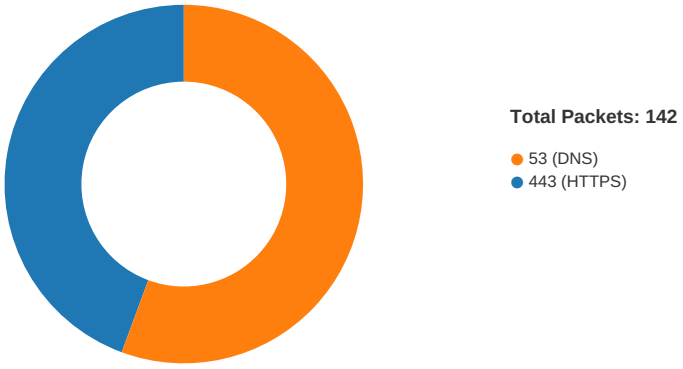
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\ServiceLogin[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	1583394
Entropy (8bit):	5.8295929702344536
Encrypted:	false
SSDEEP:	49152:vob2PslOpugyZrdevDG8EyMze3KYhjRB2OsOm+PEtqfvSzL6Z9Y9EhdBjCCaNsae:i2Ps2b
MD5:	AA3CC96C071E9B816D4346E92868A6CC
SHA1:	70B059CC3A2A9633E9AECED13D8F054A3441D89D
SHA-256:	B35AED490CF64CA396EFD1CCC18F644FB97F3FC7D78B2260BB56C7166B09C899
SHA-512:	AE44EAD2DBB4E8C400D56799FC45B472D393EBE31ABBE3484B2E7373F0D2F178AEF6D7C1796DA20106E524D571D26C3F8E47F5C69D14E907776B9A8FC43A991
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en-GB" dir="ltr"><head><base href="https://accounts.google.com/"><script data-id="_gd" nonce="vbjBJskNHZxA82DnqzD26Q">window.WIZ_global_data = {"Mo6CHc":4360839914192013 60,"OewCAd":"%.@.\"xsrf\",null,[\"\"]\n,\"AFoagUUzaU-p3Tu9ITiiOTa0sULpzmV8TA:1614048716567\"]\n","Qzxixc":"S1124579295:1614048716548779","thykhd":"AKH95etGu81BBcZYnZxybdYKeAHj8BML8Y-s-B5ppy5FzeMN1U3xwXgXx10EQmFVBczgdClvG8lwIQ-y118ZiaMSL1XeHMTwKPXmvx_tPCqEBZOJ9pbV2Ow\u003d","w2btAe":"%.@.null,null,\"\",false,null,null,true,false]\n"};</script><meta charset="utf-8"/><meta http-equiv="X-UA-Compatible" content="IE=edge"/><link rel="shortcut icon" href="//www.google.com/favicon.ico"/><noscript><meta http-equiv="refresh" content="0; url=https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fdrive.google.com%2Fdrive%2Ffolders%2F1YP_-yqhS3_exi6Kfo8Gq82qIyMlJy6_V&rip=1&nojavascript=1&service=writely&hl=en-GB"><style nonce="vbjBJskNHZxA82DnqzD26Q">body{opacity:0;}</style></nosc

