



ID: 339221
Cookbook: browseurl.jbs
Time: 17:37:27
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report https://sites.google.com/view/xfcghv/الصفحة-الرئيسية 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 23
No static file info 23
Network Behavior 23
Network Port Distribution 23
TCP Packets 24
UDP Packets 25
DNS Queries 26
DNS Answers 27
HTTPS Packets 27
Code Manipulations 28
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: iexplore.exe PID: 2592 Parent PID: 792 28
General 28

Copyright null 2021

File Activities 29
Registry Activities 29
Analysis Process: iexplore.exe PID: 3488 Parent PID: 2592 29
General 29
File Activities 29
Registry Activities 29
Disassembly 29

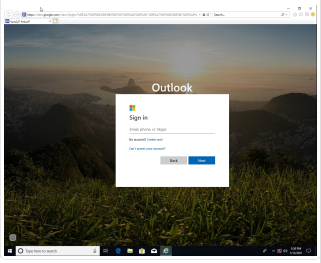
Analysis Report https://sites.google.com/view/xfcghv/ الصفحة-الرئيسية

Overview

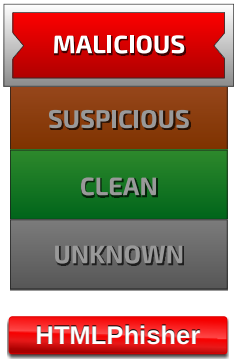
General Information

Sample URL:	http://https://sites.google.com/view/xfcghv/الصفحة-الرئيسية
Analysis ID:	339221

Most interesting Screenshot:



Detection

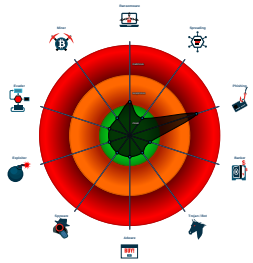


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish_20
- Phishing site detected (based on im…

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 2592 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3488 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2592 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

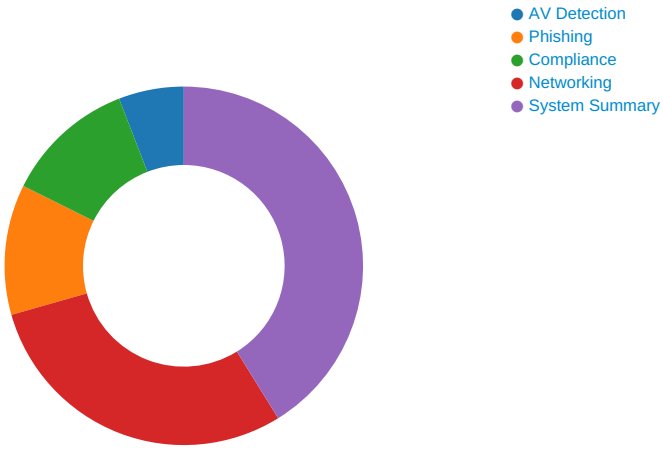
Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\??????-????????[1].htm	JoeSecurity_HtmlPhish_20	Yara detected HtmlPhish_20	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

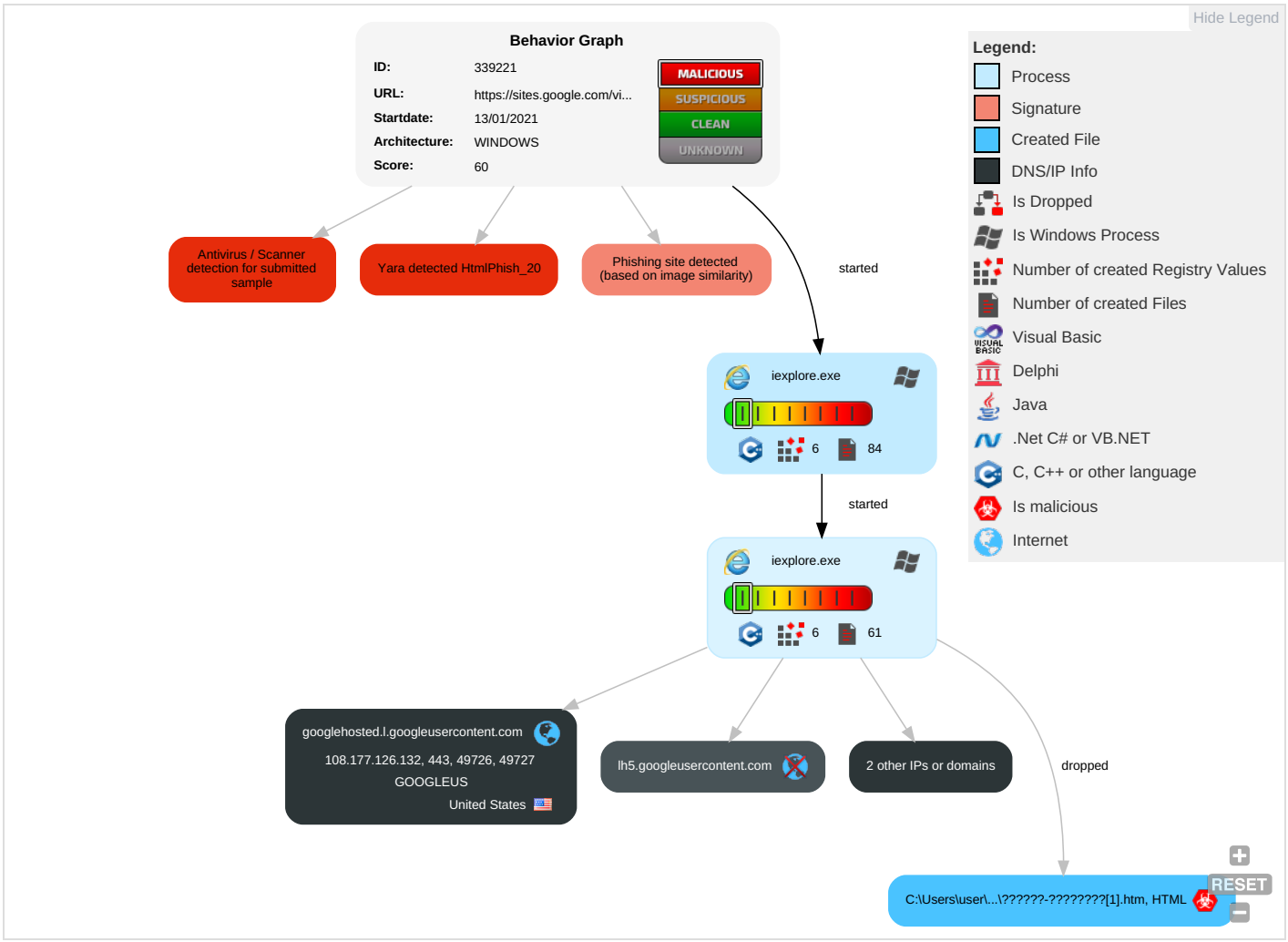
Yara detected HtmlPhish_20

Phishing site detected (based on image similarity)

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	Impac
Valid Accounts	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	Modif Syste Partiti
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	Devic Lockc
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	Delet Devic Data

