Confidential Information

Intended for Internal Use Only

Sample Report

ad8ff52301c0ef4c30fb5b08899168aa

72
Threat Score

Metadata

Sample ID	ad8ff52301c0ef4c30fb5b08899168aa	Filename	fallible.url
Magic Type	MS Windows 95 Internet shortcut text (URL=<http://fallibleliving.com/>), ASCII text	SHA-256	423f3dac5c40a04f05fc33d0b33b6fa8a524c2b23a3df8b0bc141425a72bb224
Started	Wed, 7 Jun 2023 15:48:03 GMT	SHA-1	36440efed580bedcd86dc362cbdbc0ca9549e19a
Ended	Wed, 7 Jun 2023 15:55:28 GMT	MD5	12563e9c4e538da39c89756a2b435e6f
File Type	url	OS	Windows 10 Browser
Duration	0:07:25	Access	Private

Table of Contents

Warnings

back to table of contents

TLS Stream Not Decrypted

network stream 11: unsupported cipher suite; network stream 13: unsupported cipher suite; network stream 15: unsupported cipher suite; network stream 16: unsupported cipher suite; network stream 17: unsupported cipher suite; network stream 18: unsupported cipher suite; network stream 20: unsupported cipher suite; network stream 21: unsupported cipher suite; network stream 23: unsupported cipher suite; network stream 25: unsupported cipher suite; network stream 26: unsupported cipher suite; network stream 29: unsupported cipher suite; network stream 32: unsupported cipher suite

Behavioral Indicators

back to table of contents

Title	Categories	Tags	Hits	Score
An HTML or JavaScript with Excessive Amount of JavaScript Function Definitions	Static-anomaly	Phishing, Html, Javascript	1	72

Description

An HTML or JavaScript file references an excessive amount of function definitions. This is very commonly seen in phishing attempts.

Title	Categories	Tags	Hits	Score
Page Not Found HTML Error Page Detected.	Static-anomaly	Html, Redirect	1	70

Description

A 'Page Not Found' HTML error page was detected. This is not malicious by itself, but it is very often seen alongside malicious links which reference missing content that has possibly been removed or cleaned up by previously compromised hosts.

Title	Categories	Tags	Hits	Score
JavaScript in HTML Uses Location.Replace Function	Macros	Javascript, Html, Window, Redirect	1	67

Description

A JavaScript code segment was discovered in an HTML artifact that uses the location.replace() method. The browser JavaScript guidelines state that this function is used to change the current browser location. However, using this function does not preserve the current page in the history log and therefore its use is often discouraged. Legitimate uses include acting as a soft redirect or when moving through certain web forms. This function is used less often, as many browsers encourage the use of tabs. Malware may use this to redirect through a page or series of pages which perform stages of an attack.

Title	Categories	Tags	Hits	Score
JavaScript Contains an Excessively Long String	Obfuscation	Javascript, Obfuscation	2	64

Description

A JavaScript code segment was discovered that uses a string in excess of one kilobyte. Excessively long strings are allowable within scripting languages, though they tend not to be common, as they can become difficult to read. Very long strings could be an indication of a generic output. In malware, these excessively long strings may be encoded binaries or obfuscated code.

Title	Categories	Tags	Hits	Score
Script Contains URL	Attribute	Js, Vbs, Url	7	60

Description

A JavaScript or VBScript was discovered that contains a Universal Resource Locator (URL). The script has a URL encoded within it. This is not necessarily malicious. Legitimate macros may have a URL in a comment to state where it came from. Malware may use this URL to download the next stage of an attack.

Title	Categories	Tags	Hits	Score
JavaScript Using "toString" Method	Static	Javascript	7	56

Description

A JavaScript file was found which makes use of the "toString" method. This method in JavaScript code returns a string representing the object. While the use of this function by itself does not necessarily indicate malicious intent, it is commonly used as an obfuscation technique.

Title	Categories	Tags	Hits	Score
Static Analysis Flagged Artifact As Potentially Obfuscated	Obfuscation	Obfuscation, Static	8	56

Description

A static analysis rule identified an artifact containing known obfuscation techniques. Malware may use these to evade static analysis scans for sensitive material and slow manual analysis.

Title	Categories	Tags	Hits	Score
JavaScript Calls ActiveXObject	Obfuscation	Javascript, Suspicious, Forensics	5	48

Description

JavaScript instantiated an ActiveX object using the "ActiveXObject" method. The use of ActiveX has been declining in recent years due to incompatibility across browsers, security concerns and advent of HTML5. However, ActiveX objects are often used in JavaScript malware. Therefore, its presence in a JavaScript file is suspicious.

Title	Categories	Tags	Hits	Score
HTML Contains JavaScript Using 'eval()' Function	Macros	Html, Javascript, Stream, Obfuscation	1	48

Description

An HTML file with embedded JavaScript was found which makes use of the 'eval' method. This method interprets JavaScript code from a provided string or variable. This method allows malware to use string obfuscation techniques to obfuscate its true intent and dynamically create JavaScript from the obfuscated code. However, the use of this function by itself does not necessarily indicate malicious intent.

Title	Categories	Tags	Hits	Score
Static Analysis Flagged Artifact As Anomalous	Static-anomaly	Anomaly, Static	12	48

Description

A static analysis rule identified an artifact that has one or more anomalous characteristics. These anomalies may exist due to flaws in the file generation or misunderstandings of the format. Malware may use file anomalies to confuse antivirus parsers and hide code in unusual locations.

Title	Categories	Tags	Hits	Score
JavaScript In HTML Or HTA File Calls ActiveXObject	Obfuscation	Javascript, Suspicious, Forensics	1	48

Description

JavaScript instantiated an ActiveX object using the "ActiveXObject" method. The use of ActiveX has been declining in recent years due to incompatibility across browsers, security concerns and the advent of HTML5. However, ActiveX objects are often used in JavaScript malware. Therefore, its presence in an HTML or HTA file is suspicious.