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 03:51:26.606715918 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.606823921 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.607038021 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.607168913 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.607351065 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.608177900 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.655272961 CET	443	49745	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.655352116 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.655519962 CET	443	49746	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.655592918 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.657928944 CET	443	49743	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.657978058 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.658020020 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.658108950 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.658602953 CET	443	49747	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.658689022 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.662508965 CET	443	49748	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.662564039 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.664871931 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.664968014 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.665118933 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.665313005 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.665472984 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.666215897 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.716517925 CET	443	49745	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.716903925 CET	443	49746	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.719177961 CET	443	49743	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.719225883 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.719893932 CET	443	49747	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.720331907 CET	443	49748	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.723495007 CET	443	49745	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.723557949 CET	443	49745	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.723575115 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.723613977 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.723704100 CET	443	49745	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.723757029 CET	443	49745	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.723758936 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.723809004 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.724010944 CET	443	49746	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.724067926 CET	443	49746	142.250.186.33	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 03:51:26.724072933 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.724119902 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.724132061 CET	443	49746	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.724193096 CET	443	49746	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.724195957 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.724245071 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.726548910 CET	443	49743	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726622105 CET	443	49743	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726641893 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.726687908 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.726716042 CET	443	49743	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726761103 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.726782084 CET	443	49743	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726828098 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.726850033 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726901054 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726963997 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.726968050 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.726998091 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727003098 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727013111 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727063894 CET	443	49747	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727070093 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727117062 CET	443	49747	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727135897 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727170944 CET	443	49747	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727173090 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727222919 CET	443	49747	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727224112 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727359056 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727421999 CET	443	49748	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727474928 CET	443	49748	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727487087 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727518082 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727551937 CET	443	49748	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727593899 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.727669001 CET	443	49748	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.727708101 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.748707056 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.752633095 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.753215075 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.753437996 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.753606081 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.753774881 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.753932953 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.754096985 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.754254103 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.754416943 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.754570007 CET	49744	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.754626989 CET	49748	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.759685993 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.760055065 CET	49747	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.763125896 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.763484955 CET	49743	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.769551992 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.769925117 CET	49745	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.770728111 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.771161079 CET	49746	443	192.168.2.4	142.250.186.33
Feb 23, 2021 03:51:26.800467014 CET	443	49744	142.250.186.33	192.168.2.4
Feb 23, 2021 03:51:26.800549030 CET	49744	443	192.168.2.4	142.250.186.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 03:51:17.285401106 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:17.334283113 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:17.378963947 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:17.436141014 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:17.688611984 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:17.740601063 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:17.912945986 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:17.970114946 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:19.411355019 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:19.473503113 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:20.293723106 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:20.345216036 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:21.650438070 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:21.710721970 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:22.836549997 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:22.888436079 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:23.931550026 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:23.980925083 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:24.340193987 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:24.399233103 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:24.793495893 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:24.845544100 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:25.464528084 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:25.532991886 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:26.087349892 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:26.152548075 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:26.206362963 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:26.286283970 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:26.380090952 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:26.405193090 