Behavior Graph

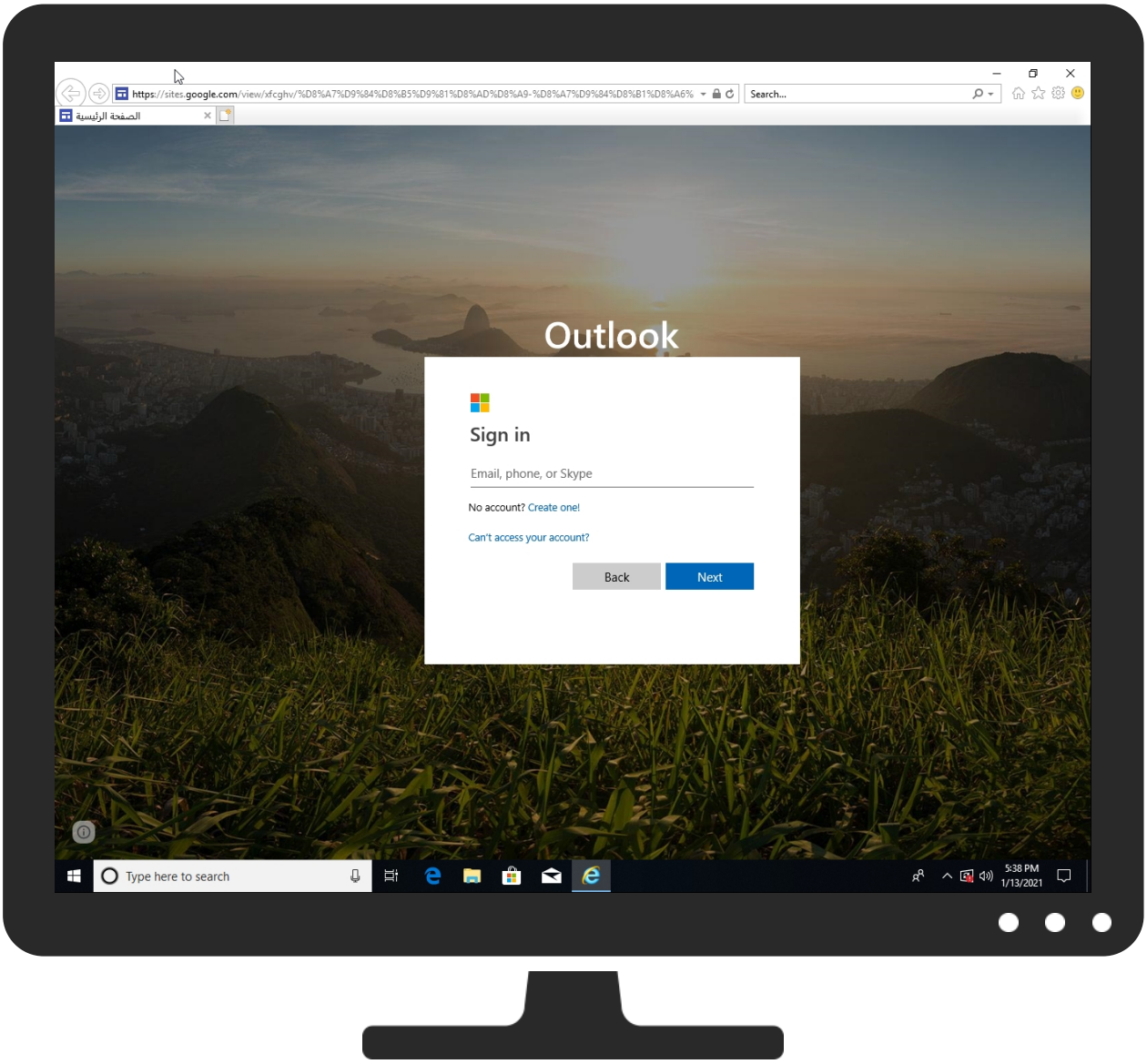


Screenshots

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://sites.google.com/view/xfcghv/%D8%A7%D9%84%D8%B5%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9	0%	Avira URL Cloud	safe	
http://https://sites.google.com/view/xfcghv/%D8%A7%D9%84%D8%B5%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	

Copyright null 2021

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://kelham-businesscentre.com/sm/xxl2.php	0%	Avira URL Cloud	safe	
http://https://kelham-businesscentre.com/sm/xxl2.php">	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

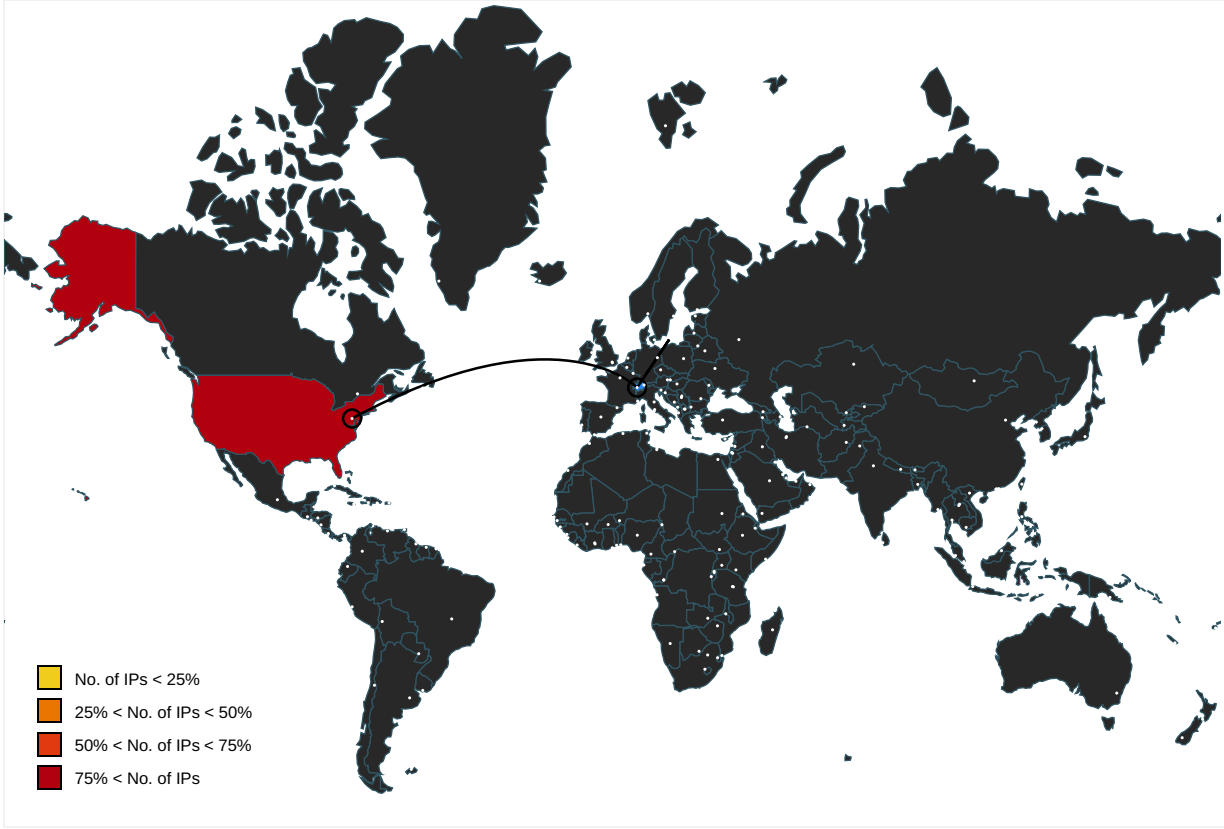
Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	108.177.126.132	true	false		high
lh5.googleusercontent.com	unknown	unknown	false		high
263052666-atari-embeds.googleusercontent.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	m=view[1].js.2.dr	false		high
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://https://code.jquery.com/jquery.min.js"></script>	??????-????????[1].htm.2.dr	false		high
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://https://263052666-atari-embeds.googleusercontent.com/embeds/16cb204cf3a9d4d223a0a3fd8b0eec5d/inner-f	??????-????????[1].htm.2.dr, ~DFD7A6DFAF6BAD27C2.TMP.1.dr	false		high
http://https://developers.googleblog.com/2018/03/discontinuing-support-for-json-rpc-and.html	cb=gapi[1].js.2.dr	false		high
http://https://code.jquery.com/jquery.min.js	~DFD7A6DFAF6BAD27C2.TMP.1.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/	EHPIBSAR.js.2.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high
http://https://kelham-businesscentre.com/sm/xxl2.php	~DFD7A6DFAF6BAD27C2.TMP.1.dr	false	• Avira URL Cloud: safe	unknown
http://schema.org/WebPage	??????-????????[1].htm.2.dr	false		high
http://https://kelham-businesscentre.com/sm/xxl2.php">	??????-????????[1].htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com	EHPIBSAR.js.2.dr	false		high

Contacted IPs

Copyright null 2021



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.126.132	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339221
Start date:	13.01.2021
Start time:	17:37:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://sites.google.com/view/xfcghv/الصفحة-الرئيسية
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:	15
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:	MAL
Classification:	mal60.phis.win@3/39@3/1
Cookbook Comments:	• Adjust boot time • Enable AMSI

Copyright null 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 88.221.62.148, 173.194.69.102, 173.194.69.139, 173.194.69.138, 173.194.69.100, 173.194.69.101, 173.194.69.113, 108.177.126.95, 108.177.126.94, 108.177.119.113, 108.177.119.100, 108.177.119.138, 108.177.119.101, 108.177.119.102, 108.177.119.139, 216.58.212.163, 108.177.127.94, 209.197.3.24, 51.11.168.160, 23.210.248.85, 152.199.19.161, 13.88.21.125, 92.122.213.194, 92.122.213.247, 205.185.216.42, 205.185.216.10, 51.103.5.186 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, ssl.gstatic.com, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, www.gstatic.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fonts.googleapis.com, client.wns.windows.com, fs.microsoft.com, plus.l.google.com, fonts.gstatic.com, ie9comview.vo.msecnd.net, sites.google.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, apis.google.com, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: https://sites.google.com/view/xfcghv/%D8%A7%D9%84%D8%B5%D9%81%D8%AD%D8%A9-%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9