Title	Categories	Tags	Hits	Score
JavaScript Obfuscation Using "fromCharCode()" Function	Obfuscation	Javascript, Stream, Obfuscation	2	40

Description

A JavaScript file was found which makes use of the ".fromCharCode()" method of the "String" object. It is used to convert Unicode values into characters. Malware may use this as a means of simple obfuscation.

Title	Categories	Tags	Hits	Score
JavaScript Obfuscation Using "eval()" Function	Obfuscation	Javascript, Stream, Obfuscation	3	40

Description

A JavaScript file was found which makes use of the "eval" method. This method evaluates JavaScript code from a provided string. This method allows malware to use string obfuscation techniques to obfuscate its true intent and dynamically create JavaScript from the obfuscated code. However, the use of this function by itself does not necessarily indicate malicious intent.

Title	Categories	Tags	Hits	Score
HTTP Redirection Response	Network-information	Network, Http, Redirect	1	25

Description

An HTTP message indicating a redirection notice was detected in a network stream. The HTTP response codes are used as a means of conveying the status of the connection with the server to the client. Items within the 300 range indicate a redirection notice. These occur when a page has been temporarily or permanently moved.

Title	Categories	Tags	Hits	Score
Sample Communicates With Only Benign Domains	Domain	Umbrella, Dns	2	19

Description

The sample contacted only benign or likely benign domains. It is unlikely that malware will download malicious content from such sites. Note that this indicator considers only domains with which data was actually exchanged, simply resolving or referencing them will not have an influence on triggering.

Title	Categories	Tags	Hits	Score
DNS Response Contains Low Time to Live (TTL) Value	Domain	Network, Ttl, Dns, Fast flux, Command and control	3	7

Description

DNS responses with low time-to-live values is a technique used by botnets to maintain a resilient command and control infrastructure of compromised hosts acting as proxies. Also known as Fast Flux, this behavior is characterized by multiple individual nodes within the network registering and de-registering their addresses as part of the DNS A record list for a DNS name. Each record has a very short TTL (time to live) value of usually less than five minutes. This creates a constantly changing list of destination addresses for a single DNS name. Please view the 'DNS' section under 'Network Analysis' for the associated traffic/communications. Additionally, the provided network PCAP will provide more details on the traffic stream.

Title	Categories	Tags	Hits	Score
Outbound HTTP GET Request From URL Submission	Network-information	Network, Http, Get	1	6

Description

Outbound HTTP GET to a remote server was detected. This is not inherently suspicious but malware will often use Gets in order to check in to the Command and Control servers upon infection or to download or exfiltrate data. Please view the 'HTTP' section under 'Network Analysis' for the associated traffic/communications. Additionally, the provided network PCAP will provide more details on the traffic stream.

TCP/IP Streams

back to table of contents

Stream	Timestamp	Process	Src. IP	Src. Port	Dest. IP	Dest. Port	Reverse Lookup	ASN	Location	Snort Hits	Transport	Artifacts	Packets	Bytes
0	+42.195s		0.0.0.0	68	255.255.255.255	67				0	UDP	0	2	657
1	+42.196s		192.168.1.11	68	192.168.1.1	67				0	UDP	0	2	664
2	+42.283s		192.168.1.11	137	192.168.1.255	137				0	UDP	0	19	1770
3	+42.898s		192.168.1.11	49664	239.255.255.250	3702				0	UDP	0	4	4416
4	+48.498s		192.168.1.11	138	192.168.1.255	138				0	UDP	0	13	2747
5	+116.842s		192.168.1.11	137	192.168.1.255	137				0	UDP	0	8	768
6	+147.535s		192.168.1.11	61923	192.168.1.1	53				0	UDP	0	2	195
7	+147.657s		192.168.1.11	61924	239.255.255.250	1900				1	UDP	0	4	808
8	+148.03s		192.168.1.11	50870	192.168.1.1	53				0	UDP	0	2	196
9	+148.847s		192.168.1.11	50083	192.168.1.1	53				0	UDP	0	2	165
10	+149.737s	24	192.168.1.11	49670	104.21.48.20	80			, , US	0	TCP	1	7	2190
11	+149.932s	24	192.168.1.11	49671	142.251.40.195	443	lga34s38-in-f3.1e100.net		Philadelphia, PA, US	0	TCP	0	21	6126
12	+150.81s	24	192.168.1.11	49672	104.21.48.20	80			, , US	0	TCP	0	8	344
13	+150.965s	24	192.168.1.11	49673	142.251.40.195	443	lga34s38-in-f3.1e100.net		Philadelphia, PA, US	0	TCP	0	21	6125
14	+151.323s		192.168.1.11	49674	104.21.48.20	80			, , US	0	TCP	0	7	304
15	+151.432s	24	192.168.1.11	49675	142.250.176.205	443	lga34s37-in-f13.1e100.net		, , US	0	TCP	0	18	5643
16	+153.706s	24	192.168.1.11	49676	142.250.176.205	443	lga34s37-in-f13.1e100.net		, , US	0	TCP	0	13	5443
17	+163.789s	24	192.168.1.11	49677	104.21.48.20	443			, , US	0	TCP	0	322	305419
18	+177.368s	24	192.168.1.11	49678	142.250.176.205	443	lga34s37-in-f13.1e100.net		, , US	0	TCP	0	24	8727
19	+187.042s		192.168.1.11	57148	192.168.1.1	53				0	UDP	0	2	168
20	+188.071s	24	192.168.1.11	49679	142.251.40.234	443	lga34s39-in-f10.1e100.net		Philadelphia, PA, US	0	TCP	0	29	11990
21	+191.201s	24	192.168.1.11	49680	142.251.40.234	443	lga34s39-in-f10.1e100.net		Philadelphia, PA, US	0	TCP	0	16	6539
22	+192.238s		192.168.1.11	53301	192.168.1.1	53				0	UDP	0	2	159