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:26.431926966 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:26.454555035 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:26.472794056 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:26.524667978 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:26.972415924 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:27.040250063 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:28.280774117 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:28.345985889 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:28.842979908 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:28.893484116 CET	53	61721	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:29.335205078 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:29.405575991 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:29.614165068 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:29.696644068 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:30.049866915 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:30.101536989 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:30.264105082 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:30.329375029 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:30.486958027 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:30.552900076 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:31.006968975 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:31.055903912 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:31.197587013 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:31.248941898 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:31.433738947 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:31.490989923 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:32.820108891 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:32.886990070 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:32.951329947 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:33.010334969 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:34.325557947 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:34.374310970 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:35.381828070 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:35.438905954 CET	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 03:51:37.727220058 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:37.776187897 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:38.985830069 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:39.034848928 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:44.069361925 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:44.115386963 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:44.134557009 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:44.175391912 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:45.001718044 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:45.063776970 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:45.906781912 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:45.966636896 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:46.906992912 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:46.955939054 CET	53	60542	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:47.357002974 CET	60689	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:47.408477068 CET	53	60689	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:47.954663038 CET	50904	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:47.961178064 CET	64206	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:48.013896942 CET	53	64206	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:48.021564007 CET	53	50904	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:49.996402025 CET	57525	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:50.074744940 CET	53	57525	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:50.766485929 CET	53814	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:50.837192059 CET	53	53814	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:51.793781996 CET	53418	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:51.858870983 CET	53	53418	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:52.044749975 CET	62833	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:52.106354952 CET	53	62833	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:52.730439901 CET	59260	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:52.795758963 CET	53	59260	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:53.072458982 CET	49944	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:53.139308929 CET	53	49944	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:54.325115919 CET	63300	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:54.380105972 CET	53	63300	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:55.056133032 CET	61449	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:55.106285095 CET	53	61449	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:55.111557961 CET	51275	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:55.176937103 CET	53	51275	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:55.327861071 CET	63300	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:55.392524958 CET	53	63300	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:55.745214939 CET	63492	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:55.813481092 CET	53	63492	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:56.054102898 CET	58945	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:56.059875965 CET	61449	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:56.109591007 CET	53	61449	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:56.123509884 CET	53	58945	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:56.331971884 CET	63300	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:56.395971060 CET	53	63300	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:57.161767006 CET	61449	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:57.210604906 CET	53	61449	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:58.345510006 CET	63300	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:58.397169113 CET	53	63300	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:59.101838112 CET	60779	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:59.165333986 CET	61449	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:59.168941021 CET	53	60779	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:59.216633081 CET	53	61449	8.8.8.8	192.168.2.4
Feb 23, 2021 03:51:59.811845064 CET	64014	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:51:59.889995098 CET	53	64014	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:02.389723063 CET	63300	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:02.450083017 CET	53	63300	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:03.166645050 CET	61449	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:03.217645884 CET	53	61449	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:03.831082106 CET	57091	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:03.896348953 CET	53	57091	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 03:52:18.828351021 CET	55904	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:18.921293020 CET	53	55904	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:19.523349047 CET	52109	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:19.601252079 CET	53	52109	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:20.190637112 CET	54450	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:20.250619888 CET	53	54450	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:20.895776033 CET	49374	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:20.954230070 CET	53	49374	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:21.371581078 CET	50436	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:21.428970098 CET	53	50436	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:21.524070024 CET	62605	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:21.595449924 CET	53	62605	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:21.955425024 CET	54256	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:22.015302896 CET	53	54256	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:22.579678059 CET	52189	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:22.659145117 CET	53	52189	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:23.401751041 CET	56131	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:23.450870037 CET	53	56131	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:24.226901054 CET	62992	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:24.278951883 CET	53	62992	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:24.718157053 CET	54432	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:24.771563053 CET	53	54432	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:27.903549910 CET	57227	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:27.968439102 CET	53	57227	8.8.8.8	192.168.2.4