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\W26YVULP\263052666-atari-embeds.googleusercontent[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aKb:JFK1rFKb
MD5:	132294CA22370B52822C17DCB5BE3AF6
SHA1:	DD26B82638AD38AD471F7621A9EB79FED448A71C
SHA-256:	451ABBE0AEFC000F49967DABF8D42344D146429F03C8C8D4AE5E33FF9963CF77
SHA-512:	6D5808CAD199A785C82763C68F0AE1F4938C304B46B70529EA26B3D300EF9430AD496C688D95D01588576B3A577001D62245D98137FD5CD825AD62E17D36F15C
Malicious:	false
Reputation:	low
Preview:	<root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2CC6C75E-5609-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8608720915555124
Encrypted:	false
SSDEEP:	96:rvfZl6ZLz2tc9WTuZtT9fTWRMTxTlTofTncX:rHZUZLz2tc9WyZthfKRMdk8fbcX
MD5:	97C78B29A0E04F78F096780B88BF1442
SHA1:	C693B6F792E9D9B996534C991338C2B7B1302063
SHA-256:	B2F85465C83628AA0FA8D1A51267197540ABCC6A3F374ACC9F8EC4CABA4F7989
SHA-512:	E237250B8B8577F71DC42AC04C1C21339DEC3A7264317D2D44669D39A2BFDF3965EC70B45A0C1AE563AF55FF9BE6986C0F347CFED5B347939450008FDE41AD(
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\{2CC6C760-5609-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	80628
Entropy (8bit):	3.4216961983411966
Encrypted:	false
SSDEEP:	1536:dQpJ13KBvKYSwFOoLfUCuAjMUTElTa9EtkLEIPEQQxWZG:dQ5KRjSwFOoLfUCuAPElTa9EtkLEIPE1
MD5:	46BC81C7F85F0CCD6A3960E1B426E827
SHA1:	CE7578CF5534C8E8FF81BD49ED3F8ACC3A98BA4A
SHA-256:	40D8F7AB1A28B8502C7CFED685BB07523AEEAD4DFD4DB1C19E3652C59FC27DEA
SHA-512:	9BC3B19D08AB2629104BA8A9E51D26FC43B4DA09F685D00774AA5B9286379260E53D49BE3BCBEB2F2AE66B1B5DB4A826F57A94CC00119C010D1654F26DF3BD 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2CC6C760-5609-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{33D77CC1-5609-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5658543415092205
Encrypted:	false
SSDEEP:	48:IwJGcprQGwpayG4pQaGrapbS2rGQpKdG7HpRtsTGIpG:rPZ4QC6MBS2FA8Tt4A
MD5:	D4DCBA0B854C3F958666CE5994D32B9D
SHA1:	C13A67B4FCFFFAA934A1B38E9E24299DB11D426A
SHA-256:	5A24C592348CB4F9BE1147721DC5F85AC60C71E2C4A9C663043982E983B73C73
SHA-512:	818050797697B4C4BE810ACFAD33FB65CC5FDB84D656471C52886F985782966922926E34F231EE6BA0EAA52918869457C0D4E168B6F15EBC915C5D05E4FC3053
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.091201774963226
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEgNcNXnWimI002EtM3MHdNMNxOEgNcNXnWimI00ObVbkEtMb:2d6NxOgSZHKd6NxOgSZ76b
MD5:	E98B6F211C63EF504B699B0159FC2F13
SHA1:	00C02CE2194B379A39647ED366D7430B1CBF3BA8
SHA-256:	4325469226CB9CDBA0932492077EF117FE6AF75FBA0628BCB91D4CADDD863A1A
SHA-512:	E114DD0C209C15ABE38BC759014BFB686059D95F6E3B404757E81F8F342DF022A562A628CD0BE5E269468F274FFF89509FD89FDB70F8457593B8D38581A07791
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x04d50bb2,0x01d6ea16</date><accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x04d50bb2,0x01d6ea16</date><accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.08115730529575
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kgOB6OBFnWimI002EtM3MHdNMNxe2kgOB6OBFnWimI00Obkak6EtMb:2d6NxrUPXSZHKd6NxrUPXSZ7Aa7b
MD5:	12A5F31FE0343040FA5FA63F29EBD31D
SHA1:	6FE9A7D3466C111A4FEF11012AE6575074C94E49
SHA-256:	040410ECDE097C93CD6E62F603C2487E52361E7FAB85538DFD018D5273DBB1D8
SHA-512:	82A960120E788FB8DA99EE354B5B3B48CE823D2E6B4E9E383E64FC0BA9486BA88064728C041999D7C83E41A47DC2B11EB4D6177175B362FECCDD3CF9F6C3CDDC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x04d046ff,0x01d6ea16</date><accdate>0x04d046ff,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x04d046ff,0x01d6ea16</date><accdate>0x04d046ff,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.10827422147257
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLgNcNXnWimI002EtM3MHdNMNxvLgNcymnWimI00ObmZEtMb:2d6NxvFSZHKd6Nxv+mSZ7mb
MD5:	CB98313E1C381538F02986A8B4653F63
SHA1:	74EC42EDF4E9E99223776475F5817D4EEE10EFD5
SHA-256:	81F594C58B0289FF4736D4F60FCCF4935E88B1BF9C84F24F68A500838F7BB396
SHA-512:	AE783809D8D92E060F7913E747C825D97174ACD65D161A94D6CD7DDFBA8ACF6CE3C0BA1DC384DBF5C3777BA147D1F0CC34D774A69BD8DFEE4042097A00813 77
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x04d50bb2,0x01d6ea16</date> <accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>.. <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x04d50bb2,0x01d6ea16</date><accda te>0x04d76dfb,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.123674114048661
Encrypted:	false
SSDEEP:	12:TMHdNMNxigQLnWimI002EtM3MHdNMNxigQLnWimI00Obd5EtMb:2d6NxWSZHKd6NxWSZ7Jjb
MD5:	047CD802BC848DFABFB4C2A199172CF5
SHA1:	850626D6A036099E6570F96A04248690A6A23442
SHA-256:	8DF787F08F9442DD5EEB90C75A610BDE7B9B4B6F314F6B1F48819FEF9A0F20BE
SHA-512:	B2939A6C2418CB79C6AF028485B480AFF2DB1E7CEC4A5571B6BC30392F66B3568F42498A453AEE43B2319AA208ED07CBF61BC3C6189B80E17649FFB80C5A8F2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x04d2a95b,0x01d6ea16</date><acc date>0x04d2a95b,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x04d2a95b,0x01d6ea16</date><accdate>0x04d2a 95b,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.102286182657604
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwgy1ymnWimI002EtM3MHdNMNxhGwgy1ymnWimI00Ob8K075EtMb:2d6NxQAEmSZHKd6NxQAEmSZ7YKajb
MD5:	A369B457F605D020F1572E67F02E5938
SHA1:	D17AE1845BEA4C917F4C7D73DC5B4BEA3FB1C8ED
SHA-256:	4DDC1E82BA786E13F8DE23A4A6EB5C4ADE8A139C9E46D931ABC482D4FBC2AF41
SHA-512:	F96EB8A424D55DF82F3098068DBBE815528C10226298FB32F47320637D52ECECF7CC767CB9E2A7E4219E04E6E7AA1E735027DABDD3DC3DAC3999D5316EEBE1 2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x04d76dfb,0x01d6ea16</date> accdate>0x04d76dfb,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x04d76dfb,0x01d6ea16</date><accdate>0 x04d76dfb,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Entropy (8bit):	5.091925941213659
Encrypted:	false
SSDEEP:	12:TMHdNMNx0ngNcNXnWimI002EtM3MHdNMNx0ngNcNXnWimI00ObxEtMb:2d6Nx0JSZHKd6Nx0JSZ7nb
MD5:	080894F77A2DA1D9D65998ACDD22BBF3
SHA1:	DD2308EE360080E488D664F64236537E28CF9126
SHA-256:	5E07764D268AD4128731DA88D2363A79EF4C589BE0012F68EE05F66B55F07E96
SHA-512:	9CA3250DAA9DB4F06CEC873FE2E3B5D46B5C4BCD943C4FC913BBCDB7B593BDC0B3AFCA264F29BE5A04840F3FD17546F851255AFB3133524E73C9795A40DBA04
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x04d50bb2,0x01d6ea16</date><accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x04d50bb2,0x01d6ea16</date><accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.131625476233922
Encrypted:	false
SSDEEP:	12:TMHdNMNxxgNcNXnWimI002EtM3MHdNMNxxgNcNXnWimI00Ob6Kq5EtMb:2d6NxzSZHKd6NxzSZ7ob
MD5:	F6303D6B5E4FBAAE3403756FBE4A206F
SHA1:	CA48AA76437566A1A088B00AA99152CA62888CF3
SHA-256:	3DAA52BCD10F25A954F189B6AAB3ABFC1B5417A465746E29DB89CA87B545960D
SHA-512:	EACDA6FAAACC8A2D9CEEA9BC833DC60F24153676C39284E3D8FEEF0EA47865BF493BFC248AAF34DBBA3FDB9AC15845115DE2AFD291EB0000017664CB1A29B20A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x04d50bb2,0x01d6ea16</date><accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x04d50bb2,0x01d6ea16</date><accdate>0x04d50bb2,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.124024757297997
Encrypted:	false
SSDEEP:	12:TMHdNMNxcgQLnWimI002EtM3MHdNMNxcgQLnWimI00ObVEtMb:2d6NxISZHKd6NxISZ7Db
MD5:	8C452E54B873206ADC283CBA3870858C
SHA1:	2A6050001B9D8CC3C8C2D5E1391B5BFFF136701A
SHA-256:	F9BC4CE42D82554A1ADD430CD68F7ECD7380C952D174D15BB42DC7E25610961A
SHA-512:	BA90D7375A4D34DFC4D3417C4948898396510755D6B98540051F371DF94D5CE57517C0A55538DE8629A574663E35D84A3107F8EB8AF2664683620801ACAAC9EA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x04d2a95b,0x01d6ea16</date><accdate>0x04d2a95b,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x04d2a95b,0x01d6ea16</date><accdate>0x04d2a95b,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.109222362250643
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngQLnWimI002EtM3MHdNMNxfngQLnWimI00Obe5EtMb:2d6NxdSZHKd6NxdSZ7ijb
MD5:	008207AE51DCD0DF63FB35095F86CD53

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA1:	E6D51564A5BCFA63473B29BE31828F5184A6377E
SHA-256:	67C84999FD81C3394170ECDC01458F155CAAA3CBC35334718CBA5D1536F751D4
SHA-512:	A47E7CD032DC9E5EE4CFF7E552AAA48BF1B459A1FEBE2EFAD21D74E8C07543134BBF0AFB0469E811A37FD40EDABEBF4B91480469D542736D18CA1A54AF87A7D5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x04d2a95b,0x01d6ea16</date><accdate>0x04d2a95b,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x04d2a95b,0x01d6ea16</date><accdate>0x04d2a95b,0x01d6ea16</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1288
Entropy (8bit):	2.7813806560382615
Encrypted:	false
SSDEEP:	6:MY4NQMBQB3WIerVcxuGRglMRQ8W828W828W828W828S8eftXfc/l3b9l:h+YB3Y+0Ogy3X3X3X3XjeVU3b9l
MD5:	E232DF047CBCD0D27089F1CC717A972F
SHA1:	4621822A447446C0302292431DE032D923CEDEB5
SHA-256:	A4FDF279882A8508200319B0DCB5114CD7E9B37056606DF3ACB69308C15DF821
SHA-512:	498C5B83B6F0D6153E62E74EAD459545C41A3C1304F7835717541A4679975E1651BA4CEF605DFB03A2D4CEEA854F04D058C51FEA190273C36FB0EC08982BF9C8
Malicious:	false
Reputation:	low
Preview:	2.h.t.t.p.s.:././.s.s.l...g.s.t.a.t.i.c...c.o.m./.a.t.a.r.i./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.2...i.c.o.~.............. .h.......(....... ....@...................P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>.....................P>..P>.............P>..P>..P>..P>..P>..P>.....................P>..P>.............P>..P>..P>..P>..P>..P>.....................P>..P>.............P>..P>..P>..P>..P>..P>.....................P>..P>.............P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>...P>..P>..P>..P>..P>..P>...P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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............../.)x$.'"j.....1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H\|#z_.O......R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%...... ...t"uM..%.......j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.........(..(...K..{.^..'........`#./..B......N+p.m`...].lQ....Drg.M..Kx.^.S.*..........h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:LyfRPUY1e32pJd75q1DzPjsnouCrZsZtetWFNFfIP0cIWvdzNcrm:uJPb1em3dSPjKrZYtWntk0wvdzh
MD5:	60FA3C0614B8FB2F394FA29944C21540
SHA1:	42C8AE79841C592A26633F10EE9A26C75BCF9273
SHA-256:	C1DC87F99C7FF228806117D58F085C6C573057FA237228081802B7D8D3CF7684

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxM[1].woff	
SHA-512:	C921362A52F3187224849EB566E297E48842D121E88C33449A5C6C1193FD4842BBD3EF181D770ADE9707011EB6F4078947B8165FAD51C72C17F43B592439FFF4
Malicious:	false
Reputation:	low
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...$.....W.cvt .....T...T+...fpgm...p...5....w.`.gasp.....glyf.....;Q..ID..&0hdmx..H....n..... ..head..Hx...6...6.j.zhhea..H.....$....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.I..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\0W10PBUV\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	271
Entropy (8bit):	4.9884517789448
Encrypted:	false
SSDEEP:	6:UccrNMMsjcL1Ms0HzIV1MsXJJCRd1Ms1HF1MsjnK0DdT0:UccrNpsjcLms0H8VmsXJYms1HFmsjDDe
MD5:	23FE2C128B889E133D1949B2A3484C5B
SHA1:	8338D0BC9033FB9B36E8EA2E0A290C9E014E9525
SHA-256:	72018CFD44C30A588ECAE74C214001787E08B2B114FAF6DCCBF52A7B43578898
SHA-512:	D4B77E2CBD76D7F266022E3BF4314C63383A51C924903791BB7CEF8EE0638404248DAD41BA21063D0EB89148C4EE112D7DEA3143D6E739301B89B778186C03C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_US.SnHyU412DY0.O/m=gapi_rpc/exm=client/rt=j/sv=1/d=1/ed=1/am=wQE/rs=AGLTcCObTkZu7kqIvAlB0bY4g3IzlKIb5g/cb=gapi.loaded_1
Preview:	/* JS */ gapi.loaded_1(function(_){var window=this;_.z("gapi.rpc.setup",_.Pl);_.z("gapi.rpc.register",_.El);_.z("gapi.rpc.call",_.Il);_.z("gapi.rpc.unregister",_.Fl);_.z("gapi.rpc.sendHandshake",function(a,b){_.Pl(a)();_.zl.send(a,_.zl.EC(b),"*")});..});// Google Inc..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\inner-frame-minified[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):	2021
Entropy (8bit):	5.175853528118763
Encrypted:	false
SSDEEP:	24:hY4q3pksVqq2MzuJbprOXymRVBLPRRF0oReRtMQ1Kv3MlHoZkBwBepeUJ3hUUFWR:AyK1x+XoMlHoZkHhUoWAs+hg7j
MD5:	BB6B878935B0C4C96AE6E6DD83930DAD
SHA1:	B726BFF3C3F32A38262EBD3AC4ED82EEA5445316
SHA-256:	80E142904C9FEECA9D8C64AF55DABFDA8032B2AC29FC26CA11D59AA1ABDDC6AB
SHA-512:	35356A9D406613C501009AD3F60EC84CF42B9DA6435C61AB41D12A0D5C16CC2E8DB1783D2D61FC38042FD2D967D5F695FB85B16907F56548B5BA7AD31D464B1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://263052666-atari-embeds.googleusercontent.com/embeds/16cb204cf3a9d4d223a0a3fd8b0eec5d/inner-frame-minified.html?jsh=m%3B%2F_%2Fscs%2Fapps-static%2F_%2Fjs%2Fk%3Doz.gapi.en_US.SnHyU412DY0.O%2Fam%3DwQE%2Fd%3D1%2Fct%3Dzgms%2Frs%3DAGLTcCObTkZu7kqIvAlB0bY4g3IzlKIb5g%2Fm%3D__features__
Preview:	<!DOCTYPE html>.<html>.<head>. <style>body,html,iframe{margin:0;padding:0;height:100%;width:100%;overflow:hidden}.forceIosScrolling{overflow:scroll;-webkit-overflow-scrolling:touch}</style>.</head>..<body>.<iframe id='userHtmlFrame' frameborder='0' scrolling='yes'>.</iframe>..<script>function loadGapi(){var loaderScript=document.createElement('script');loaderScript.setAttribute('src','https://apis.google.com/js/api.js?checkCookie=1');loaderScript.onload=function(){this.onload=function(){};loadGapiClient();};loaderScript.onreadystatechange=function(){if(this.readyState==='complete'){this.onload();}};(document.head||document.body||document.documentElement).appendChild(loaderScript);}function updateUserHtmlFrame(userHtml,enableInteraction,forceIosScrolling){var frame=document.getElementById('userHtmlFrame');if(enableInteraction){if(forceIosScrolling){var iframeParent=frame.parentElement;iframeParent.classList.add('forceIosScrolling');}else{frame.style.overflow='auto';}}else{frame.setAttr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rs=AGEqA5keFj278I7UZ01QR4UKHsO_o5zzEA[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):	361139
Entropy (8bit):	5.700897891332934
Encrypted:	false
SSDEEP:	3072:6Zz79lLLshxYkZcPixSDrybVtO0GufSuDITk:C9lLLsx2ixS07
MD5:	7553957FFAE7090CB2C6294C8461B261
SHA1:	D643B65081AC628423A714E3249562BC31EB44C3
SHA-256:	7F0B94881F51F07528089A8737E63AB3F128E3912C19872DB98B90F3FDDB1F3D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\rs=AGEqA5keFj278I7UZ01QR4UKHsO_o5zzEA[1].css	
SHA-512:	FD58658B1EA5894102C8AA6552F5C5F68CE685235DC0B66F4C87197D78EF1389D072B16F71BB5553A4D84605FE6F999D8A9EB7E0B0E11C8DF2E4C0BF0A37B5E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/_/atari/_/ss/k=atari.vw.Lwr-IooTrXE.L.I11.O/d=1/ct=zgms/rs=AGEqA5keFj278I7UZ01QR4UKHsO_o5zzEA
Preview:	/*! normalize.css v2.1.1 | MIT License | git.io/normalize */article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,video{display:inline-block}audio:not([controls]){display:none;height:0}[hidden]{display:none}html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}a:focus{outline:thin dotted}a:active,a:hover{outline:0}h1{font-size:2em;margin:.67em 0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}hr{box-sizing:content-box;height:0}mark{background:#ff0;color:#000}code,kbd,pre,samp{font-family:monospace,serif;font-size:1em}pre{white-space:pre-wrap}q{quotes:"\201C" "\201D" "\2018" "\2019"}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:0}fieldset{border:1px solid silver;margin:0 2px;padding:.35em .625em .75em}legend{bo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\EHPIBSAR.js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1063500
Entropy (8bit):	5.61243137375731
Encrypted:	false
SSDEEP:	12288:toE09UPLbHe7v34F2BxpzmwExciU6qRMMM8B/:tL0qPLbHe7v3dBxFmbH5apB/
MD5:	495B618D32CED0E972701317CCD0D9F7
SHA1:	1C80A1C55F6727AF86CF66862AD16C4C7F43964F
SHA-256:	4998C47261B1C926E631901C27B66753BEF999AE2AF209820667ED5CC1105AB5
SHA-512:	45B345B4701C4775233B12C5339AC2AE93423F823DC72A607CCBFE38C649967E8CEA547D8A4131C24EA3B1BC9CCFC3F30C0B30044F4E350EBE3B1C556DB76CD
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("A4UTCb");:._.A();..}catch(e){_._DumpException(e)}.try{._.n("qAKInc");.var yG=function(a){_.Kn.call(this,a.ua);this.B=this.getData("active").ub(!1);this.C=this.O("vyyg5");this.D=_.db(_.eb(this).Bc().Ra(function(){var b=this.aa();this.B?b.Ta("qs41qe"):b.Ta("sf4e6b");this.B&&this.C.hf(b.getData("loadingmessage").string(""));this.B||setTimeout(this.Or.bind(this),500)}))};_.F(yG,_.Kn);yG.ia=_.Kn.ia;yG.prototype.Ib=function(){return this.B};_.zG=function(a,b){_.nn(a.aa(),"data-active",b)};.yG.prototype.Xm=function(a){var b=a.data.xy;switch(a.data.name){case "data-active":this.B="true"==b,this.D()}};yG.prototype.Or=function(){var a=this;_.db(_.eb(this).Ra(function(){var b=a.aa();_.gn(b,"sf4e6b")&&(_.hn(b,"sf4e6b"),a.B||_.hn(b,"qs41qe"),a.C.hf(""),a.xa(_.Cl))}))();_.Q(yG.prototype,"kWijWc",function(){return this.Or});_.Q(yG.prototype,"dyRcpb",function(){return this.Xm});_.Q(yG.prototype,"qs41qe",function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	43713
Entropy (8bit):	5.513395553273763
Encrypted:	false
SSDEEP:	768:pH9H5VPU98T8yXQ0H1doZ+oBVymo2Ry/NqDpp4zF9Mteh3LyCVTVbcXB/yCjWIuR:ppzU98YyvVdPqEF9Mte5VbM/PjWAxqB
MD5:	130D7B0198C0E4397C17D9C8B2753F89
SHA1:	D1E53CD4FE66CCE194E30BE7D41AC656CC526CC2
SHA-256:	A762AE4F4D0D95769C363081097055F98E008CB0AEC4D40223AD110653E0123E
SHA-512:	BFCFDE4996FA954B9ABD9586AB357FAC9B14C5A84E949A497911F49E7B4186926340A287E40644A34B9411E34712B90B6C0D567E090E667C32BBB1C97CFEDB3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_US.SnHyU412DY0.O/m=gapi_rpc/rt=j/sv=1/d=1/ed=1/am=wQE/rs=AGLTcCObTkZu7kqIvAlB0bY4g3IzlKIb5g/cb=gapi.loaded_0
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,pa,ra,Ca,Ea,Ja,Sa;_.ba=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};ka="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};.pa=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");};ra=pa(this);Ca=function(a,b){if(b)a:{var c=ra;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&&ka(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\client[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12530
Entropy (8bit):	5.460187265355198
Encrypted:	false
SSDEEP:	192:8iApwYKUa9u5vocJJBA1Uwg7Cwm5Mi0+Sczlw:83pw9dk9JO1UCwmR0+Scxw
MD5:	BBCA6CE9FD075E1CEFFC0FBE577E6E3E
SHA1:	5AA932DAB5FB4FBE198E0BC586B8A0B41A421C96
SHA-256:	09EB156DAC054CB50E17986447280D2117FEA6A8697E587131581F0EE2476E9A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\client[1].js	
SHA-512:	D9BF6BDD86DB2B0435BF2262DCC09B74A75D6D9E382F2F05BC691323754D403E25DFA8287A9FE84D02C60FBED03BF00FF4878F919BA8E57134379457AB014E9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/client.js?onload=gapiLoaded
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\MEEXW4H4\m=pB6Zqd,syt,IZT63,SF3gsd,vfuNJf,syo,syn,sym,syr,sys,syu,syy,YNjGDd,n73qwf,syx,syz,PrPYRd,xs1Gy,hc6Ubd,o02Jie,SpsfSb,sy15,sy14,syj,sy13,zbML3c[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	25561
Entropy (8bit):	5.401938204280719
Encrypted:	false
SSDEEP:	768:1Bn3gdE0vAS2b0w10otV+mToPy0+OB+oBF6PWLB4zwm2+3J44ouJKVTxS8DUwp:1BsDw1zROB+oBF6PWLB4X2+Zu84Ui
MD5:	6E6D50B0F39FAA43F001752CEDF5459A
SHA1:	EE0A9D08B33D62AA42059056F8A38D094999346B
SHA-256:	813020461F85B2F489C07B579575B219A33C3B37FCB9E0F7FCCBEA5B69907912
SHA-512:	7A4146001B9EEEEB4D233CD638E8AAD4FD76B65ED9021EE9E5264FC75CB2D24726BE9605E4F6A1EAB63F7753FFCA82AAE2E64154C458E22E1C034D5D2CDD8B8
Malicious:	false
Reputation:	low
Preview:	"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("pB6Zqd");._.lk(_.Xw);.._.A();..}catch(e){_._DumpException(e)}.try{._.xD=function(a,b){return(b=b.WIZ_global_data)&&a in b?b[a]:null};_.n("syt");.._.A();..}catch(e){_._DumpException(e)}.try{._.n("IZT63");._.yD=function(a){_.rl.call(this,a.ua)};_.F(_.yD,_.rl);_.yD.ia=_.rl.ia;_.yD.prototype.get=function(a){var b=_.xD("nQyAE",window)[a];return void 0!==b?new _.vn("nQyAE."+a,b):null};_.yD.prototype.getAll=function(){return(new _.vn("nQyAE",_.xD("nQyAE",window))).D()};_.yD.prototype.isEnabled=function(a){return this.get(a).ub()};_.Jn(_.cpa,_.yD);.._.A();..}catch(e){_._DumpException(e)}.try{._.n("SF3gsd");._.lk(_.$w);.._.A();..}catch(e){_._DumpException(e)}.try{._.n("vfuNJf");.var ZD=function(a){_.rl.call(this,a.ua)};_.F(ZD,_.rl);ZD.ia=_.rl.ia;_.Jn(_.Zw,ZD);.._.A();..}catch(e){_._DumpException(e)}.try{._.n("syo");.._.A();..}catch(e){_._DumpException(e)}.try{._.n("syn");.var uB=function(a,b){this.eb=a;this

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	279841
Entropy (8bit):	7.9830026217040855
Encrypted:	false
SSDEEP:	6144:/r4Ft4cjlEv8FqF3BRpgxsll3Om0JwrwTigL5h83bCEUp6t3:Dk4LBRCxsll3Om0SQBhmbsUp
MD5:	BCC8C3ADD31D42B2C4B6D13C0DB8D3A5
SHA1:	022579B72587DDA481F4C3C51E5139D092011966
SHA-256:	6BDE963A562FFD594492BDFF280C01E9E6518856AA3A9F14B96FCAD867CE2F0F
SHA-512:	152895B08A61C27738B02F447895C2C05EE6AD3201906A0AA373C414D0FFED22D30CE06972A52F7F866143B0C06B7079295CB4F1CBCBEFD6E46ACB2810CC5E5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://lh5.googleusercontent.com/omAG2gYfq3pkx-zHvXG8rqmfJC60NjuUaLu1ap51rxW1ypKygNrQEzgUeH0uxHTxh09oH5qO=w16383
Preview:	......JFIF.....C.....#"""#"""""...C.....!! !!"""""".....8...."..... .....J.....!1A."Qa.2q.BR..#br.....3....$C.....S.c..4Ds%&.....=.....!1"A2B.QRb.ar.....q.....#....C3.$.....?.....3.y..&L.....1.l..-@.Y..9.q..YI..A.....`.q...C..@0.Y+.A.A.C.C...%a.E`...&L.d...2d.&L.0..&L.....2a...cd.L.+&PL.+.d..&.+ .k.`...a.... a.a.....-... ... >.i~..9.@..l!/.8.d(.....p.x.....85.d.8.<.A..<...%./!....L..S...d.?t.|p.97.....Si.,ef.:...W.....&.H..2...6{.Q@L!=...6{..E[}...l.....^.+.....X..&...@0.0\p...(@1.....v{....d.....(.....6Wq..q.M..%...}.B..`...K..'#.K.....7...P.C%a.....Y1..`....J..a.;q....5....a...k .d..... a....x0.... ..r`....+(&@2.....&...0.B..a...J..V..8k%`.....J.Xrd...2`.&L...&.2d.....1.r.d...2d....L.`#.L.k...+(.n...0...Ya..e ...$d...+.d.A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20464, version 1.1
Category:	downloaded
Size (bytes):	20464
Entropy (8bit):	7.969622511404751
Encrypted:	false
SSDEEP:	384:edA/1eSg82dg1kGeF2BFDEE+/adkuouo34TjkWqTExYOYg/c1iuHotcO:ey/1eSnLkGeWFQECadcLlc/TEfYr1RO
MD5:	87284894879F5B1C229CB49C8FF6DECC
SHA1:	FB1BD3BAF122D5D350EB387F0536C20DA71F09DF
SHA-256:	BA98F991D002C6BFAAF7B874652FFDCDE9261A86925DB87DF3ED2861EA080ADF
SHA-512:	663BA95BBBC6F7E65D7B1293E4A044C9111438A03B16664FC38A2B2F2C1A4CE96991C847B36691388AB322525A83DB2724CB4D1B9BF0440727F0B5CA7073AB8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOlCnqEu92Fr1MmEU9fBBc-[1].woff	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmEU9fBBc-.woff
Preview:	wOFF.....O.....D.....GDEF.....G...d....GPOS.....~..GSUB.....'.....r.OS/2.....Q...`t...cmap...\.....W.cvt ...T...\...\1..Kfpgm.....2.....$.gasp.....glyf.. ....;...l..(.4hdmx..H....l....."..head..l<...6...6...rhhea..It.....$....hmtx..I....x.....gO.loca..L.....,_.C|maxp..M.... ... .(..name..N.....:.post..N..... .m.dprep..O.....S...)x...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...../.)x$.'"j... ..1LGmaGxQxG....~.:'.A..hd.z,.k..KO.....^.}H\|#z_.O.....R..A...9..A..!.(./..."..:.Iq1.r..s..r.7r.7s..q.wr....nz..]...2..d4c..c....d....T.1...d....\....,c9k.g..Yv.#O."%..... ...t"uM..%..... .j.#^.....}\c.q.i...<jy.D...C.01.2.r.....V..z.W.7b..L.S.41]..kUs.X/6..b.....(..(...K..{.^..'.....`#./..B.....N+p.m`...].lQ....Drg.M..Kx.^.S.*.....h ..$.k.'Hy.I.ze..4z.-T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\KFOlCnqEu92Fr1MmSU5fBBc-[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 20348, version 1.1
Category:	downloaded
Size (bytes):	20348
Entropy (8bit):	7.971548837012925
Encrypted:	false
SSDEEP:	384:sSRPUR1eEsGitLcRtdt6S1PvpjwY9O1V6LTFY88fFFEagMR3SAFNE/A:saP+1eBX4Rtdt6EJjwY9O1V6Pm82lR39
MD5:	B00849E00F4C2331CDDD8FFB44A6720B
SHA1:	5B7820FEC8F9810E291E1EB98764979830ED6621
SHA-256:	76B05400FFF9DA5B43862E3713099E3913916A629560265ED24B19D031227CBF
SHA-512:	64F2BB1D16525CB5435CC3AA253D83669C321D68695CDF14218EEE43B5347DD6BC67B23D6F5E359971B1FFA72857C2C9DCEC0370535F12EDC20AF42CF41CF6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmSU5fBBc-.woff
Preview:	wOFF.....O|.....GDEF.....G...d....GPOS.....GSUB.....'.....r.OS/2.....P...`t6..cmap...$.....W.cvt .....X...X/...fpgm...t...4.....".gasp.....glyf.. ....;...lxRn..hdmx..Hl...l.....head..H....6...6.Y.ihhea..I.....$....hmtx..I0....._Gloca..K.....k.N.maxp..M.... ... .(.\name..M.....|..9.post..N..... .m.dprep..N.....:z/.Wx...1. .P.....PB..U.=l.@..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'/.....ks5zY 5c...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\PSUEOSZZ\cb=gapi[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	308000
Entropy (8bit):	5.528397091372971
Encrypted:	false
SSDEEP:	6144:pKhyr6C6RlnOrE5zwkkaf5s6wCKeDHMDzb/PiBNO+:pyyrr+tOI1k7CDLQE
MD5:	E41FC242EF1337574A488143FFDB86FB
SHA1:	FCE52270E2E0785236E47256EB75CF8B964B4A57
SHA-256:	9C8218196A8B72663BD53CC1B1E0F31D27EF3FB2AA66993293EAD312A75ED303
SHA-512:	997C8AC2F7D1E4897DF462146C799C51BB65F12BA01FEC49AB91EA251FD5FFC53EA0B846DCA7025AA1D490A3B16DBEBA55ADCB96669704433D4E42620CB968A1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/_/scs/apps-static/_/js/k=oz.gapi.en_US.SnHyU412DY0.O/m=client/rt=j/sv=1/d=1/ed=1/am=wQE/rs=AGLTcCObTkZu7kqIvAlB0bY4g3IzlKIb5g/cb=gapi.loaded_0
Preview:	/* JS */ gapi.loaded_0(function(_){var window=this;./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var ia,ka,pa,ra,Ca,Ea,Ja,Sa;_.ba=function(a){return function(){return _.aa[a].apply(this,arguments)}};_._DumpException=function(a){throw a;};_.aa=[];ia=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}};ka="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};.pa=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");};ra=pa(this);Ca=function(a,b){if(b)a:{var c=ra;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&&ka(c,a,{configurable:!0,writable:!0,value:b})}}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\intermediate-frame-minified[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):	2303
Entropy (8bit):	5.082372609214882
Encrypted:	false
SSDEEP:	48:A2E99KXccTrPllsBYN0i49YWAaMlLZ2y8ErHhUogVj:A2EYccXPlLN0r9YWPuLZ2y8S4V
MD5:	395EBFE6449B3DDFD31BB24C08B33B2D
SHA1:	927F8CABD22E19D9CFF81854DABF9D8C2CF4CD93
SHA-256:	B8436DEDA167997143CF3A97B1FC3077530530F0DF46F28B7DC4DA849B066BE4
SHA-512:	E94A12A656E6FFFDF5ECFEC8F9F8D0EAADA2F485A87CB20E9CF97081955541A34E5BD95B1000C24D1AB709259C785ED3B900C7C3CE7A46EEDABF9504CAE580A4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\intermediate-frame-minified[1].htm	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/atari/embeds/5de913a2354e93acf4d43c4db53928e5/intermediate-frame-minified.html?jsh=m%3B%2F_%2Fscs%2Fapps-static%2F_%2Fjs%2Fk%3Doz.gapi.en_US.SnHyU412DY0.O%2Fam%3DwQE%2Fd%3D1%2Fct%3Dzgms%2Frs%3DAGLTcCObTkZu7kqIvAlB0bY4g3IzlKlb5g%2Fm%3D__features__&r=426232770
Preview:	<!DOCTYPE html>.<html>.<head>. <style>body,html,iframe{margin:0;padding:0;height:100%;width:100%;overflow:hidden}.forceIosScrolling{overflow:scroll;-webkit-overflow-scrolling:touch}</style>.</head>..<body>.<iframe id='innerFrame' name='innerFrame' sandbox='allow-scripts allow-popups allow-forms allow-same-origin allow-popups-to-escape-sandbox allow-downloads' frameborder='0' allowfullscreen>.</iframe>..<script>function loadGapi(){var loaderScript=document.createElement('script');loaderScript.setAttribute('src','https://apis.google.com/js/api.js?checkCookie=1');loaderScript.onload=function(){this.onload=function(){};loadGapiClient();};loaderScript.onreadystatechange=function(){if(this.readyState==='complete'){this.onload();}};(document.head||document.body||document.documentElement).appendChild(loaderScript);}function updateInnerFrame(url,enableInteraction,forceIosScrolling){var urlEl=document.createElement('a');urlEl.setAttribute('href',url);if(urlEl.protocol!="https:"&&urlEl.protocol!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95821
Entropy (8bit):	5.3940293615751695
Encrypted:	false
SSDEEP:	1536:/PEkjP+iADIOr/NEe876nmBu3HvF38sEeLHFoqqhJ7SerN5wVI+xcBmPv7E+nzm8:ENMyqhJvN32cBC7M6Whca98Hrh
MD5:	D4A20D75DB01A33E2D65E303CE5C34F3
SHA1:	B14A228C3632EBFE3D20E5EA830CEEA313523353
SHA-256:	4B940065E2A67C37E3BD02B23C651F4744A3C219ABA2D4FB99A631113494D376
SHA-512:	D34DAAD4E8046B47E28F7A54DD89B223E9364AFB4B9F0AB6642603F3229C02C131AFD780ADA57B521BD56CDD90B1AB09FA367502F869540CDC506E58B278762
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://code.jquery.com/jquery.min.js
Preview:	/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\??????-????????[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):	63290
Entropy (8bit):	5.8040520519765195
Encrypted:	false
SSDEEP:	768:SHwW6fdll8qBkZ1+xWa4TUNUGhFIPZFFBS53HJbHjtOG6wHEnm6:SHI3qBkZ1+xWaa/GhiBXB0ptL6wHEm6
MD5:	8FFFD47D9D64F7184FD9B9271327EC12
SHA1:	3C65506AE61025055C484BFE5494634C161B4E91
SHA-256:	1C77F68991A3EBA8434DB950C89CC8F5924E6237578D7B91490F7E6C09686AF9
SHA-512:	61BB5304332C77F1324B60DEB15669093D86E83FE1A7F434220BDDBB5749F8F72185A7C37096EF1723097BD3A738CE54DB6810EA6D8A6759B1F779A468C14ED7
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_20, Description: Yara detected HtmlPhish_20, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\??????-????????[1].htm, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html><html lang="en-US" itemscope itemtype="http://schema.org/WebPage"><head><meta charset="utf-8"><script nonce="AygQYOHxcR5A83rEiebGgQ">var DOCS_timing={}; DOCS_timing['sl']=new Date().getTime();</script><script nonce="AygQYOHxcR5A83rEiebGgQ">function _DumpException(e) {throw e;}</script><script nonce="AygQYOHxcR5A83rEiebGgQ">_docs_flag_initialData={"atari-eiicg":false,"atari-eiitev":false,"docs-sup":"","docs-eea":false,"docs-ecci":false,"docs-ipmmp":true,"docs-esi":false,"docs-liap":"/logImpressions","ilcm":{"eui":"AHKXmL1ISINiSYe3PBl9mrLvq1qtGOpz9D3aenzCm7mrKBnB9Xo2JdsJB1cuFCEAQbtXOmi7sjDW","je":1,"sstu":1610555901217000,"si":"ClySiKOsme4CFQtFHwod_vICAQ","gsc":null,"ei":[5715286,5709892,5713211,14101454,5703022,14101514,14101502,5708870,5720060,5721004,14100854,5714628,14101510,5713207,14101538,14101462,14101442,5711850,5715290,5711808,14100834,5706832,5720925,14101430,5706836,5719651,5712211,5703839,5704621,14101254,5714550,5713049,5707711],"crc":0,"cvi":[]},"docs-ccdil"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\api[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	12518
Entropy (8bit):	5.461151739893325
Encrypted:	false
SSDEEP:	192:8iApwYKUa9u5vocJJBA1UwgRCwm5Mi0+Sczlb:83pw9dk9JO1U8wmR0+Scxb

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\api[1].js	
MD5:	D2E15D41B50707F172A289D465A6C717
SHA1:	A1AD6F1BFE4FCF9BD585C71E45FB3C81318DA94F
SHA-256:	9B9A769F26929AC9DBE5B7E6DE2015E7959804086C9F993017840C7169CDCC71
SHA-512:	611412590856E99141CE619D7C584C793A77B31CC028B49DCAA2342ADAA847B3F1F944A3511118024570585643893D5F83DC06FD1C0CE2E3469122A9E80C155B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://apis.google.com/js/api.js?checkCookie=1
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\WJ8I2OL4\css[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1168
Entropy (8bit):	5.134353630032397
Encrypted:	false
SSDEEP:	24:53Y3QYGal+q03Y3QY7alt3Y3QYN0al+503OYGalO3OY7alG3OYN0aII:pY3Q1al+5Y3QEallY3Qpal+AO1al0OEq
MD5:	6427988FBBD306471F9ADC048D8BB309
SHA1:	4A84AFD7BD33766334AC757E08E15A8ED19DA928
SHA-256:	0B5CD225186F00CDAA634377B64D124F7AD0F524B3926927068FC781B67E033C
SHA-512:	686B32D275B35BA2943204C23D5B21D660AEF0261749BB573BA22A4B7A1904E2D41F29DDEDD55F40F4CFFA50C1449A8C051818FCB6363ECF24BADFC3C93247(
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.googleapis.com/css?family=Lato%3A300%2C300italic%2C400%2C400italic%2C700%2C700italic&display=swap
Preview:	@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI9w2_Gwfr.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u8w4BMUTPHjxsAXC-s.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: italic;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u_w4BMUTPHjxsI5wq_Gwfr.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lato/v17/S6u9w4BMUTPHh7USSwiPHw.woff) format('woff');.}.@font-face {. font-family: 'Lato';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/lato/v17/S6uyw4BMUTPHjx4wWA.woff) format('woff');.}.@font-face {. font-family:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\css[2].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1749
Entropy (8bit):	5.22976294226381
Encrypted:	false
SSDEEP:	48:IOEaRqP/OXaRWO1aNsOEaNtCOXaNCOpaNxOEaL1OpaGU:IOEaeOXaYO1aNsOEaNtCOXaNCOpaNxOz
MD5:	05A339E7D2C78834F80DC1865DF9BD64
SHA1:	0122A9D31CE36E12C0AA48CE313C06299F0FA188
SHA-256:	C7303D7EE1480C9B183FFDE55A0AA236D2586AF40775267B7EB6118D67545770
SHA-512:	0341F1AEF6F061208062B2A67DF57C385E38ED56FFB3E75059C3D0E9D8CF4C76786E5F38665394FA034E3A6220B2B457BA48B8D6902BDF2786B84AB4F5EAC6B9
Malicious:	false
Reputation:	low
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. font-display: swap;. 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;. font-display: swap;. src: url(https://fonts.gstatic.com/s/googlesans/v27/4UabrENHsxJlGDuGo1OIlLU94YtzCwA.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 300;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOlCnqEu92Fr1MmSU5fBBc-.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/roboto/v20/KFOmCnqEu92Fr1Mu4mxM.woff) format('woff');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. font-display: swap;. src

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon_2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 16x16, 32 bits/pixel
Category:	downloaded
Size (bytes):	1150
Entropy (8bit):	2.3710475547263856
Encrypted:	false
SSDEEP:	6:RlMRQ8W828W828W828W828S8eftXfc/lk:Ry3X3X3X3XjeVUk
MD5:	EA69A3F95DD5484853D128186DB7E13D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon_2[1].ico	
SHA1:	5FDB5FE05108FD6E5386BBDA06778AF4B446DC6A
SHA-256:	8179E80BCFEF62154D1FF7371A1C60BD2C6C1E71C3DA2F4A8B1DB518A1900EC2
SHA-512:	2169D31065059C3677D025F27A5650C1E35BF83B6D6B3D80842B0809FF67E85388CB00213A4BD3FA76F71909A21298C824B39299A3980BA3B11C0297DB472610
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ssl.gstatic.com/atari/images/favicon_2.ico
Preview:	.... .h.......(....... ....@....................P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P >..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>.................... .P>..P>.............P>..P>..P>..P>..P>..P>.....................P>..P>.............P>..P>..P>..P>..P>..P>.....................P>..P>.............P>..P>..P>..P>..P>..P>.....................P>..P>. ....P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>....... ....P>..P>..P>..P>..P>..P>...P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>. .P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P>..P

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\m=sy1a,fgj8Rb,EGNJFf,sy1b,uY3Nvd,syg,syi,HYv29e[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>21690</td></tr>
<tr><td>Entropy (8bit):</td><td>5.5551208477469265</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:FP+tW6Z2WEanMTTSqfek4Dk9yoJDvkfd25cI2vvkofsZZunCvHut+RiipBbs6a:Z6ZeTS4vyoP2vvkinCvOtETbs6a</td></tr>
<tr><td>MD5:</td><td>3E0CE2D7193DADADFA0862F855EA8900</td></tr>
<tr><td>SHA1:</td><td>2A0AC38CCEE930CAC17CFBB9354818AFF99AD170</td></tr>
<tr><td>SHA-256:</td><td>D2156269EAC569C028A2F09D1692B00183D6FE1BAEE41B84CD83739621070B62</td></tr>
<tr><td>SHA-512:</td><td>5F26A8252BD4D789D5DCFBB4438ACA6758FC494A9AD45D8954704C8626F3D1F88E65CBBBE37BA78687FB31D43364468DF33DF829B2E6D26F1CE824ECA8E2D7
E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{._.n("sy1a");.._.A();..}catch(e){_._DumpException(e)}.try{.var yza,zza;yza=function(a){var
b=_.Un;try{_.Un=1,a.apply(void 0)}finally{_.Un=b}};zza=function(){return(0,_.R)('<svg width="24" height="24" viewBox="0 0 24 24" focusable="false" class="'+_.S("XAUpl
d")+'"><path d="M19 6.41L17.59 5 12 10.59 6.41 5 5 6.41 10.59 12 5 17.59 6.41 19 12 13.41 17.59 19 19 17.59 13.41 12z"></path><path d="M0 0h24v24H0z" fill="none
"></path></svg>')};._.EF=function(a){a=a||{};var b=a.Ja,c=a.cI,d=a.zu,e=a.content,f=a.Sb,g=a.position,m=a.transition,r=a.title,u=a.ul,v=a.close,E=a.PU,H=a.OU,L=
a.buttons,T=a.NU,W=a.vx,pa=a.Iba,ta="",Ja=_.Rp(g)&&-1!=(""+_.Pp(g)).indexOf("PositionFullScreen");g=null!=E?E:null!=u?u:null!=v;E=null!=T?T:L;T=_.Rp(r)||g;var w
b=Ja?"TNczib":"tOrNgd";Ja=Ja?"X1clqd":"qRUolc";if(T){d='<div jsname="'+_.S("r4nke")+'" class="'+_.S("R6Lfte")+" "+_.S(wb)+" "+_.S(Ja)+(d?" "+_.S(d):"")+'">';if(
g||_.Rp(H)){g='<div</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\m=view[1].js</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with very long lines</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>480373</td></tr>
<tr><td>Entropy (8bit):</td><td>5.560819478229992</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6144:B2J11q+Nv2fh851lxCLUe8ayXDL7Ycr4xf2YRL4:B61+hGXx5L71YO</td></tr>
<tr><td>MD5:</td><td>7492D2DE499DA01734BADD4A4B133D2C</td></tr>
<tr><td>SHA1:</td><td>870CC93BBCB1BA92B0A133E1F2260B8182038AD3</td></tr>
<tr><td>SHA-256:</td><td>A9315424DA3E3178962FE75BC52AC6382CB79213019AAFE05EA0B848FD7AB4F4</td></tr>
<tr><td>SHA-512:</td><td>E6032610C877FBAD5F35B9EAA0E3F2155D77DFE642E99DE663003E0A07AE172ADD099413F856B0570C159D11631BD40C1949C013F0D725D17A158305359CADC</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://www.gstatic.com/_/atari/_/js/k=atari.vw.en_US.zvyITglA-UA.O/d=1/ct=zgms/rs=AGEqA5mOtu0fC3gH9x9ySEpQ8u5uFRZo2w/m=view</td></tr>
<tr><td>Preview:</td><td>"use strict";this.default_vw=this.default_vw||{};(function(_){var window=this;.try{.var aaa,baa,Ia,daa,Sa,eaa,gaa,haa,jaa,gb,maa,naa,paa,raa,Cb,Db,uaa,Gb,vaa,wa
a,Lb,yaa,Faa,Haa,Iaa,Kaa,Maa,Oaa,Paa,Uaa,Yaa,Zaa,nc,$aa,oc,pc,aba,zb,bba,qc,tc,uc,fba,xc,yc;_.aa=function(a){if(Error.captureStackTrace)Error.captureStackTrace(
this,_.aa);else{var b=Error().stack;b&&(this.stack=b)}a&&(this.message=String(a));this.B=!0};_.ea=function(a){return a[a.length-1]};_.fa=function(a,b,c){for(var d="string
"===typeof a?a.split(""):a,e=a.length-1;0<=e;--e)e in d&&b.call(c,d[e],e,a)};._.ia=function(a,b,c){b=_.ha(a,b,c);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]};_.h
a=function(a,b,c){for(var d=a.length,e="string"===typeof a?a.split(""):a,f=0;f<d;f++)if(f in e&&b.call(c,e[f],f,a))return f;return-1};_.ja=function(a,b,c){for(var d="string"===type
of a?a.split(""):a,e=a.length-1;0<=e;e--)if(e in d&&b.call(c,d[e],e,a))return e;return-1};_.la=function(a,b){return 0<=(0,_.ka)(a,b)};_.ma=function(a){if(!Array</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\~DF34392B1F52AB3DA5.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.48206895517659615
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loWF9loa9lWzSkKnZDe:kBqoI1jzSh4
MD5:	D410D90A4F725BA8D65E5B90E3962839

Copyright null 2021

C:\Users\user\AppData\Local\Temp\~DF34392B1F52AB3DA5.TMP	
SHA1:	E398DCBAC32590AA3951247C636070569DDCAD8A
SHA-256:	9D3F41FDC10D9E0D288313CAB8BE1600615E5918FA36DBAE7081FC98CB77F778
SHA-512:	2A82F3406CAF6C3E0F3381B0EFD869CF1D93E5D4C4040B2CF5B8AB49F6780EA80F2796A4595BD1921E77D47F152841C1278A4C1C34EF58314DD14EC6918B91B
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF47EFAA0EAA46CB18.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

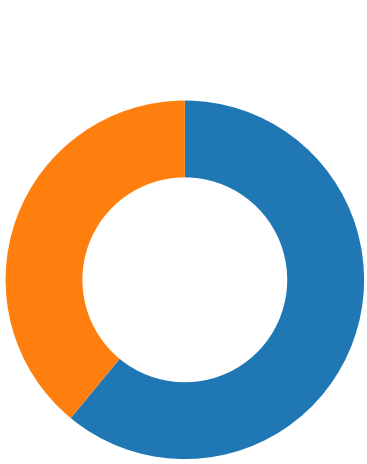
C:\Users\user\AppData\Local\Temp\~DFD7A6DFAF6BAD27C2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	83632
Entropy (8bit):	2.568168828249672
Encrypted:	false
SSDEEP:	1536:0J13KBvKYSwFOoLfUCuAjMUTElTa9EtkLEIPEQQxWZB:4KRjSwFOoLfUCuAPElTa9EtkLEIPEQQ+
MD5:	93B387A2204909D43211047CCEA24CC5
SHA1:	26671279D4BFFF264E820ECC7707414A7B788A9D
SHA-256:	F830382282C08A2262538AE61251B9E9D8C7F5B6969F0AB43DB60AABF961E926
SHA-512:	84BBAB32AF42D9EB3AE68F662FE382E45CFD36498223BA1BBC700F946610247DC99939239CA2CD2BC91278320D493B96F01678BA3DEAC125F17C5473B0D2087
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:38:22.124236107 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.133276939 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.172264099 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.172420025 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.181046963 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.181317091 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.230132103 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.231826067 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.278254032 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.278462887 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.278489113 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.278522968 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.278578043 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.278614998 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.278639078 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.278680086 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.278702021 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.279808044 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.279954910 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.279978991 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.280000925 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.280019045 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.280019999 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.280076027 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.287312031 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.287787914 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.288055897 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.335607052 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.335648060 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.335675955 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.335695982 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.335732937 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.336483002 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.341187954 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.345582962 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.346008062 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.384511948 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.393659115 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.393676043 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.393768072 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.393776894 CET	443	49727	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.393857002 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.443872929 CET	49727	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.497915030 CET	443	49727	108.177.126.132	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:38:22.524450064 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.524501085 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.524538040 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.524574995 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.524615049 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.524660110 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.526873112 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.526926994 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.526987076 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.527044058 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.529232979 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.529289007 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.529372931 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.529431105 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.531668901 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.531811953 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.531831026 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.531894922 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.534058094 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.534095049 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.534132957 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.534157038 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.536505938 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.536544085 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.536585093 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.536609888 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.538834095 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.538872957 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.538906097 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.538930893 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.541255951 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.541292906 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.541336060 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.541363001 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.543752909 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.543788910 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.543859959 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.543896914 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.546015024 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.546061993 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.546148062 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.546194077 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.548543930 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.548645973 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.572801113 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.572839022 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.572933912 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.572976112 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.573873997 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.573918104 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.573973894 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.573996067 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.576365948 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.576397896 CET	443	49726	108.177.126.132	192.168.2.3
Jan 13, 2021 17:38:22.576457024 CET	49726	443	192.168.2.3	108.177.126.132
Jan 13, 2021 17:38:22.576478958 CET	49726	443	192.168.2.3	108.177.126.132

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:38:16.908272982 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:16.956190109 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:18.107666016 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:18.158494949 CET	53	63492	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:38:19.518605947 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:19.581244946 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:20.730365038 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:20.797768116 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:21.378881931 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:21.400329113 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:21.432457924 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:21.435197115 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:21.459774971 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:21.509681940 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:21.999713898 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:22.063779116 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:23.974432945 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:24.022357941 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:25.015414953 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:25.063246965 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:25.709886074 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:25.774365902 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:26.256400108 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:26.321454048 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:26.878166914 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:26.926246881 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:37.510166883 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:37.569292068 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:44.679994106 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:44.728996992 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:45.238061905 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:45.295880079 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:49.509574890 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:49.557564974 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:50.407780886 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:50.455764055 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:50.521578074 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:50.577781916 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:51.411678076 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:51.468069077 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:51.537266016 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:51.585294008 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:52.426909924 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:52.476349115 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:53.183073044 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:53.233715057 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:53.907886028 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:53.955693007 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:54.547039032 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:54.603310108 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:56.005141020 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:56.055860043 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:57.664546013 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:57.712833881 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:57.911773920 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:57.960093975 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 17:38:58.552373886 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:38:58.600114107 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 17:39:00.388300896 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:39:00.445990086 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 17:39:02.827776909 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:39:02.888293982 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 17:39:03.810307026 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 17:39:03.868386984 CET	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:38:21.999713898 CET	192.168.2.3	8.8.8.8	0x1d40	Standard query (0)	lh5.google usercontent.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:38:26.256400108 CET	192.168.2.3	8.8.8.8	0xaf70	Standard query (0)	263052666-atari-embeds.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 13, 2021 17:38:26.878166914 CET	192.168.2.3	8.8.8.8	0x3b7b	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:38:22.063779116 CET	8.8.8.8	192.168.2.3	0x1d40	No error (0)	lh5.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:38:22.063779116 CET	8.8.8.8	192.168.2.3	0x1d40	No error (0)	googlehosted.l.googleusercontent.com		108.177.126.132	A (IP address)	IN (0x0001)
Jan 13, 2021 17:38:26.321454048 CET	8.8.8.8	192.168.2.3	0xaf70	No error (0)	263052666-atari-embeds.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 17:38:26.321454048 CET	8.8.8.8	192.168.2.3	0xaf70	No error (0)	googlehosted.l.googleusercontent.com		108.177.126.132	A (IP address)	IN (0x0001)
Jan 13, 2021 17:38:26.926246881 CET	8.8.8.8	192.168.2.3	0x3b7b	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		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
Jan 13, 2021 17:38:22.278639078 CET	108.177.126.132	443	192.168.2.3	49726	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 Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 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		
Jan 13, 2021 17:38:22.280019999 CET	108.177.126.132	443	192.168.2.3	49727	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 Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 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		
Jan 13, 2021 17:38:26.425961971 CET	108.177.126.132	443	192.168.2.3	49736	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 Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 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
Jan 13, 2021 17:38:26.427371025 CET	108.177.126.132	443	192.168.2.3	49735	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 Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 2592 Parent PID: 792

General

Start time:	17:38:17
Start date:	13/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7a3290000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Copyright null 2021

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: 3488 Parent PID: 2592

General

Start time:	17:38:18
Start date:	13/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2592 CREDAT:17410 /prefetch:2
Imagebase:	0x380000
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

Disassembly

Copyright null 2021