Stream	Timestamp	Process	Src. IP	Src. Port	Dest. IP	Dest. Port	Reverse Lookup	ASN	Location	Snort Hits	Transport	Artifacts	Packets	Bytes
23	+193.042s	24	192.168.1.11	49681	142.250.80.67	443	lga34s35-in-f3.1e100.net		Staten Island, NY, US	0	TCP	0	51	38312
24	+213.608s		192.168.1.11	52806	192.168.1.1	53				0	UDP	0	2	129
25	+213.775s	24	192.168.1.11	49682	192.0.77.48	443	s.w.org		San Francisco, CA, US	0	TCP	0	33	12930
26	+213.828s	24	192.168.1.11	49683	192.0.77.48	443	s.w.org		San Francisco, CA, US	0	TCP	0	26	11889
27	+264.197s		192.168.1.11	5353	224.0.0.251	5353				0	UDP	0	2	136
28	+268.951s		192.168.1.11	62601	192.168.1.1	53				0	UDP	0	2	171
29	+273.063s	24	192.168.1.11	49684	142.251.35.163	443	lga25s78-in-f3.1e100.net		, TX, US	0	TCP	0	33	17720
30	+322.415s		192.168.1.11	5353	224.0.0.251	5353				0	UDP	0	1	68
31	+326.965s		192.168.1.11	59025	192.168.1.1	53				0	UDP	0	2	284
32	+331.449s	24	192.168.1.11	49685	142.250.65.225	443	lga25s73-in-f1.1e100.net		Philadelphia, PA, US	0	TCP	0	97	106348

Processes

back to table of contents

Process	Name	Parent	Children	File actions	Registry Actions	Analysis Reason
1	Explorer.EXE	61	0	0	5	Process activity after target sample started.
9	chrome.exe		8	58	16	Is target sample.
13	chrome.exe	9 (chrome.exe)	0	4	0	Parent is being analyzed
18	svchost.exe	49	0	0	0	Process activity after target sample started.
19	svchost.exe		0	0	0	Process activity after target sample started.
22	svchost.exe	49	0	0	0	Process activity after target sample started.
23	chrome.exe	9 (chrome.exe)	0	0	0	Parent is being analyzed
24	chrome.exe	9 (chrome.exe)	0	34	2	Parent is being analyzed
25	chrome.exe	9 (chrome.exe)	0	0	0	Parent is being analyzed
27	RuntimeBroker.exe	53	0	0	0	Process activity after target sample started.
28	dwm.exe	52	0	0	0	Process activity after target sample started.
29	chrome.exe	9 (chrome.exe)	0	0	0	Parent is being analyzed
30	chrome.exe	9 (chrome.exe)	0	0	0	Parent is being analyzed
31	chrome.exe	9 (chrome.exe)	0	0	0	Parent is being analyzed
32	wmiprvse.exe	53	0	0	0	Process activity after target sample started.
35	chrome.exe	9 (chrome.exe)	0	0	0	Parent is being analyzed
39	chrome.exe	37	0	0	1	Process activity after target sample started.
40	chrome.exe	37	0	0	2	Process activity after target sample started.
41	chrome.exe	37	0	0	0	Process activity after target sample started.
47	svchost.exe	508	0	0	0	

Artifacts

back to table of contents

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
1	fallible.url	423f3dac5c40a04f05fc33d0b33b6fa8a524c2b23a3df8b0bc141425a72bb224	0	submitted		50	0	0
2	\TEMP\fallible.url	423f3dac5c40a04f05fc33d0b33b6fa8a524c2b23a3df8b0bc141425a72bb224	0	disk		50	0	0
3	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\82eda46a-8215-4eea-985b-b96318534024.tmp	0f376600fa067def492d654e801022b178510398219ea04682c4d0f2c8eab5ab	0	disk	Process 24	367	0	0
4	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\9cb99e6c-0aff-426f-9274-e8023fd071ca.tmp	11eb5f5560ad29cf783b1a7f7c5473f7ef93a057e282bee0855289f566479818	0	disk	Process 24	220	0	0
5	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7c8ddfbcd2b8704_0	6a0b723d2c19fa901219b4c1854c7966c3086aa42467ee23752a18abfecd7c55	0	disk		237	0	0
6	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\History	8931744884f3d9fa0a7bdbcd6491e06cc135d7ed8d32aea5ad48ce26f799a38d	0	disk		126976	0	0
7	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	8484763be91ba0373508e4d86bf4b05cdd0363550f86cd0222d44698ca60e562	0	disk	Process 9	346	0	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
8	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old	1962fd3a84da7c4c8d5bca6ee936a0b120dee779d61f455e621660198359b1ce	0	disk	Process 9	346	0	0
9	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Network Action Predictor	4b074c4dabcd0dbe5144bff46fdfba97d0a565bafcf73cebd8abef0d18004be4	0	disk		155648	0	0
10	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	64ef802220ec1d7034736a0c0576bad9b490067ed513def406f14c26104be314	0	disk	Process 9	333	0	0
11	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old	f5307ffbd124976578db81a1049290cefe7fa51bf7bb49afe721fc77c1e664db	0	disk	Process 9	333	0	0
12	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13330626552375856	b3f55a6137cc127a8ef2fcc9a6076ada21ed6ac876a5ab3e66dc99ad32ff2474	0	disk	Process 9	48837	0	0
13	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Shortcuts	1bfd49438d3bc944519326bc99f24e78a453e3060b73e27217af2dcb74cb7375	0	disk		20480	0	0
14	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\data_0	6b114b61902d560d80d38294637389913a1d1ed2e2fcbff1a7ab92ece4af9dda	0	disk	Process 24	45056	0	0
15	\Windows\System32\umstartup.etl\32b586c.rbf\data_1	aa4bf56ff65f382f1fce76b82cd2ede642095de17e44c9d5e69e962f89d271a2	0	disk		270336	0	0
16	\Windows\System32\umstartup.etl\32b586c.rbf\data_2	87cfbdf18e369ade5ca6bc4ce85d3628ce560581a071c028dc6c9f609ee53e0a	0	disk		1056768	0	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
17	\Windows\System32\umstartup.etl\32b586c.rbf\data_3	8c012da4605915248fc2c7c83675dfb4514bed32d157345fbad74dacc793065f	0	disk		4202496	0	0
18	\Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx	2b6be8ada8a3c8f589ff50904f6286b5abaee7652403a676814bdc64faead40d	0	disk		1052672	0	0
19	\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx	b868542e5499274361fd5f9f1ee547e4761b8045ab17f62c007d9b19e6ebbf7e	0	disk		69632	0	0
20	\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx	80b835edc973344d8c1f4cd8ad29095c6337da227e815c7106b1d2a8dc708c01	0	disk		69632	0	0
21	\Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Operational.evtx	d79de2b61d74851efa4d3fb35783f7a018f65b72e10e1b649e5ad75c481f3877	0	disk		1052672	0	0
22	\Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Operational.evtx	89298f9a9b7dcc76e8d8208445cb6c411a28345c3ff177486c614137cb0cee36	0	disk		1118208	0	0
23	\Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx	9fae3c0edd7c03704c941a2ff60861c0bc2d16bde0f98f1de42719277afa00a6	0	disk		1118208	0	0
24	\Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx	2d71936ba517a7562ca824781e3616f83f130126ef413f42152eefc15e33bad0	0	disk		1052672	0	0
25	1488-svchost.exe	dd90898035ae568b860d2f2fb0ab7671ffd40bf309b955af36a15858497a914d	0	memory		34816	100	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
26	1520-chrome.exe	bd147289cfc4f76bc135891d8f1ff3c7ee3a3dc01a97158fbe8d946f4b826bbc	0	memory		2240512	100	3
27	1576-chrome.exe	bb1057ddcdc17764b864b0e6bc96c7ebf37afa68f38933ac8a75bb20e5aa8de4	0	memory		2240512	100	3
28	2192-wmiprvse.exe	8add19c52656e9ace11ee7f1989206013e8aef74a71724aa9bb3587cb752d990	0	memory		504832	100	0
29	2292-chrome.exe	2cf7cef3f0fa7e08de6f0b4cb69402917fb040db5e1ee9ffa6c0d576549022a8	0	memory		2240512	100	3
30	2520-chrome.exe	8a0320633a8261f5d7516e29832eba5f68cec0d0c613917d959ced56cec53b17	0	memory		2240512	100	3
31	2672-chrome.exe	2c37b808c9174ae10058d6f262e1b453f37a78c46c861ef4236fb98dbab0b032	0	memory		2240512	100	3
32	2692-chrome.exe	7ddb5074bb7565ad8e8c2c2571eb0ec0220aec5770851f6335e02cb9cbd0d3e5	0	memory		2240512	100	3
33	2724-chrome.exe	2e0b78be93c0c19dce2702dec3e55d3bbf63afb93732c9171cd8caf55ef53ce2	0	memory		2240512	100	3
34	2872-chrome.exe	bb886d02ee6999ca34a1377b433b183ace2331419de5470787474c9c82105423	0	memory		2240512	100	3
35	2888-chrome.exe	0d1a1bab54678683d170ed88f31e1f6cff678449eb3328eb6dd7cb67380bd310	0	memory		2240512	100	3

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
36	3040-chrome.exe	b7e3792fdb359cc35c612910734ec26bac9ccaf6e090932432920665 19a448fa	0	memory		2240512	100	3
37	\users\administrator\appdata\local\google\chrome\user data\default\sessions\tabs_13272048940376722	38aaab704fc00f4b5124b8f73f7e2ecbea2e50a2f63dc8144f4952fc4a7892c3	0	disk		64536	0	0
38	\users\administrator\appdata\local\google\chrome\user data\default\sessions\session_13272048940282722	14b4eeb552c620e44ae0b82da8f7fa212cbbe8419d6b359032bc2f5be3a7a13a	0	disk		984	0	0
39	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003	52d7e7467318fe5852eb10d7ebc81649a63bdaa1daa138df2fb1afb9d3436b23	0	disk	Process 63	36356	0	0
40	\users\administrator\appdata\local\google\chrome\user data\browsermetrics\browsermetrics-6102cec1-b8c.pma	bb9f8df61474d25e71fa00722318cd387396ca1736605e1248821cc0de3d3af8	0	disk		4194304	0	0
41	\users\administrator\appdata\local\google\chrome\user data\browsermetrics\browsermetrics-6102d422-90c.pma	05d27498dfd7cbb7c3a2deab0101c25f19d97c8e2c393239a5b50746aeb38639	0	disk		4194304	0	0
42	\users\administrator\appdata\local\google\chrome\user data\browsermetrics\browsermetrics-6102d427-b48.pma	649cec2fe8575bb88a6c58d6e39ac7e6e89c035db001258fcc2f1f2e571d53fa	0	disk		4194304	0	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
43	\users\administrator\appdata\local\google\chrome\user data\browsermetrics\browsermetrics-6102d42c-b04.pma	a656a7ea2e2639c33104d5a11f86cf2f3ebebe5af2c1ea107c2508baa8781300	0	disk		4194304	0	0
44	\users\administrator\appdata\local\google\chrome\user data\browsermetrics\browsermetrics-628cf28e-ad0.pma	ce4786192783010612 8c08802925b6880f64e cb2a31ec977774ee7fb b9ad4a4e	0	disk		4194304	0	0
45	\users\administrator\appdata\local\google\chrome\user data\browsermetrics\browsermetrics-6480a6f6-a84.pma	bb9f8df61474d25e71f a00722318cd387396c a1736605e1248821cc 0de3d3af8	0	disk		4194304	0	0
46	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004	d7e07319bfd12ba45e4 ce170bddcbd3231618 309a0c0df40f03b5a8b 8c391638	0	disk	Process 64	35708	0	0
47	\users\administrator\appdata\local\google\chrome\user data\chrome_shutdown_ms.txt	6596c0e0815319857f9 08f92e314541495d58 57282a1aaae49253cf2 25ef4047	0	disk		4	0	0
48	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005	84c7ca8902d9bc611bf 437ff5ff34406cce4028 1e41603e991d457f43a 99966c	0	disk	Process 65	18980	0	0
49	\users\administrator\appdata\local\google\chrome\user data\subresource filter\indexed rules\27\9.27.0\ruleset data	0f58b5d6f89bffe34a44 803f70aefd5a435abd6 92fdd00d3b1c885759 33ba752	0	disk		197616	0	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
50	\users\administrator\appdata\local\google\chrome\user data\default\history provider cache	d6f83bff16a850d31437ce5f6abd9cd9d9152359faf5c04351ece08c28a23228	0	disk		9707	0	0
51	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	0e1970ccbabf2f766f8736de4b4bca09886d82f30d4e682455bbb6e7280ec149	0	disk	Process 66	230254	0	0
52	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000007	957e3d17407eed8406466e7a738276f52b4a76f23cf80e8f839b7561c53d645c	0	disk		17378	0	0
53	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000008	1cf04407e728ea1ebf82dc1c6b45d12632cb3202ff8f4556f380b16e57484f27	0	disk		21552	0	0
54	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000009	f2c761ee3ce27469f940a05b64e38a829a400427727cd0bdbb4e36f1d572afd7	0	disk		21716	0	0
55	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a	5b030993686f7f33b2d7b63e38cb045dd18b70dc6f261d6d56a01d1183726dba	0	disk	Process 67	36854	0	0
56	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b	841a2999f024457388333ced34d9d9038a3ad9a74d3ab798f98da854caa838a4	0	disk	Process 68	26171	0	0
57	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000c	d7e07319bfd12ba45e4ce170bddcbd3231618309a0c0df40f03b5a8b8c391638	0	disk	Process 64	35708	0	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
58	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d	8dccf8c405e0d35df7034cbae96d5db92d9b08c1f3677c34c65f5efd8d69b3af	0	disk	Process 69	73051	0	0
59	\users\administrator\appdata\local\google\chrome\user data\default\history provider cache	d6f83bff16a850d31437ce5f6abd9cd9d9152359faf5c04351ece08c28a23228	0	disk		9707	0	0
60	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000e	91df30176742931 56a79dc6bc03fe0f98ea2644a2e1e82d220820ae1d13eeb14	0	disk	Process 70	102642	0	0
61	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f	1c4228ce901f278eb90a83e7f4de20da8a6a1867b367b601fff00d0df04c0326	0	disk	Process 71	17985	0	0
62	http-fallibleliving.com-80-10-1	3bbe72f3baa8ec61de17a1d767fca58704769684b7abe9161d0c4eaf4c8f0982	0	network	Process 10	707	0	0
63	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003	3c039c07f705f3e4f4f980dc9e75cd10f8260ea1323ce73dd3b54f80e4ae1588	0	extracted	Process 39	100100	0	0
64	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004	66732d29f4cb8058c3ca53d3b673dd97c36eec63ed101bbe81a316163d60edad	0	extracted	Process 46	104027	0	0
65	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005	0f3be44690ae9914ae3e47b7752e1bdea316f09938e9094f99e0de19ccd8987a	0	extracted	Process 48	47332	0	0
66	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	0	extracted	Process 51	761938	0	0

Artifact	Path	SHA-256	AV Sigs	Source	Most Relevant	Size	Imports	Exports
67	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a	a3416d7f5581d355a241e2c9cce05d8b3acaa8b5e19ffec414ab003fd6f45130	0	extracted	Process 55	102162	0	0
68	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b	d5943651 2c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	0	extracted	Process 56	72511	0	0
69	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	0	extracted	Process 58	212527	0	0
71	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f	dccef0a18cc6701fef6084b76fb924c24266bd35b899bceefbf3af93e85ed3d8	0	extracted	Process 61	51532	0	0

Registry Keys (Consolidated)

back to table of contents

Key	Activity
USER\S-1-5-21-3467368655-986044752-3166994390-500	created (4)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SESSIONINFO\1\APPLICATIONVIEWMANAGEMENT\W32:0000000000006013C	created (1), modified (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SESSIONINFO\1\APPLICATIONVIEWMANAGEMENT\W32:0000000000090232	deleted (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\HOMEGROUP\UISTATUSCACHE	deleted (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SESSIONINFO\1\APPLICATIONVIEWMANAGEMENT\W32:0000000000090140	deleted (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\THIRDPARTY	modified (2)
MACHINE\SOFTWARE\WOW6432NODE\GOOGLE\UPDATE\CLIENTSTATEMEDIUM\{8A69D345-D564-463C-AFF1-A69D9E530F96}\FIRSTNOTDEFAULT	modified (1)
MACHINE\SOFTWARE\WOW6432NODE\GOOGLE\UPDATE\CLIENTSTATEMEDIUM\{8A69D345-D564-463C-AFF1-A69D9E530F96}\LASTWASDEFAULT	modified (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\BLBEACON	modified (3)
MACHINE\SOFTWARE\WOW6432NODE\GOOGLE\UPDATE\CLIENTSTATEMEDIUM\{8A69D345-D564-463C-AFF1-A69D9E530F96}	modified (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME	modified (1)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\UPDATE\CLIENTSTATE\{8A69D345-D564-463C-AFF1-A69D9E530F96}	modified (5)
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\STABILITYMETRICS	modified (1)

Key	Activity
USER\S-1-5-21-3467368655-986044752-3166994390-500_CLASSES\LOCAL SETTINGS\MUICACHE\28\52C64B7E	modified (2)

Created Keys

back to table of contents

Created Key	Process	Access List	Options List
USER\S-1-5-21-3467368655-986044752-3166994390-500	9 (chrome.exe)	CREATE_SUB_KEY, ENUMERATE_SUB_KEYS, NOTIFY, QUERY_VALUE, READ_CONTROL, SET_VALUE, WOW64_32KEY	REG_OPTION_NON_VOLATILE
USER\S-1-5-21-3467368655-986044752-3166994390-500	24 (chrome.exe)	QUERY_VALUE, SET_VALUE	REG_OPTION_NON_VOLATILE
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SESSIONINFO\1\APPLICATIONVIEWMANAGEMENT\W32:000000000006013C	1 (Explorer.EXE)	CREATE_SUB_KEY, READ_CONTROL, SET_VALUE	REG_OPTION_VOLATILE
USER\S-1-5-21-3467368655-986044752-3166994390-500	39 (chrome.exe)	QUERY_VALUE, SET_VALUE	REG_OPTION_NON_VOLATILE
USER\S-1-5-21-3467368655-986044752-3166994390-500	40 (chrome.exe)	QUERY_VALUE, SET_VALUE	REG_OPTION_NON_VOLATILE

Modified Keys

back to table of contents

Modified Key	Process	Value Name	Data
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\THIRDPARTY	9 (chrome.exe)	StatusCodes	
MACHINE\SOFTWARE\WOW6432NODE\GOOGLE\UPDATE\CLIENTSTATEMEDIUM\{8A69D345-D564-463C-AFF1-A69D9E530F96}\FIRSTNOTDEFAULT	9 (chrome.exe)	S-1-5-21-3467368655-986044752-3166994390-500	
MACHINE\SOFTWARE\WOW6432NODE\GOOGLE\UPDATE\CLIENTSTATEMEDIUM\{8A69D345-D564-463C-AFF1-A69D9E530F96}\LASTWASDEFAULT	9 (chrome.exe)	S-1-5-21-3467368655-986044752-3166994390-500	
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\THIRDPARTY	9 (chrome.exe)	StatusCodes	AQAAAA==
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\BLBEACON	9 (chrome.exe)	failed_count	0
MACHINE\SOFTWARE\WOW6432NODE\GOOGLE\UPDATE\CLIENTSTATEMEDIUM\{8A69D345-D564-463C-AFF1-A69D9E530F96}	9 (chrome.exe)	usagestats	0
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME	9 (chrome.exe)	UsageStatsInSample	0
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\UPDATE\CLIENTSTATE\{8A69D345-D564-463C-AFF1-A69D9E530F96}	9 (chrome.exe)	metricsid_installdate	0
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\UPDATE\CLIENTSTATE\{8A69D345-D564-463C-AFF1-A69D9E530F96}	9 (chrome.exe)	lastrun	13330626554588237
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\BLBEACON	9 (chrome.exe)	state	1
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\UPDATE\CLIENTSTATE\{8A69D345-D564-463C-AFF1-A69D9E530F96}	9 (chrome.exe)	metricsid	

Modified Key	Process	Value Name	Data
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\STABILITYMETRICS	9 (chrome.exe)	user_experience_metrics.stability.exited_cleanly	0
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\UPDATE\CLIENTSTATE\{8A69D345-D564-463C-AFF1-A69D9E530F96}	9 (chrome.exe)	metricsid_enableddate	0
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\CHROME\BLBEACON	9 (chrome.exe)	state	2
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\GOOGLE\UPDATE\CLIENTSTATE\{8A69D345-D564-463C-AFF1-A69D9E530F96}	9 (chrome.exe)	dr	1
USER\S-1-5-21-3467368655-986044752-3166994390-500_CLASSES\LOCAL SETTINGS\MUICACHE\28\52C64B7E	24 (chrome.exe)	LanguageList	en-USen
USER\S-1-5-21-3467368655-986044752-3166994390-500\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\SESSIONINFO\1\APPLICATIONVIEWMANAGEMENT\W32:000000000006013C	1 (Explorer.EXE)	VirtualDesktop	EAAAADAwRFb0BwKtsB1qQ5DP0vmf3UYC
USER\S-1-5-21-3467368655-986044752-3166994390-500_CLASSES\LOCAL SETTINGS\MUICACHE\28\52C64B7E	40 (chrome.exe)	LanguageList	en-USen

File Activity

back to table of contents

Process	Action	Path
9 (chrome.exe)	Checked	\DEVICE\NETBT_TCPIP_{59C4E170-D253-11E5-BDC2-806E6F6E6963}
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\a3b26927-50fd-441d-b329-427b33e57129.tmp
9 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Address Validation Rules
9 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\BrowserMetrics-spare.pma
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-6480A6F6-A84.pma
9 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\BrowserMetrics\BrowserMetrics-6480A6F6-A84.pma
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\1c25b26a-3241-42f7-9cb4-cc5703b81573.tmp
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\1c25b26a-3241-42f7-9cb4-cc5703b81573.tmp
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\5791aa7d-5c07-48f9-93af-c7992ca0fff6.tmp
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\a772779c-e7a3-43b0-9dc6-448c7513ee90.tmp
9 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Custom Dictionary.txt
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF9ff755e4.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF9ff755e4.TMP
9 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\File System\primary.origin

Process	Action	Path
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old~RF9ff74356.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old~RF9ff74356.TMP
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old~RF9ff7302c.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old~RF9ff7302c.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Preferences
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF9ff73378.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF9ff73378.TMP
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF9ff75a59.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF9ff75a59.TMP
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\LOG.old~RF9ff7305b.TMP

Process	Action	Path
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Service Worker\Database\LOG.old~RF9ff7305b.TMP
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RF9ff743c4.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RF9ff743c4.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13272048940282722
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sessions\Session_13330626551688856
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13272048940376722
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sessions\Tabs_13330626552375856
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RF9ff724c2.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RF9ff724c2.TMP
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RF9ff72510.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RF9ff72510.TMP

Process	Action	Path
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old~RF9ff75306.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old~RF9ff75306.TMP
9 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Trusted Vault
9 (chrome.exe)	Modified	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Last Version
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State~RF9ff74942.TMP
9 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Local State~RF9ff74942.TMP
9 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\lockfile
9 (chrome.exe)	Modified	\Users\Administrator\AppData\Local\Temp\2cc8d5c5-c00f-4fc0-9585-3073a024ccea.tmp
9 (chrome.exe)	Modified	\Users\Administrator\AppData\Local\Temp\3439ad56-e696-4880-af1c-9b0f4c10a1d2.tmp
9 (chrome.exe)	Modified	\Users\Administrator\AppData\Local\Temp\7b712d8d-32ef-4387-bcf9-11860a59370a.tmp
9 (chrome.exe)	Created	\Users\ADMINI~1\AppData\Local\Temp\2cc8d5c5-c00f-4fc0-9585-3073a024ccea.tmp
9 (chrome.exe)	Created	\Users\ADMINI~1\AppData\Local\Temp\3439ad56-e696-4880-af1c-9b0f4c10a1d2.tmp
9 (chrome.exe)	Created	\Users\ADMINI~1\AppData\Local\Temp\7b712d8d-32ef-4387-bcf9-11860a59370a.tmp

Process	Action	Path
24 (chrome.exe)	Checked	\DEVICE\NETBT_TCPIP_{59C4E170-D253-11E5-BDC2-806E6F6E6963}
24 (chrome.exe)	Checked	\Device\RasAcd
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\82eda46a-8215-4eea-985b-b96318534024.tmp
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\9cb99e6c-0aff-426f-9274-e8023fd071ca.tmp
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\data_0
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000001
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000002
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Cache\index
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State~RF9ff7a28d.TMP
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State~RF9ff7a28d.TMP
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\data_0
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\data_1

Process	Action	Path
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\data_2
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\data_3
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000003
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000004
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000005
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000006
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000007
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000008
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_000009
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_00000a
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_00000b
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_00000c
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_00000d
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_00000e
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\old_Cache_000\f_00000f
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity
24 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity~RF9ff7a0b9.TMP
24 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity~RF9ff7a0b9.TMP

Process	Action	Path
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\24BD96D5497F70B3F510A6B53CD43F3E_3A89246FB90C5EE6620004F1AE0EB0EA
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\24BD96D5497F70B3F510A6B53CD43F3E_50E5641F4A1A13E8A8C9935375B2CC3A
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\3C523155507C9096C34DE70913E2CA08
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4748633DC5731827D4B432DBAC7A3ECE
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\572BF21E454637C9F000BE1AF9B1E1A9
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\646C991C2A28825F3CC56E0A1D1E3FA9
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\70DAE932E3BCB3C00656A27B544BA9CA
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\87845598FFD4CEA35D62EF090FCB1653
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\892BD135CF0BA5A31C6B8A7554540845
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_2E5FB3DF55F6A1FE946987C264867A14
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_89854CA6A0F0936A4D2ECA78845CEA25
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAF4703619713E3F18D8A9D5D88D6288_A7725538C46DE2D0088EE44974E2CEBA
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAF4703619713E3F18D8A9D5D88D6288_B06877B42FB9C16CBD891F59CEE20302

Process	Action	Path
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAF4703619713E3F18D8A9D5D88D6288_CD1122F18E4775F3E03AF8494FF24E2A
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAF4703619713E3F18D8A9D5D88D6288_F2DAF19C1F776537105D08FC8D978464
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D0E1C4B6144E7ECAB3F020E4A19EFC29_0CF5D547EE14BE7C672D39412B9C1C45
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D0E1C4B6144E7ECAB3F020E4A19EFC29_B5F77004C894173A10E3A199871D2D90
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F07644E38ED7C9F37D11EEC6D4335E02_074F77B302B084C9682372CF584D65BA
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F07644E38ED7C9F37D11EEC6D4335E02_44F0D418403D3C084D11F31F84524B38
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F07644E38ED7C9F37D11EEC6D4335E02_D4D5A511944208643D9E0DD4100257E2
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F07644E38ED7C9F37D11EEC6D4335E02_E967084282EA9223CC430E56F1470429
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F2DDCD2B5F37625B82E81F4976CEE400_17BFCC0C3436C37AB912079E4A6C400B
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F2DDCD2B5F37625B82E81F4976CEE400_2195A4DB0E815BF9F8093B4E7B4E72B7
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F2DDCD2B5F37625B82E81F4976CEE400_600B23BA858839DB61075D23CA8AB395
24 (chrome.exe)	Checked	\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F2DDCD2B5F37625B82E81F4976CEE400_DEF74B87E9716FF4F8A2FB1A0403D9C8
23 (chrome.exe)	Checked	\Program Files\Google\Chrome\Application\88.0.4324.104\SwiftShader.ini

Process	Action	Path
13 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma
13 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-active.pma
13 (chrome.exe)	Checked	\Users\Administrator\AppData\Local\Google\Chrome\User Data\CrashpadMetrics-spare.pma
13 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma
13 (chrome.exe)	Created	\Users\Administrator\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma~RF9ff71d31.TMP
13 (chrome.exe)	Deleted	\Users\Administrator\AppData\Local\Google\Chrome\User Data\CrashpadMetrics.pma~RF9ff71d31.TMP
27 (RuntimeBroker.exe)	Checked	\Users\Administrator\AppData\Roaming\Microsoft\Spelling\en\
32 (wmiprvse.exe)	Checked	\Windows\system32\OemInfo.Ini
32 (wmiprvse.exe)	Checked	\Windows\system32\OemLogo.Bmp

An HTML or JavaScript with Excessive Amount of JavaScript Function Definitions

Artifact ID	SHA256	Path	Filetype
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html

Page Not Found HTML Error Page Detected.

Artifact ID	SHA256	Path
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006

JavaScript in HTML Uses Location.Replace Function

Artifact ID	SHA256	Path
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006

JavaScript Contains an Excessively Long String

Artifact ID	SHA256	Path	Filetype
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d	js

Script Contains URL

Artifact ID	SHA256	Path	Script Type
67	a3416d7f5581d355a241e2c9cce05d8b3acaa8b5e19ffec414ab003fd6f45130	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a	js
65	0f3be44690ae9914ae3e47b7752e1bdea316f09938e9094f99e0de19ccd8987a	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005	js
68	d59436512c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b	js
71	dccef0a18cc6701fef6084b76fb924c24266bd35b899bceefbf3af93e85ed3d8	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f	js
64	66732d29f4cb8058c3ca53d3b673dd97c36eec63ed101bbe81a316163d60edad	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004	js
63	3c039c07f705f3e4f4f980dc9e75cd10f8260ea1323ce73dd3b54f80e4ae1588	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003	js
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d	js

JavaScript Using "toString" Method

Artifact ID	SHA256	Path
64	66732d29f4cb8058c3ca53d3b673dd97c36eec63ed101bbe81a316163d60edad	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d
67	a3416d7f5581d355a241e2c9cce05d8b3acaa8b5e19ffec414ab003fd6f45130	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a
65	0f3be44690ae9914ae3e47b7752e1bdea316f09938e9094f99e0de19ccd8987a	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005

Artifact ID	SHA256	Path
71	dccef0a18cc6701fef6084b76fb924c24266bd35b899bceefbf3af93e85ed3d8	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f
63	3c039c07f705f3e4f4f980dc9e75cd10f8260ea1323ce73dd3b54f80e4ae1588	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003
68	d59436512c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b

Static Analysis Flagged Artifact As Potentially Obfuscated

Artifact ID	SHA256	Path	Rule	Description
71	dccef0a18cc6701fef6084b76fb924c24266bd35b899bceefbf3af93e85ed3d8	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f	js_double_obfuscation	A javascript file has an multi-layered obfuscated string.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_base64	An HTML file contains large base64 strings.
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d	js_double_obfuscation	A javascript file has an multi-layered obfuscated string.
64	66732d29f4cb8058c3ca53d3b673dd97c36eec63ed101bbe81a316163d60edad	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004	js_double_obfuscation	A javascript file has an multi-layered obfuscated string.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_double_obfuscation	An HTML file contains an multi-layered obfuscated string.
68	d59436512c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b	js_double_obfuscation	A javascript file has an multi-layered obfuscated string.

Artifact ID	SHA256	Path	Rule	Description
67	a3416d7f5581d355a241e2c9cce05d8b3acaa8b5e19ffec414ab003fd6f45130	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a	js_double_obfuscation	A javascript file has an multi-layered obfuscated string.
63	3c039c07f705f3e4f4f980dc9e75cd10f8260ea1323ce73dd3b54f80e4ae1588	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003	js_double_obfuscation	A javascript file has an multi-layered obfuscated string.

JavaScript Calls ActiveXObject

Artifact ID	SHA256	Path
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d
65	0f3be44690ae9914ae3e47b7752e1bdea316f09938e9094f99e0de19ccd8987a	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005
63	3c039c07f705f3e4f4f980dc9e75cd10f8260ea1323ce73dd3b54f80e4ae1588	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003
67	a3416d7f5581d355a241e2c9cce05d8b3acaa8b5e19ffec414ab003fd6f45130	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a
68	d59436512c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b

HTML Contains JavaScript Using 'eval()' Function

Artifact ID	SHA256	Path
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006

Static Analysis Flagged Artifact As Anomalous

Artifact ID	SHA256	Path	Rule	Description
67	a3416d7f5581d355a241e2c9cce05d8b3acaa8b5e19ffec414ab003fd6f45130	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000a	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.

Artifact ID	SHA256	Path	Rule	Description
64	66732d29f4cb8058c3ca53d3b673dd97c36eec63ed101bbe81a316163d60edad	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_double_body	HTML file has multiple bodies.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_double_close	HTML file has multiple closing blocks
68	d59436512c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.
63	3c039c07f705f3e4f4f980dc9e75cd10f8260ea1323ce73dd3b54f80e4ae1588	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000003	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_excessive_functions	An HTML file contains an excessive amount of functions definitions.
71	dccef0a18cc6701fef6084b76fb924c24266bd35b899bceefbf3af93e85ed3d8	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_empty_script	An HTML file contains a script with no content.

Artifact ID	SHA256	Path	Rule	Description
65	0f3be44690ae9914ae3e47b7752e1bdea316f09938e9094f99e0de19ccd8987a	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d	js_excessive_functions_and_blank_returns	A javascript file contains an excessive functions definitions.
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006	html_background_image_url	An HTML file contains a reference to a remote background image.

JavaScript In HTML Or HTA File Calls ActiveXObject

Artifact ID	SHA256	Path
66	8169437b684ed451ca236d90c63aa4065c217d0e094d9a6bbd263c5c0b7b9c9d	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000006

JavaScript Obfuscation Using "fromCharCode()" Function

Artifact ID	SHA256	Path
65	0f3be44690ae9914ae3e47b7752e1bdea316f09938e9094f99e0de19ccd8987a	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000005
69	12ec1a91795af74ad855c157c0784dded22501e0af2ccf5f6a20e1fac7d5e564	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000d

JavaScript Obfuscation Using "eval()" Function

Artifact ID	SHA256	Path
64	66732d29f4cb8058c3ca53d3b673dd97c36eec63ed101bbe81a316163d60edad	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_000004
71	dccef0a18cc6701fef6084b76fb924c24266bd35b899bceefbf3af93e85ed3d8	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000f
68	d59436512c5ec9414655bc4dcaaa9a5aed3def41120c576c51429178830d3688	\users\administrator\appdata\local\google\chrome\user data\default\old_cache_000\f_00000b

HTTP Redirection Response

Network Stream	Trans ID	Code	Status	Method	URL
10	0	301	Moved Permanently	GET	http://fallibleliving.com:80/

Sample Communicates With Only Benign Domains

Domain	Status	Categories	Security
fonts.gstatic.com	innocuous	Infrastructure	
fonts.googleapis.com	innocuous	Search Engines Search Engines and Portals	

DNS Response Contains Low Time to Live (TTL) Value

Query ID	Query Data	Answer Data	Answer Type	TTL
18369	fallibleliving.com	104.21.48.20	A	300
18369	fallibleliving.com	172.67.176.5	A	300
51462	s.w.org	192.0.77.48	A	292

Outbound HTTP GET Request From URL Submission

Network Stream	Method	URL
10	GET	http://fallibleliving.com:80/