Feb 23, 2021 03:52:59.323235989 CET	58383	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:52:59.373842001 CET	53	58383	8.8.8.8	192.168.2.4
Feb 23, 2021 03:53:00.528848886 CET	63136	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:53:00.588501930 CET	53	63136	8.8.8.8	192.168.2.4
Feb 23, 2021 03:53:05.849822998 CET	50911	53	192.168.2.4	8.8.8.8
Feb 23, 2021 03:53:05.930305958 CET	53	50911	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 03:51:26.454555035 CET	192.168.2.4	8.8.8.8	0x4ba1	Standard query (0)	drive-thirdparty.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:32.951329947 CET	192.168.2.4	8.8.8.8	0x2a19	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:47.954663038 CET	192.168.2.4	8.8.8.8	0x8a94	Standard query (0)	kstatic.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:51.793781996 CET	192.168.2.4	8.8.8.8	0x473e	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:52.044749975 CET	192.168.2.4	8.8.8.8	0x65e0	Standard query (0)	about.google	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:55.111557961 CET	192.168.2.4	8.8.8.8	0x876e	Standard query (0)	www.blog.google	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:59.101838112 CET	192.168.2.4	8.8.8.8	0x984e	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 03:51:26.524667978 CET	8.8.8.8	192.168.2.4	0x4ba1	No error (0)	drive-thirdparty.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 03:51:26.524667978 CET	8.8.8.8	192.168.2.4	0x4ba1	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:33.010334969 CET	8.8.8.8	192.168.2.4	0x2a19	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 03:51:33.010334969 CET	8.8.8.8	192.168.2.4	0x2a19	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 03:51:48.021564007 CET	8.8.8.8	192.168.2.4	0x8a94	No error (0)	kstatic.googleusercontent.com		35.241.11.240	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:50.074744940 CET	8.8.8.8	192.168.2.4	0x9d8c	No error (0)	pagead46.l.doubleclick.net		216.58.212.130	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:51.858870983 CET	8.8.8.8	192.168.2.4	0x473e	No error (0)	www.google.co.uk		142.250.186.67	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:52.106354952 CET	8.8.8.8	192.168.2.4	0x65e0	No error (0)	about.google		216.239.32.29	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:55.176937103 CET	8.8.8.8	192.168.2.4	0x876e	No error (0)	www.blog.google	ghs-svc-https-sni.ghs-ssl.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 03:51:55.176937103 CET	8.8.8.8	192.168.2.4	0x876e	No error (0)	ghs-svc-https-sni.ghs-ssl.googlehosted.com		216.58.212.179	A (IP address)	IN (0x0001)
Feb 23, 2021 03:51:59.168941021 CET	8.8.8.8	192.168.2.4	0x984e	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 03:51:26.723757029 CET	142.250.186.33	443	192.168.2.4	49745	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:26.724193096 CET	142.250.186.33	443	192.168.2.4	49746	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:26.726782084 CET	142.250.186.33	443	192.168.2.4	49743	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:26.727013111 CET	142.250.186.33	443	192.168.2.4	49744	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:26.727222919 CET	142.250.186.33	443	192.168.2.4	49747	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:26.727669001 CET	142.250.186.33	443	192.168.2.4	49748	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:33.161595106 CET	142.250.186.33	443	192.168.2.4	49779	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:33.161957026 CET	142.250.186.33	443	192.168.2.4	49776	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:33.162055016 CET	142.250.186.33	443	192.168.2.4	49777	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 03:51:33.162180901 CET	142.250.186.33	443	192.168.2.4	49775	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:33.164453983 CET	142.250.186.33	443	192.168.2.4	49778	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:33.245219946 CET	142.250.186.33	443	192.168.2.4	49780	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:48.150202036 CET	35.241.11.240	443	192.168.2.4	49796	CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 17 19:22:26 CET 2020 Tue Nov 17 19:22:26 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Sun May 16 20:22:25 CEST 2021 Sun May 16 20:22:25 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 17 19:22:26 CET 2020	Sun May 16 20:22:25 CEST 2021		
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 03:51:48.168279886 CET	35.241.11.240	443	192.168.2.4	49800	CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 17 19:22:26 CET 2020 Tue Nov 17 19:22:26 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Sun May 16 20:22:25 CEST 2021 Sun May 16 20:22:25 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 17 19:22:26 CET 2020	Sun May 16 20:22:25 CEST 2021		
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:48.168687105 CET	35.241.11.240	443	192.168.2.4	49797	CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 17 19:22:26 CET 2020 Tue Nov 17 19:22:26 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Sun May 16 20:22:25 CEST 2021 Sun May 16 20:22:25 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 17 19:22:26 CET 2020	Sun May 16 20:22:25 CEST 2021		
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:48.170974016 CET	35.241.11.240	443	192.168.2.4	49795	CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 17 19:22:26 CET 2020 Tue Nov 17 19:22:26 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Sun May 16 20:22:25 CEST 2021 Sun May 16 20:22:25 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 17 19:22:26 CET 2020	Sun May 16 20:22:25 CEST 2021		
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 03:51:48.173067093 CET	35.241.11.240	443	192.168.2.4	49799	CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 17 19:22:26 CET 2020 Tue Nov 17 19:22:26 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Sun May 16 20:22:25 CEST 2021 Sun May 16 20:22:25 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 17 19:22:26 CET 2020	Sun May 16 20:22:25 CEST 2021		
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:48.309094906 CET	35.241.11.240	443	192.168.2.4	49798	CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 17 19:22:26 CET 2020 Tue Nov 17 19:22:26 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Sun May 16 20:22:25 CEST 2021 Sun May 16 20:22:25 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=kstatic.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 17 19:22:26 CET 2020	Sun May 16 20:22:25 CEST 2021		
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:50.168692112 CET	216.58.212.130	443	192.168.2.4	49801	CN=*.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:01:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:00:59 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:50.172725916 CET	216.58.212.130	443	192.168.2.4	49802	CN=*.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:01:00 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:00:59 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 03:51:52.198703051 CET	216.239.32.29	443	192.168.2.4	49807	CN=about.google, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:06:25 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:06:24 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:52.199589014 CET	216.239.32.29	443	192.168.2.4	49808	CN=about.google, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:06:25 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:06:24 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:55.277671099 CET	216.58.212.179	443	192.168.2.4	49816	CN=www.blog.google CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GTS CA 1D2, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Wed Jan 13 08:17:44 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 13 09:17:44 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 23, 2021 03:51:55.278256893 CET	216.58.212.179	443	192.168.2.4	49815	CN=www.blog.google CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GTS CA 1D2, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Wed Jan 13 08:17:44 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 13 09:17:44 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=GTS CA 1D2, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

● iexplore.exe
● iexplore.exe

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6968 Parent PID: 800

General

Start time:	03:51:23
Start date:	23/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff682b70000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 7032 Parent PID: 6968

General

Start time:	03:51:24
Start date:	23/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6968 CREDAT:17410 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly