



ID: 331433
Sample Name:
view_attach_72559.vbs
Cookbook: default.jbs
Time: 20:40:06
Date: 16/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report view_attach_72559.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Signature Overview 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
Data Obfuscation: 5
Persistence and Installation Behavior: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 14
JA3 Fingerprints 14
Dropped Files 15
Created / dropped Files 15
Static File Info 29
General 29
File Icon 29
Network Behavior 29
Network Port Distribution 29
TCP Packets 30
UDP Packets 30

DNS Queries 32
DNS Answers 32
HTTP Request Dependency Graph 32
HTTP Packets 32
HTTPS Packets 33
Code Manipulations 33
Statistics 34
Behavior 34
System Behavior 34
Analysis Process: wscript.exe PID: 960 Parent PID: 3424 34
General 34
File Activities 34
File Deleted 34
File Read 34
Registry Activities 35
Analysis Process: iexplore.exe PID: 5528 Parent PID: 800 35
General 35
File Activities 35
Registry Activities 35
Analysis Process: iexplore.exe PID: 5500 Parent PID: 5528 35
General 35
File Activities 36
Disassembly 36
Code Analysis 36

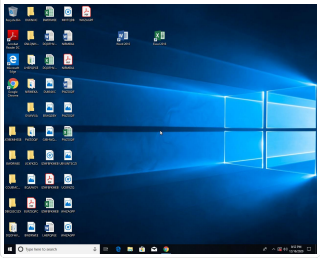
Analysis Report view_attach_72559.vbs

Overview

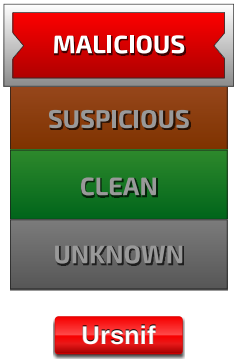
General Information

Sample Name:	view_attach_72559.vbs
Analysis ID:	331433
MD5:	29933320f02dfc1..
SHA1:	29db771aef8cfe3..
SHA256:	7c4f0d072bdbf9a..

Most interesting Screenshot:



Detection

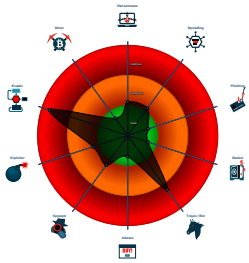


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Benign windows process drops PE f…
- System process connects to networ…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- Creates processes via WMI
- Deletes itself after installation
- Tries to detect sandboxes and other…
- AV process strings found (often use…
- Contains capabilities to detect virtua…
- Drops PE files
- Drops files with a non-matching file e…
- Found WSH timer for Javascript or V…

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 960 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\view_attach_72559.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- iexplore.exe (PID: 5528 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5500 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5528 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

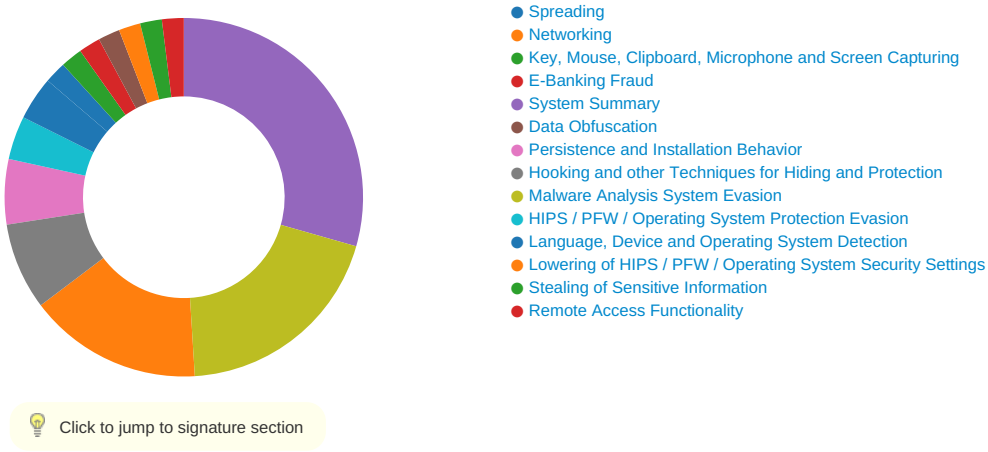
Source	Rule	Description	Author	Strings
00000007.00000003.841219747.0000000004DC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.841280724.0000000004DC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000002.844945859.0000000004DC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.841043510.0000000004DC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000007.00000003.841145092.0000000004DC8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 4 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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)

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

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

Stealing of Sensitive Information:

Yara detected Ursnif

Copyright null 2020

Remote Access Functionality:

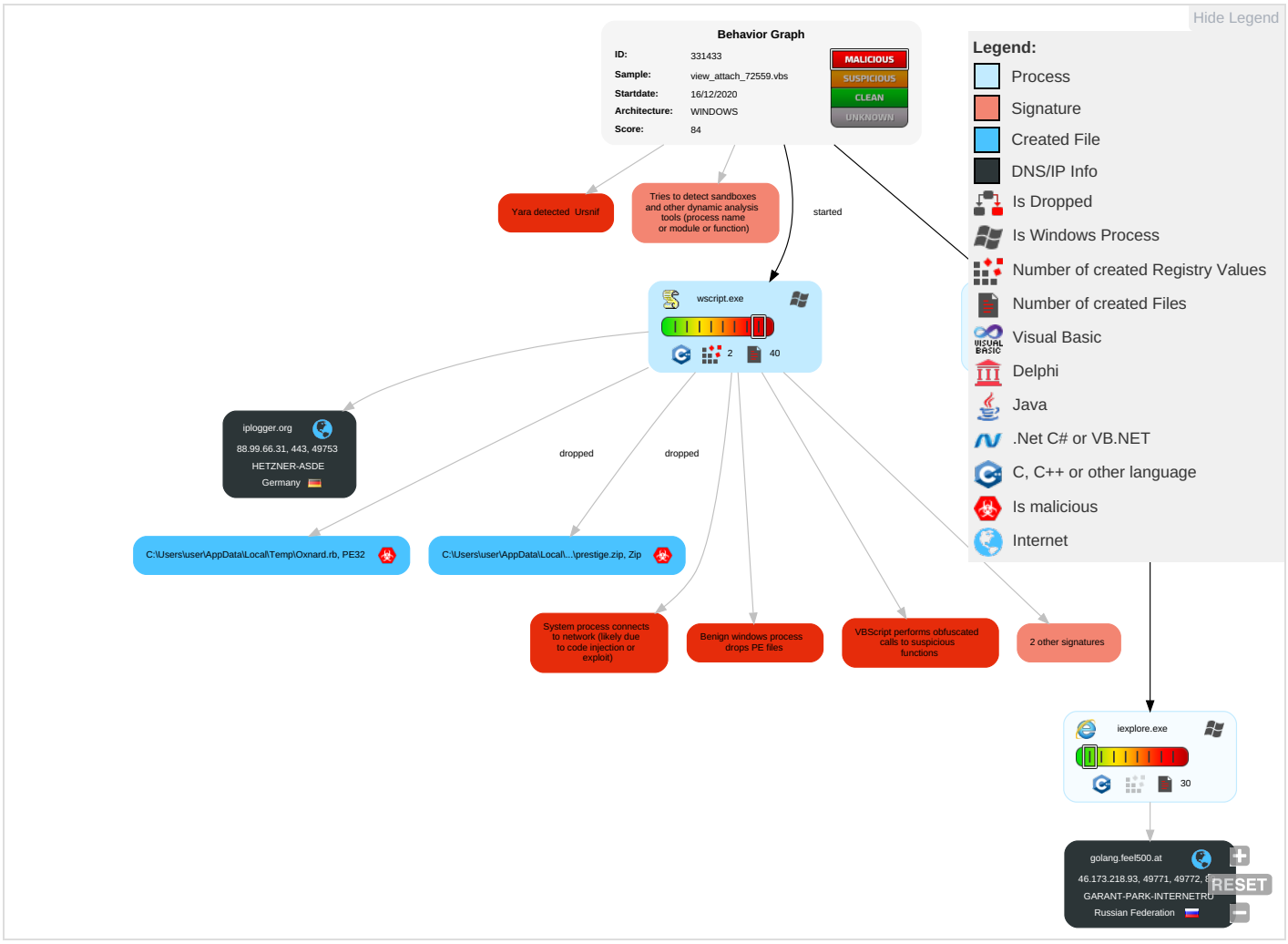


Yara detected Ursnif

Mitre Att&ck Matrix

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

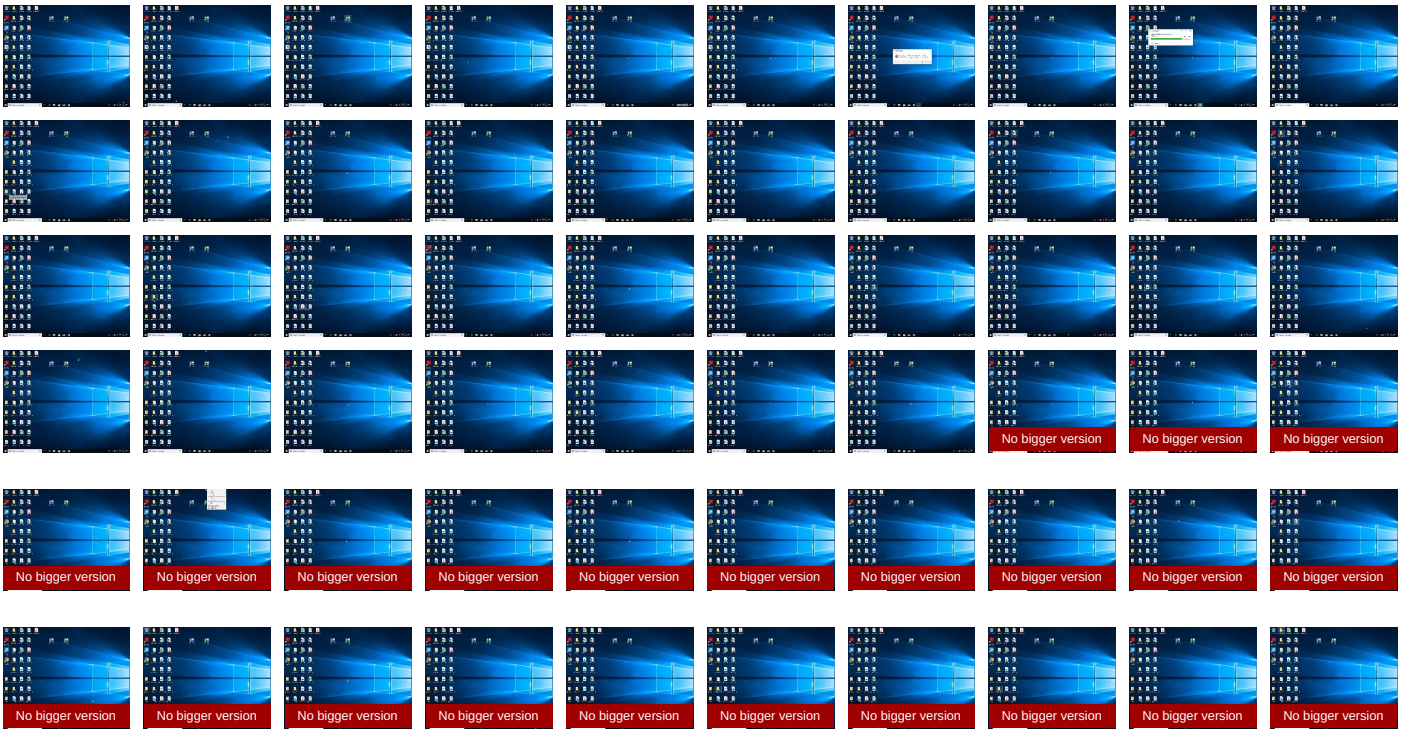
Behavior Graph

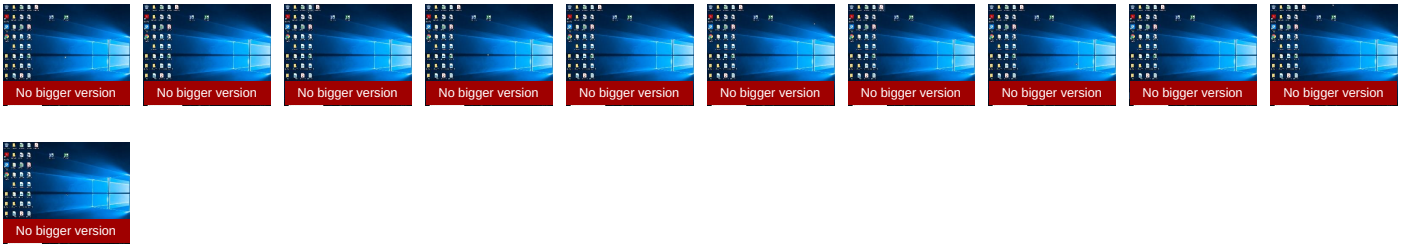


Screenshots

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
view_attach_72559.vbs	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
golang.feel500.at	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crl.com9	0%	Avira URL Cloud	safe	
http://golang.feel500.at/api1/DIwBQ8Rv7j7xfqFjg4_2BA9/g0fzfaOWqj/Y_2BPGiAPfzGcs2Be/I_2BUuYEc0ea/KBka	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://golang.feel500.at/favicon.ico	0%	Avira URL Cloud	safe	
http://crl.com	0%	Virustotal		Browse
http://crl.com	0%	Avira URL Cloud	safe	
http://golang.feel500.at/api1/DIwBQ8Rv7j7xfqFjg4_2BA9/g0fzfaOWqj/Y_2BPGiAPfzGcs2Be/I_2BUuYEc0ea/KBkab56Bm_2/FWmqnzUOX9_2B0/YbRWfB6IMq7TSr21K5FNM/xWmFuq_2FeEONGMO/1ZuPh_2FNFAeM3T/FM11WlspOeJ_2FqYpl/U_2F6jwXu/YXiyreYoS1UAkST_2FVa/JT_2Fx9W7QvoG6HJsdC/ExFIoNdpiPpyKG7cmJGp40/huNnlqBJ9uVVH/QyyRFE1b/30os8htaDb_2FAitT_2BOsm/SKMxwp3_0A/_0DyvsrFrDpoMB3eg/_2BPhnWhGFuU/FPA93GCv8Zd/FBoszW1uVg1_2B/gtKiRyRf4RAjLF4_2F0P1/_2FR	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iplogger.org	88.99.66.31	true	false		high
golang.feel500.at	46.173.218.93	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

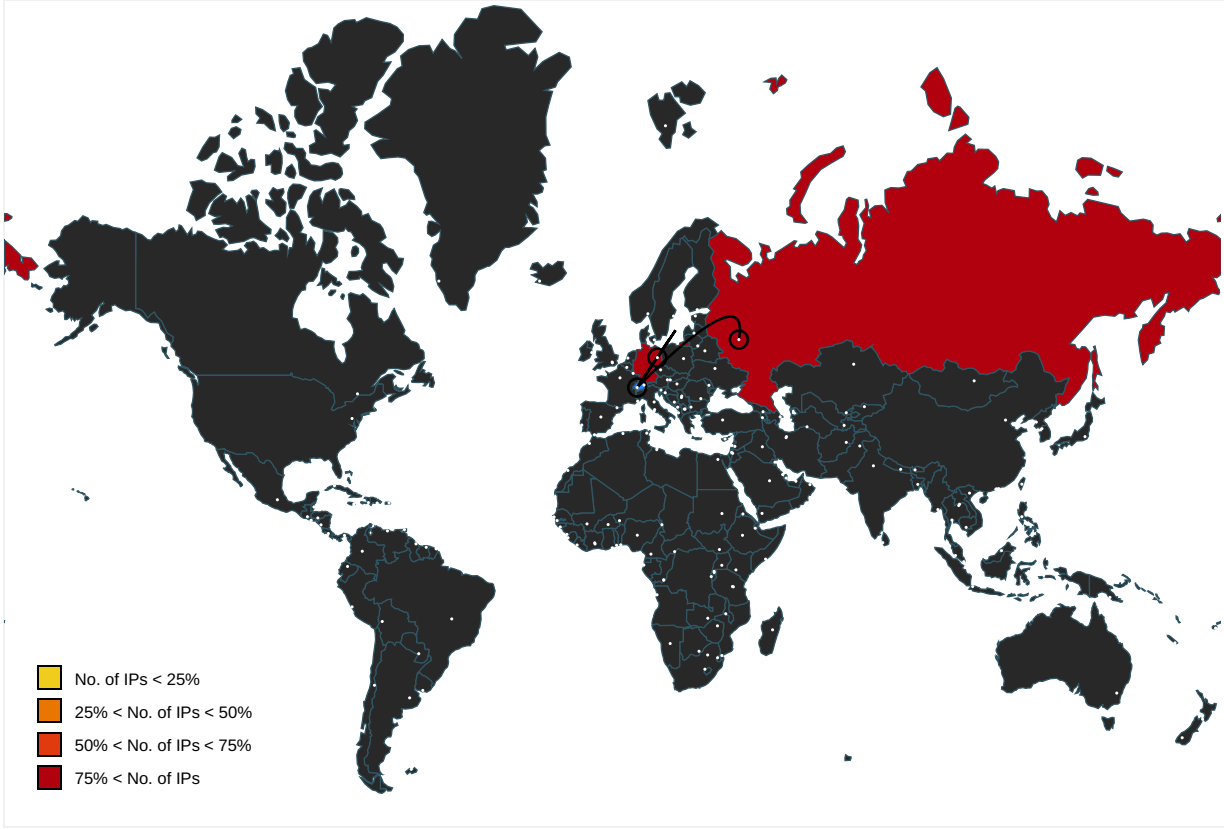
Name	Malicious	Antivirus Detection	Reputation
http://golang.feel500.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://golang.feel500.at/api1/DIwBQ8Rv7j7xfqFjg4_2BA9/g0fzfaOWqj/Y_2BPGiAPfzGcs2Be/I_2BUuYEc0ea/KBkab56Bm_2/FWmqnzUOX9_2B0/YbRWfB6IMq7TSr21K5FNM/xWmFuq_2FeEONGMO/1ZuPh_2FNFAeM3T/FM11WlspOeJ_2FqYpl/U_2F6jwXu/YXiyreYoS1UAkST_2FVa/JT_2Fx9W7QvoG6HJsdC/ExFIoNdpiPpyKG7cmJGp40/huNnlqBJ9uVVH/QyyRFE1b/30os8htaDb_2FAitT_2BOsm/SKMxwp3_0A/_0DyvsrFrDpoMB3eg/_2BPhnWhGFuU/FPA93GCv8Zd/FBoszW1uVg1_2B/gtKiRyRf4RAjLF4_2F0P1/_2FR	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	wscript.exe, 00000000.00000003.711285112.000001C8B6751000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nytimes.com/	msapplication.xml3.17.dr	false		high
http://https://sectigo.com/CPS0	wscript.exe, 00000000.00000003.711285112.000001C8B6751000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.sectigo.com0	wscript.exe, 00000000.00000003.711285112.000001C8B6751000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/policy	wscript.exe, 00000000.00000003.711756068.000001C8B66D1000.00000004.00000001.sdmp	false		high
http://crl.com9	wscript.exe, 00000000.00000003.716624163.000001C8B6063000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/1D5y47	wscript.exe, 00000000.00000003.712665350.000001C8B3A16000.00000004.00000001.sdmp	false		high
http://www.youtube.com/	msapplication.xml7.17.dr	false		high
http://https://iplogger.org/18j267Nums	wscript.exe, 00000000.00000003.711430309.000001C8B676D000.00000004.00000001.sdmp	false		high
http://golang.feel500.at/api1/DIwBQ8Rv7j7xfqFjg4_2BA9/g0fzfaOWqj/Y_2BPGiAPfzGcs2Be/I_2BUuYEc0ea/KBka	{CFFA0380-3FD6-11EB-90EB-ECF4BBEA1588}.dat.17.dr, ~DFCE3CEB3DA92FCDD0.TMP.17.dr	false	• Avira URL Cloud: safe	unknown
http://https://iplogger.org/18j267	wscript.exe, 00000000.00000003.711430309.000001C8B676D000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.712532222.000001C8B5BEB000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.712769407.000001C8B4CF0000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.712764101.000001C8B3A55000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.711820977.000001C8B6690000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.712694780.000001C8B3A4B000.00000004.00000001.sdmp	false		high
http://www.wikipedia.com/	msapplication.xml6.17.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://iplogger.org/	wscript.exe, 00000000.00000003.711863605.000001C8B6372000.00000004.00000001.sdmp, wscript.exe, 00000000.00000003.711756068.000001C8B66D1000.00000004.00000001.sdmp	false		high
http://www.amazon.com/	msapplication.xml.17.dr	false		high
http://crl.com	wscript.exe, 00000000.00000003.716624163.000001C8B6063000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.live.com/	msapplication.xml2.17.dr	false		high
http://www.reddit.com/	msapplication.xml4.17.dr	false		high
http://www.twitter.com/	msapplication.xml5.17.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.173.218.93	unknown	Russian Federation		47196	GARANT-PARK-INTERNETRU	false
88.99.66.31	unknown	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	331433
Start date:	16.12.2020
Start time:	20:40:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	view_attach_72559.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:	33
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:	mal84.troj.evad.winVBS@4/52@2/2

Copyright null 2020

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, rundll32.exe, ielowutil.exe, RuntimeBroker.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 51.11.168.160, 92.122.213.194, 92.122.213.247, 52.155.217.156, 8.248.131.254, 8.241.79.126, 8.241.90.126, 2.20.142.210, 2.20.142.209, 20.54.26.129, 104.108.39.131, 152.199.19.161, 40.126.1.145, 40.126.1.142, 40.126.1.128, 40.126.1.166, 20.190.129.17, 20.190.129.2, 20.190.129.130, 20.190.129.160, 93.184.220.29, 40.127.240.158, 51.104.139.180 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, go.microsoft.com, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • 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
20:41:23	API Interceptor	2x Sleep call for process: wscript.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
88.99.66.31	TrustedInstaller.exe	Get hash	malicious	Browse	• iplogger.org/1yekr7.gz
	zeppelin.exe	Get hash	malicious	Browse	• iplogger.org/1D2XM6.tgz
	cli.exe	Get hash	malicious	Browse	• ezstat.ru/1BiQt7.html
	R7w74RKW9A.exe	Get hash	malicious	Browse	• ezstat.ru/1BiQt7.html
	pqSZtQiuRy.exe	Get hash	malicious	Browse	• iplogger.org/14mvt7.gz
	3MndTUzGQn.exe	Get hash	malicious	Browse	• iplogger.org/14qK87
	fEBNeNkRYI.doc	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	Delivery-77426522.doc	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	mesager43.exe	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	hci0xn0zip.exe	Get hash	malicious	Browse	• iplogger.org/1cyy87.jpg
	DOC001.exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	DOC001 (3).exe	Get hash	malicious	Browse	• 2no.co/1Lan77
	urgently.exe	Get hash	malicious	Browse	• iplogger.org/1Uu547.tgz
	SecuriteInfo.com.Generic.mg.e26982b170856ca8.exe	Get hash	malicious	Browse	• iplogger.org/1Uu547.tgz
	trwf3446.doc	Get hash	malicious	Browse	• iplogger.org/1Uu547.tgz
	2020_1549496734.doc	Get hash	malicious	Browse	• maper.info/XtDei
	2020_1549496734.doc	Get hash	malicious	Browse	• maper.info/XtDei
	http://maper.info	Get hash	malicious	Browse	• maper.info/
	clipp.exe	Get hash	malicious	Browse	• iplogger.com/1NAnw7
	por.exe	Get hash	malicious	Browse	• ezstat.ru/1kDj27

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
golang.feel500.at	attach_12.12.2020-4570.vbs	Get hash	malicious	Browse	• 47.241.19.44
iplogger.org	w2XNdMowdt.exe	Get hash	malicious	Browse	• 88.99.66.31
	AX73LXm0uW.exe	Get hash	malicious	Browse	• 88.99.66.31
	fOahv51tTZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	RvunN9dC5z.exe	Get hash	malicious	Browse	• 88.99.66.31
	qn1tGLHD7L.exe	Get hash	malicious	Browse	• 88.99.66.31
	DAK0SFLsXV.exe	Get hash	malicious	Browse	• 88.99.66.31
	TrustedInstaller.exe	Get hash	malicious	Browse	• 88.99.66.31
	Pw5WhqWFzK.exe	Get hash	malicious	Browse	• 88.99.66.31
	soft.exe	Get hash	malicious	Browse	• 88.99.66.31
	yVjUyduR6F.exe	Get hash	malicious	Browse	• 88.99.66.31
	EJG80crXtR.exe	Get hash	malicious	Browse	• 88.99.66.31
	h1GodtbhC8.exe	Get hash	malicious	Browse	• 88.99.66.31
	YzvGNYMkTT.exe	Get hash	malicious	Browse	• 88.99.66.31
	zeppelin.exe	Get hash	malicious	Browse	• 88.99.66.31
	6GwRAlSS4F.exe	Get hash	malicious	Browse	• 88.99.66.31
	Hlxj8nfBay.exe	Get hash	malicious	Browse	• 88.99.66.31
	7z6cDuH7Md.exe	Get hash	malicious	Browse	• 88.99.66.31
	cpMHTTwNC1.exe	Get hash	malicious	Browse	• 88.99.66.31
	IaGdBpfkmV.exe	Get hash	malicious	Browse	• 88.99.66.31
	A5RsEkXArf.exe	Get hash	malicious	Browse	• 88.99.66.31

Copyright null 2020

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	dridex.doc	Get hash	malicious	Browse	• 116.202.162.137
	dridex.doc	Get hash	malicious	Browse	• 116.202.162.137
	contractpharmacy_SOA2143083-pdf.html	Get hash	malicious	Browse	• 95.217.33.203
	5BYmpzCkVn.doc	Get hash	malicious	Browse	• 116.202.162.137
	tlALsHy73R.exe	Get hash	malicious	Browse	• 95.217.228.176
	http://https://ucf2e159dcdc627dd91c5955a5b2.dl.dropboxusercontent.com/cd/0/get/BFIJR_DLx5TrpQ0LUrIdtB-TiMb8hXWBtyaxeUO96o9pDO2kuhn8C1M100sfcNRduSe85JbdWYokMfX07myXHHCiJews_d8d9AU4Vbqsj4mNqfzUgaLCJ-Q80my2kOBIkNQ/file?dl=1	Get hash	malicious	Browse	• 116.202.162.137
	SKM_C33501911071023000.exe	Get hash	malicious	Browse	• 5.9.83.154
	INVOICE.EXE	Get hash	malicious	Browse	• 95.216.7.161
	sample.exe	Get hash	malicious	Browse	• 136.243.187.20
	output.xls	Get hash	malicious	Browse	• 188.40.95.144
	INVOICE3DDH.exe	Get hash	malicious	Browse	• 168.119.57.232
	SecuriteInfo.com.Heur.20246.xls	Get hash	malicious	Browse	• 46.4.92.222
	w2XNdMowdt.exe	Get hash	malicious	Browse	• 88.99.66.31
	attach_12.12.2020-4570.vbs	Get hash	malicious	Browse	• 88.99.66.31
	http://annabeller.cpsus.org/?YW5uYWJlbGxlckBoZXJiYWxpZmUuY29t/3	Get hash	malicious	Browse	• 95.217.10.244
	AX73LXm0uW.exe	Get hash	malicious	Browse	• 88.99.66.31
	fOahv51tTZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	http://gmai.com	Get hash	malicious	Browse	• 168.119.139.96
	Ca4fOzoNzJ.exe	Get hash	malicious	Browse	• 88.99.66.31
	RvunN9dC5z.exe	Get hash	malicious	Browse	• 88.99.66.31
GARANT-PARK-INTERNETRU	Sly.exe	Get hash	malicious	Browse	• 91.203.193.144
	rEjVPo1E9f.exe	Get hash	malicious	Browse	• 46.173.214.78
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 46.173.214.227
	2020-12-01_01-59.exe	Get hash	malicious	Browse	• 46.173.214.135
	7pxcKjFYgp.exe	Get hash	malicious	Browse	• 46.173.214.122
	7HKZyhjCXK.exe	Get hash	malicious	Browse	• 195.22.153.143
	UP8VQkNe42.exe	Get hash	malicious	Browse	• 195.22.153.143
	TQ-03865.exe	Get hash	malicious	Browse	• 195.22.153.143
	NEFT_pdf.exe	Get hash	malicious	Browse	• 46.173.218.160
	ODnxDOTnzJ.exe	Get hash	malicious	Browse	• 195.22.153.143
	SQ_07394.exe	Get hash	malicious	Browse	• 195.22.153.143
	Remittance Advice_pdf.exe	Get hash	malicious	Browse	• 195.22.153.143
	BANK_TT_pdf.exe	Get hash	malicious	Browse	• 195.22.153.143
	BANK_TT_COPY_PDF.exe	Get hash	malicious	Browse	• 195.22.153.143
	TQ-06383.exe	Get hash	malicious	Browse	• 195.22.153.143
	TQ-07372.exe	Get hash	malicious	Browse	• 195.22.153.143
	Pvm3Bq1eV0SeTcL.exe	Get hash	malicious	Browse	• 195.22.153.143
	TQ-06871.exe	Get hash	malicious	Browse	• 195.22.153.143
	6VXhGBVj7lE6iuH.exe	Get hash	malicious	Browse	• 195.22.153.143
	Payment Advice.pdf.exe	Get hash	malicious	Browse	• 195.22.153.143

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	New Order 34566.xlsx	Get hash	malicious	Browse	• 88.99.66.31
	Invoice.xlsb	Get hash	malicious	Browse	• 88.99.66.31
	24KHK5538n.exe	Get hash	malicious	Browse	• 88.99.66.31
	k7EKbgSEPj.exe	Get hash	malicious	Browse	• 88.99.66.31
	sample.exe	Get hash	malicious	Browse	• 88.99.66.31
	servises.exe	Get hash	malicious	Browse	• 88.99.66.31
	Invoice.xlsb	Get hash	malicious	Browse	• 88.99.66.31
	http://snenpinfrresertts.com/ref-151220-BTC2XU590R2HT8.xls	Get hash	malicious	Browse	• 88.99.66.31
	#Ud544#Ub9bd#Uc2a4_smartcontrol (Zvm4Gi etK6GFlvHkOIml25j995X5KM8FRT4M).js	Get hash	malicious	Browse	• 88.99.66.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Ud544#Ub9bd#Uc2a4_smartcontrol (Zvm4Gi etK6GFlvHkOIml25j995X5KM8FRT4M).js	Get hash	malicious	Browse	• 88.99.66.31
	Consulta urgente para el proyecto KD958838 Madrid.docx	Get hash	malicious	Browse	• 88.99.66.31
	w2XNdMowdt.exe	Get hash	malicious	Browse	• 88.99.66.31
	attach_12.12.2020-4570.vbs	Get hash	malicious	Browse	• 88.99.66.31
	AX73LXm0uW.exe	Get hash	malicious	Browse	• 88.99.66.31
	fOahv51tTZ.exe	Get hash	malicious	Browse	• 88.99.66.31
	RvunN9dC5z.exe	Get hash	malicious	Browse	• 88.99.66.31
	qn1tGLHD7L.exe	Get hash	malicious	Browse	• 88.99.66.31
	H4H2YCoM5P.exe	Get hash	malicious	Browse	• 88.99.66.31
	fw2.exe	Get hash	malicious	Browse	• 88.99.66.31
	yVjUyduR6F.exe	Get hash	malicious	Browse	• 88.99.66.31

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CFFA037E-3FD6-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7701768832338793
Encrypted:	false
SSDEEP:	192:rUZHZo289WAt78if7XtU2zMbX/u36aCB0DX/lpB:rE5/8UE7R7XAbX10DXp
MD5:	F79622EE63525B4F8608F84868DFE64C
SHA1:	881B8FE73BA7134429292FA913F9AE6C599E661E
SHA-256:	87E71F2719C309D4F31E840EB912AB6BAC45500CBC7633BBCD9321E4E8B8FBA6
SHA-512:	A9CDC6A27EAE18A10217AC6AC42962A023844B8D75A4F6AD57FD294F7B4690811EA9004CD02E50E6D5F9702F9B5321A8B8941B7DE614208C3E95C0644EF8326
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\{CFFA0380-3FD6-11EB-90EB-ECF4BBEA1588}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28200
Entropy (8bit):	1.936498638579297
Encrypted:	false
SSDEEP:	96:r3aZNXQ+26bBSeFjx2AkWbMSYhLny47Uj9FlLnHFny47UjPFA:rqZhQt6bkeFjx2AkWbMSYhLSFlbVcFA
MD5:	75AD93FDE8741ABE37803C57C7239F62
SHA1:	015E864C55F8E1152F6F6EE987453DB7F2554EA5
SHA-256:	4D891ECADF4E21298FA5B588920BC7A6847CCD39BFA282EDD0EAEDCFA575CB10
SHA-512:	C0B3BCB338DF064AFB1C84E7713E5267C72E7C16E7BD6894298F76EF97F8367E5C0D92D931996D5BF9EEFC438D2566D33BC14C246CEB2AFD2859CE208D94A67
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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Entropy (8bit):	5.0924934037317415
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEwqHQqH7nWimI002EtM3MHdNMNxOEwqHQqH7nWimI00OYGVbkEtMb:2d6NxOWSZHKd6NxOWSZ7YLb
MD5:	F118AEC2673FB7058A3CC8DA0D7D4AA7
SHA1:	5555C3A98FB3C085E2F34E47F861BF1DF6D9D790
SHA-256:	4C1E33AF19507D8A14145A71D2DF742FEB871A259E6B95911E6C80931DDDA273
SHA-512:	5384D61F6790C091031D59422067F5EFF888FB1FB9A2C83EB74AEDD05186A82D4D792C1E4538B9FE19524C103A9A6637622C17E8AC08B4D42AF2835958EC6FD6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa594b73e,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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>0xa594b73e,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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):	5.092780265835011
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kX+H3+H7nWimI002EtM3MHdNMNxe2kX+H3+H7nWimI00OYGkak6Ety:2d6NxrmgASZHKd6NxrmgASZ7Yza7b
MD5:	A752957DBDCE7BC9B7212DE222FC0A63
SHA1:	5F7D2280928F83FD777CA377001DE777213D21CA
SHA-256:	6B23E294E42DD7416B8C9A5720006E5820DE129214584F637CEB87F3B61A59E3
SHA-512:	2616DB7FA6A0E5DCDA4722D1A020E048FB2FAAF6014758DDA8852D856874CD9625834C64C82AF2B22253B6AED7E942880C27CC5B2CD2897EB6B1AD15BFB10DF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa58d905a,0x01d6d3e3</date><accdate>0xa58d905a,0x01d6d3e3</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>0xa58d905a,0x01d6d3e3</date><accdate>0xa58d905a,0x01d6d3e3</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):	5.110590777299088
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLwqHQqH7nWimI002EtM3MHdNMNxvLwqHQqH7nWimI00OYGmZEtMb:2d6NxvzSZHKd6NxvzSZ7Yjb
MD5:	4A00FF0525AA01F76F9A730DDABEED97
SHA1:	83EF255D7777444EC9BE0AF8058BCC9B0FDC1CE5
SHA-256:	6FA38B6513CE17F990E9A559A3C167A1C562E372F01EA7A194237A7029283002
SHA-512:	B6EDC682B1EB35556464BE065CA0E6907E78F64AECCA8819C2D46ED6A6E1E690EF16AF84CAFC158A73C27C1AC6C50644F1682070636F6B159D451AB55DA55A7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa594b73e,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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>0xa594b73e,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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):	5.129646037897988
Encrypted:	false
SSDEEP:	12:TMHdNMNxi6HaH7nWimI002EtM3MHdNMNxi6HaH7nWimI00OYGd5EtMb:2d6Nx2SZHKd6Nx2SZ7YEjb
MD5:	0C0B09F48D0F73E503AFD4DCB83E3675

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA1:	CD36BFAD97E933468642BE459C5B3E5C41A58F61
SHA-256:	233D3AA7A29EDABA7FDFBB0DC9EDAA5AFBABC7F00C154E092B62A6BDB1C7A10C
SHA-512:	5BB2FA52E354B94E47FE1E22204CFA06A815FCB7DFE571D4B08EF7A6CF13C6CA1CF1C06ADA9F014CDBB98EA7F332A09386EE4A06ABB7A08D99DA3BF7E126A83A
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</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>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</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):	5.123132870081053
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwwqHQqH7nWimI002EtM3MHdNMNxhGwwqHQqH7nWimI00OYG8K075Es:2d6NxQaSZHKd6NxQaSZ7YrKajb
MD5:	C9796C6A36471AFF211A16538759B55E
SHA1:	8FD013141E6276108ADD3571F4FE9FD2EA2849DB
SHA-256:	9F085CEA786625280255FDDDD337C7364451C1A7FFD79CECA4BC89B69FF2B213
SHA-512:	20E14BA5C6083B7483CBAE963C41250FB2706B33A64FFE7F02C49C88A0513367F8805DB0D734559BBE773B48DC311BDEC3DA0DC2EED5C81A56FECCD455A676CE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa594b73e,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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>0xa594b73e,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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):	5.113145425337172
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n6HaH7nWimI002EtM3MHdNMNx0n6HQqH7nWimI00OYGxEtMb:2d6Nx0VSZHKd6Nx0ASZ7Ygb
MD5:	3F7384E58009F1CF89B9912978C4983B
SHA1:	9E7F7226713E5B62E76BDFAFEBC811538E799A2D
SHA-256:	7A32144D9ACC7F1722A8DA578F8CE3293E19D223732DDAECCFF4B9F62A21F54C
SHA-512:	4AF65E952579D831BAC94496BA976CBBF93641FD330BA963167CD65DD1ED515DCF153DB11FDF81E29D508ADAB5BA14A7C59B4791845A62CE280FD163CDC065
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</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>0xa59254cb,0x01d6d3e3</date><accdate>0xa594b73e,0x01d6d3e3</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\pin202591677780\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):	5.153541411757083
Encrypted:	false
SSDEEP:	12:TMHdNMNxx6HaH7nWimI002EtM3MHdNMNxx6HaH7nWimI00OYG6Kq5EtMb:2d6NxfSZHKd6NxfSZ7Yhb
MD5:	421D29A8C883F69BB5754DF7CE4F96AD
SHA1:	C5E13B11AD57F7037B2AEA0B1A58EED219FFB0D3
SHA-256:	A566F16A6C77A2882B4A46813BF591A5C4ED68335D19DAC22BA61253639E45CB
SHA-512:	BDC65009F7BC219B00B1BFAF13879280E06B3FEAF69B593BA8698D1B41EBBA1962F6BFDCD3489A8408B67E07DD86C11EE102DC82443549901312E047919E46D

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</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>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</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):	5.085454073408255
Encrypted:	false
SSDEEP:	12:TMHdNMNxceNH+NH7nWimI002EtM3MHdNMNxceNH+NH7nWimI00OYGVEtMb:2d6NxX0xSZHKd6NxX0xSZ7Ykb
MD5:	E0566B8AF457CE4DD71186D64FBCCA92
SHA1:	3A94CF67B68C80868D31365FA2E3A1B7ED25ED44
SHA-256:	5C86257A4B2C437BE193C2C479ABE6096A553AE84988F988BE670D740845A660
SHA-512:	D34BFD76913E7F93B55D67FE33C93D05ECE42E204D155AE59E3DEC3910C8AFECEE46F8E6003D643E06D3C2A0B02F6CFA450EFA918EA079283C6D5824C84EE241
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa58ff2cd,0x01d6d3e3</date><accdate>0xa58ff2cd,0x01d6d3e3</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>0xa58ff2cd,0x01d6d3e3</date><accdate>0xa58ff2cd,0x01d6d3e3</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):	5.11480315323285
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn6HaH7nWimI002EtM3MHdNMNxfn6HaH7nWimI00OYGe5EtMb:2d6Nx9SZHKd6Nx9SZ7YLjb
MD5:	7BD67AD55FF3C4101DA0C7F72E2FBCDE
SHA1:	C279B261784109300D57FD101AC3C9F3DFB872A9
SHA-256:	6F1F7BC1DB754F350765508AD40473224F9AE50909233D9F8625E78EC71AD43B
SHA-512:	3BAC50BEEA7859C0FB2C2F3880A8351629404DC6466B851F9E8CE689809CB4064CE2ADC8CF88C5FCF105030AAA40A796A214CFB46CF217E1EDEFA2C982E2220
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</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>0xa59254cb,0x01d6d3e3</date><accdate>0xa59254cb,0x01d6d3e3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Temp\Chester.ape	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	67
Entropy (8bit):	5.102964936532685
Encrypted:	false
SSDEEP:	3:+pKKCd/EggPkI9L77njPLn/Pq:+kKCdjgPj17DjL/Pq
MD5:	D48899079DE705741C3E83077284BC4D
SHA1:	DE88E6F59311959EE0DEEFA999D98A0A09D5748D
SHA-256:	DC4916A8C803ADE7FD3DC750B3E6252BB1AD688821A613A2B74F6FB89C7130F0
SHA-512:	3EB78FE49FDB82F5A0ADA26D02C933D19AE67CAB116712E4BD9D795BF6AFE7BA1BE8DB1323AE7C8EF88787A39660BE28DD9A50ED5DEA570B82D16C71BE7DB88B
Malicious:	false
Reputation:	low
Preview:	RHTwabCooICxfqqaZVfyFRBIEJebJEtpNvKfjlcXwjemEvLWsptItkqcjFjDYUBZVFO

C:\Users\user\AppData\Local\Temp\Cicero.rm	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	4.962817180187938
Encrypted:	false
SSDEEP:	3:f5whkbZcC2eIr1iCcVlVn:/bTIrUCcVlV
MD5:	3C94E13E6629EF203D6CD694C0821837
SHA1:	A346BB508F82B411C01759C7E71862C7C1B0E170
SHA-256:	7B20234A44EFFF257AD0F356B0C4E9006BEB8A78C8DDA36257DBD3815A70E442
SHA-512:	953FA86146AD7B26F733C0E5F76A1D5D1A8551A05ABE2A2E1CC79FF65CCD27E94CF05B3E8F8C462456BE3AE3CD06A7609262771DDD4238AE5C79064AE88F86 8
Malicious:	false
Reputation:	low
Preview:	uoenSmIsJHesnhUkOkeWoRBrwqVRQSDZqcpCdZsfHBTfqNPYVXOZOqBqysHBtlScyp

C:\Users\user\AppData\Local\Temp\Dorchester.asf	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	95
Entropy (8bit):	5.3035002133435984
Encrypted:	false
SSDEEP:	3:tQgq1AAtZjBbikbGcQokoHTP9a/CZhQDgY2en:Lq1AAtZRikxnH7YqfhK
MD5:	87FAC5EFC1BD7DFD5C26E19B0807902C
SHA1:	289768A56820126CDD4AAFF5562F08ADCA08238D
SHA-256:	D18D532187E5C9196D1C91A36280717C3DCBFF8BA550C543FCAD770148725874
SHA-512:	B5CBFBC317B9DFAA68DE31BF3E4CACB8DB968756BDD5951D654F250AD86E41B29CFDC31BB08FD64ED01C73729898ACD5985AD75A236327C1D60EC70493003 0E
Malicious:	false
Reputation:	low
Preview:	QqNaEOCgOWCxeQACPImElXHbcJqvJdjFGGbINekLtyzVhKtjMAOLjPDbObIQqRZXxhGRnOUKOJefBfjDgRFwDuPlEQDSyum

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:	modified
Size (bytes):	89
Entropy (8bit):	4.17594063356479
Encrypted:	false
SSDEEP:	3:oVXVPDJ/ZohW8JOGXnFPDJ/Zomn:o95FqJF
MD5:	4A9ED9208CA05A8386F95FC9F422CCA4
SHA1:	D1B65C43289A8F80F66F04443D1ABEA023A229B8
SHA-256:	A62D21121F55F9CB9FEB8336312813787C664B5436A74B57DBBBC520281CBE06
SHA-512:	7C24EB6F044F38BCA0687FDC8EFA3655CBDA005CE26E11B6B2489FB1BAD376A4CCE404703560DC4A3CC969862B627798324A4218BB7CCE6BFAED8C0E20CE5 A21
Malicious:	false
Reputation:	low
Preview:	[2020/12/16 20:42:22.912] Latest deploy version: ..[2020/12/16 20:42:22.912] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\Macon.gif	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	3.459431618637298
Encrypted:	false
SSDEEP:	3:83y:8C
MD5:	47B6C296517745D4F1BA7D0E75249DE7
SHA1:	EEB0E2F74752AE1D88645D8A3B56EFE14DB2CD46
SHA-256:	6F96AE646DCC5F8A930FAE413CD9F6F3D59E048DBDD8664C8CBCB73B05ADDC2D
SHA-512:	7F69026DCBF31AFF3CCF11C6DB30CFE5657AD86CAF62DABE5B0643D4DAEB39219CCFD79FFEAC4E59B485F904A2F13882991EE206A1F303FF36379102D131F1 0

C:\Users\user\AppData\Local\Temp\Macon.gif	
Malicious:	false
Preview:	hnBsgKzdRJO

C:\Users\user\AppData\Local\Temp\Martian.apk	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.913400745661379
Encrypted:	false
SSDEEP:	3:caHAGfhC0R+IvzT1XS:lHAgBEgzT1XS
MD5:	74F94C761841D291E484C7A1B5D09DCB
SHA1:	61135B95844BEBB3D2B0447A26CFBCB712B94C20
SHA-256:	39916BAF4F30926112C13F34B50D7B0BA74F6AFF36120A21271C1F7F3BAAE183
SHA-512:	26A3E075BFEA62EF972AFECE832A9859C97E9DF42CFE0464DDE8FD1E0F6C721089B1627D0758E85CBC82D4B984694A15E5B4B5A47A7A032CD7189E291C7E53 0
Malicious:	false
Preview:	ICYIGfWbkJoJZXIUbUChaNhwtRGLahlZHXKcFfNKIAggyoibZNVMwnKyJhzTtw

C:\Users\user\AppData\Local\Temp\Oxnard.rb	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	417792
Entropy (8bit):	5.6572317615997525
Encrypted:	false
SSDEEP:	6144:67ZZcPOHchp9XPhKt+Y0qc4jN2uzWoI7GwZEm/0itnsfUCTz:wKp9Z++Yjj4uKCCENidsfb
MD5:	C320A187099D091B08E3E6F6CCD13951
SHA1:	C97C1B6F0815A1040203F2439A54E80809CF094C
SHA-256:	04ECC922E98B64E4B13C966B9705D5E4B7BD4E789F27FD3C4B873D97C7E6722D
SHA-512:	E9E76CC8FBBC9E0330C38A7D751811ACA77C063AE46E991B2CEF3A439B7477900D11927448018C4C34239634D2EA2EB9E86B997F31E6AD97B78359DFC7CE536
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e..!..!..!....d.5....d..L...(...$..!...A....d.....d. ....d. ....d. ...Rich!..... PE..L.....cG.....!.....8).....<.....@.....H.....t ext..... ..`.data...0..... .....@....rsrc..... .....@..@.reloc..z!.....0...0.....@..B.....

C:\Users\user\AppData\Local\Temp\Schneider.mp2	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.349648912578752
Encrypted:	false
SSDEEP:	3:nAJ7spAQsI:AJ7spb
MD5:	4EF348200316D38EE63509A576AC5178
SHA1:	5D4867714E6B2289523FE7A0DD3562E95FA26AD6
SHA-256:	4A888A767FAEA5B08AFFA8F1021B6A1FEB7AE25936CF41B1518DAD22FDA6A607
SHA-512:	B4105067EC9E1735C8C53E25FBB39F8B6BDEFDF43AB21CEEB2D400A0D35F750E0BE7D673677E8AFA8E9FF2C653C43E45BAC766494617CD8EA1EEF4DB8C68E 612
Malicious:	false
Preview:	pjXXGlVJgoQAPCLeuItUISN

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

C:\Users\user\AppData\Local\Temp\adobe.url	
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\arisen.mp2	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	4.1523912776298655
Encrypted:	false
SSDEEP:	3:bmnJgrCfELv/:PrCqn
MD5:	8EC33937ABA9AEFCBE9A2370714CC7D8
SHA1:	727B5AA9782CD506D96AC4E2FDD8F059DE779A37
SHA-256:	77416C24DDCF896D44CE78F68A979F0CD032B1CB2A1EC61465FC908CB724DD58
SHA-512:	94F757688EAB873C8C1ECC3BAE4DE29B3C816B8769F1445489DDFD90237C4C2EE65000D7848193D1BDA96067D0ACCB3F682336F1DD9AD978D746EA8201B13A1
Malicious:	false
Preview:	BKqteLBLlgFOuHUzanBhXZ

C:\Users\user\AppData\Local\Temp\barbarous.otf	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.578638720860855
Encrypted:	false
SSDEEP:	3:bfcKnQ3otRS2MIGP:nLrMIGP
MD5:	BA060A184D10E715F484591DC34CFB98
SHA1:	344469DAE1D650793D63F75A1A3EB7EFE648046B
SHA-256:	E92BFC6E289B368A641A2CA39BEF7BB3A76C03E4C4EEE8FC24CDC5C0B88E9177
SHA-512:	C3D0FDC98781430DACFB8EB983BE7498C1135814DE383A903FB10B0BEE7504F0F3D334D2CBDC719148353C6443CBA949B5328C368664766F1DEC2562157807B
Malicious:	false
Preview:	cFFuQWnMbyyokmwASNmkRMmNhStwngRxPnKBekVmcTkW

C:\Users\user\AppData\Local\Temp\bard.msi	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	14
Entropy (8bit):	3.521640636343319
Encrypted:	false
SSDEEP:	3:K72:H
MD5:	DED2859B328A8261C90815003AB419C5
SHA1:	6BB23F7CB3F0B0D93BB4C4D720699E227D0FCABC
SHA-256:	D1667387C73330BB64AF8EC36BC0896ABCC7CDA47ACFEB5389AD026F074F16AC
SHA-512:	4F22EB5A0891C6C0C5BE9C2352A1834DE728DA7C61ACEE179FDDD4C7A759B668FEFA464BC77B24F223CE590C1D71318BB65E3ABE74125F8B565AC1B827B37798
Malicious:	false
Preview:	TvkahGUDSBhdev

C:\Users\user\AppData\Local\Temp\bitt.rmvb	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	25
Entropy (8bit):	4.323856189774724
Encrypted:	false
SSDEEP:	3:DMG/rm:YV
MD5:	2638D21CE62C0B7738B093F75D7AD079

C:\Users\user\AppData\Local\Temp\bitt.rmvb	
SHA1:	582B8F3607046B4FE39B141BBAA792DFA232E56B
SHA-256:	0BAABBC641A84FB5ECFEF898C1DB1EF93B480CCFBFAFBFEBA3D33B1B89BDECFC
SHA-512:	6EAF4E1724E7B26267672639B57F41584F7312F8A2870E485F1FCCB314553D07EDE19F010188E3BFB2FBC59A628A54B1ACE62D4BF259C736CD6A4A86D3D2B11
Malicious:	false
Preview:	lXzJTjBGWExHqFpEZjfhCeKzC

C:\Users\user\AppData\Local\Temp\cloak.mp2	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.869245454481559
Encrypted:	false
SSDEEP:	3:Q9iotyIuxA/+0I:QTyNxaII
MD5:	18F6CCBFA502608CAA267F266D33E12B
SHA1:	03A91161E0BFC5031CD547AABE1399E5AF65FB38
SHA-256:	D8FD4BBF9119DE441078766C75FEAADC9055881A7F597D3F16EB6C467CB72970
SHA-512:	F0771B40CD85596388E3A5644479761AB8E98A1AA22A06F399C7603AEF19C56FA8B0423566DC13547C2F2EEFD3B30CAC13DEBCCF36CBAE15E2470E37EA6265C
Malicious:	false
Preview:	rlKiYxQNsSakimCKwJxodFHShdFwYgflHzWZlEZTmaUlgpflritom

C:\Users\user\AppData\Local\Temp\curium.m4	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	73
Entropy (8bit):	5.0646332508332
Encrypted:	false
SSDEEP:	3:6VAnmLm1mAHVYtw2siDL8i2xrGyyn:+CmLymAHVAw5iqxqyy
MD5:	77BC018BF1A2D16E03105FC2BF050C0A
SHA1:	6D2A38E3B4D987F850D009BE6D6A057A7E3FCC9C
SHA-256:	E63CBF675CAD78DC1220AE6566804B4FDDE700E9BAE8732DAF495CA9B4D981F0
SHA-512:	12B3117BFE4EB484683F2059CDD036F8AB38E8B2C6AC680E01C1EDD80853D47FAE1837CA453676A806028E918682C0D99D0EC851D5B4B60841925EB927B8E07
Malicious:	false
Preview:	CFJgwbpSkmSOseBCnCylkiBsDbEbtVjEHUWSoSoIhQOKuSSBrYrhoCozdDGWzsChNcyNMjPWW

C:\Users\user\AppData\Local\Temp\delicacy.ra	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	5.2123467390093605
Encrypted:	false
SSDEEP:	3:l7dU10NnoOGKMxopfdY2RmJpHc:m0XGKEopW2AJVc
MD5:	F8B64D575FCE190560D975E2A0F0CE76
SHA1:	73C8FF470D77285E121B8B5A860E759CBF2DA6A3
SHA-256:	3F1B695E2E104E384AA86E347B7EDE93251312B1F405952CD0FD79746CA80FEE
SHA-512:	6738D563AD000C8D1F475441E9D9A60764742BE8FA3FDE242F7D12EB34F7A27FC81E23C9EEC37B369151CB38BFA650F7E1A1381D7601CC12A62DEC2E9B02985
Malicious:	false
Preview:	PXpjRfxANRkSysGgKLGRkgwhnvMSHfymixRoQQMBEBToJaCjoeYLKbeXpXxaXWfehHkBzdmwoWtCFPLoyIX

C:\Users\user\AppData\Local\Temp\diopter.java	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	98
Entropy (8bit):	5.254930446501113
Encrypted:	false
SSDEEP:	3:xr3j4V6qhnwDWIy005zNISLPgr49GpFPMS:5UV6FDNn0lNvLPgZFr
MD5:	45573CE53218D6EA19C7CC41245FE267
SHA1:	231B7D38516BA11A3E5559B2FAFE95F91411BCAE

C:\Users\user\AppData\Local\Temp\diopter.java	
SHA-256:	8B634FD184C64F75BB77DAFECA97F82D6AD7850A34D42976A16CCA149CFEB43A
SHA-512:	B5099608CEA0876348D2BF39944B43663737B9E9D616B7EEA7D720B63DEAAE40BE4B23E9DB653F9FC06D1FDC91DD28AC175B62754B9917BBE20589C81CE0D3D
Malicious:	false
Preview:	pRVNSUFnRlZhrCJsYpgKmODWQSrnKmNnTBMEhrVkQGNlpKMhykyYeNyhoVpwSIHXENmomyhRzeOLUGtVqDWasnxJhCUmzLQjiw

C:\Users\user\AppData\Local\Temp\doorman.xcodeproj	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	4.765795487926596
Encrypted:	false
SSDEEP:	3:lx5853sFU8f6:I22U8C
MD5:	05EB58AA3CCBA32BC83E45AE10ACAFBE
SHA1:	F8EDE4F30B392A5EF706664A13AD15CE99D93B07
SHA-256:	513D9B46FFF583E0A64745ACEE6042D4022F834C89400CE164DAEC98BA5C3D43
SHA-512:	F57D6C60AF514CC09D00D04FDFF157D6A49B725790C7507B5656BE7F54FEDE52125A1BA2CF08B461A66958F150E71C3CFD729827B11CE162FB13CB64223A9D3
Malicious:	false
Preview:	BeHUVmvXJXXrTSdnYUJtqiNNIdVFMEQGxhoUzOd

C:\Users\user\AppData\Local\Temp\elfin.msi	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	5.030394654123194
Encrypted:	false
SSDEEP:	3:LkpV2AEiSqTOtAoSfnN:LkZEiSqTuAhfnN
MD5:	AAD3DCA56C72421509F79865EA213C40
SHA1:	4FADB10E78DCEDC576860A79A29BBA752EBADA1A
SHA-256:	97A9F32C0BE7C499EBEA5DD658AE26EC6D5E1AAFEA316FD7A88299A08A45179E
SHA-512:	9B097184DE64F7FC3DAB7788DAE1BDBA0003B74C0C92E5F50342598FBAE655F3A39C5C9E1AE98017B6518BEC9012DF51BCA7284027B335CAD28274B05A00B0E8
Malicious:	false
Preview:	vIXjubAMzOtMtbfyRxFRSIGyadqjiNOvgbBXZJZmQxgoIAKclWaSBiwd

C:\Users\user\AppData\Local\Temp\failsoft.css	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	35
Entropy (8bit):	4.672140159802107
Encrypted:	false
SSDEEP:	3:09ZxQL8kOu1dn:0VQIsn
MD5:	87EB13C401656709E21D621F47B18557
SHA1:	70494FD665DEA237528B096CA1199D0BA6E8CF02
SHA-256:	AFD0A828606FFA09B925CF31537B0E8BDB06A9BA69E2D0132DB778827C5E5E26
SHA-512:	8817C0E2AB282E511216915E5855DD5C1694F0A17FA220AE3B4BDD95094B676A12B515D359279191B345DE95D3C72DB9B6C48A95CD191A23BB15F90BEAA09C4
Malicious:	false
Preview:	FEIqSDTWXHbvTONLdpNHBYAXhshYPafMwfI

C:\Users\user\AppData\Local\Temp\fallout.tbz2	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	5.087161684484503
Encrypted:	false
SSDEEP:	3:KNQErr3jKmsTB+tHOQ4+In2dF/J+3YLn:tc4aHOQbI2df+3m
MD5:	5EAF6223A7ADE9F271332CA0F163BA08
SHA1:	D04304007AB79F32F02D12301BBBE0D2838CC800

C:\Users\user\AppData\Local\Temp\fallout.tbz2	
SHA-256:	E033621AD4E989DFE3E779187FC0C4B446654FE491C774282277D9493DC8A354
SHA-512:	96F12B9E5DA5838475687A49461FFE6F2BB98CE7B342E38DB6D64B91E6DA6BF2BCF9E08777F2554AC62A331BD1321AAC501A6864EA86D9F9BBCF904D26FE918 1
Malicious:	false
Preview:	xUZNKguEdCyNRrVocZkecBclvZiWYIALSwLRhogAJXEwQkBuAXdASSidfJVrBLULxFycscVZquXSCefRPwn

C:\Users\user\AppData\Local\Temp\guise.ar	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	81
Entropy (8bit):	5.245662466056343
Encrypted:	false
SSDEEP:	3:8K08hWULN1Z48sB1xCbdk:J0hSnZ4t1xMC
MD5:	B795A4FAA2FDD3BB6435D4D61F706F0A
SHA1:	5B415EF7EE8CC39613C2A4ABE5AD59CF537EEBAB
SHA-256:	5E1B7EF9DB3A6D7B379EAF37CDA2C0E0B5F18445DEF7F12D429DB21955A17274
SHA-512:	8F7CBA655AB4779CD48533FF03231D8213853F4DC99A92D8E1EFFD31CFBC7DE989BC6E0B9ACA861ED51486F14AF18E2EE29106802E76655DAECB6105573597(E
Malicious:	false
Preview:	daKXqBcaQNXQoBmHQHAqnhPpJhhcoqXzWgswesqMCcWhnoYvzLWyiOYxjFFoINHfgZWUhODGEiUKQwkgS

C:\Users\user\AppData\Local\Temp\halvah.scss	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.7399104927405515
Encrypted:	false
SSDEEP:	3:oQ/iyGT3tAoiY3Y382HmGRA:oqiyGT39t3cGGG
MD5:	699EB6004A0A1AEAD73B1ED4A1B243DE
SHA1:	2BA320B96697217B225942979CAC7281449AA045
SHA-256:	9172D32E6AE8183F23FB0956E38E6EE1BA51B4B04A2B2437B5B6160453B5BC71
SHA-512:	D608E010BA58A1B25080C0BD71964ABF55F3187644041926C1CFDD2A89B93A748E5DAD3D41453DE6D06F29F1C6B594325E9870CA8644753F2F5492DB6D6C591
Malicious:	false
Preview:	QtXQsKHZAMQWzzSRIGRHesrtdGwNRVQRHXJIOJQabCXkFtHjvtLle

C:\Users\user\AppData\Local\Temp\hitch.rst	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.942275084497218
Encrypted:	false
SSDEEP:	3:sSjWORn3sVmw0H:sUl3omw8
MD5:	C149DE3F79DCD0BD05A1B94DB1C238F2
SHA1:	943CD6C632C0731F4A696CB654470E1CD3496473
SHA-256:	70C0F8A99E5E744CA3418D8D0C15CD8A6ED59ECE69C073243456EE32A658B47C
SHA-512:	0333661DD49938AA7EB83B791A925ECEA0E771611B5B09D12F09F6B70976273D81E06C01E2295D6EBCB10DF150FA0A7755DBE105244414F7B7868BE70DAA20BI
Malicious:	false
Preview:	XVoTFAAHalpmRnuTukcsBExTUtRIsNoNwbqbchGQqeDJ

C:\Users\user\AppData\Local\Temp\hour834.flv	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	4.004886164091842
Encrypted:	false
SSDEEP:	3:n/yZuLxr/fWmhn:/VLl+Wn
MD5:	DC09826292EC48B0CBD504D2BE3B8167
SHA1:	83B1443E3F88C85DD2BD789D36BAB2A1C8679FA7

C:\Users\user\AppData\Local\Temp\hour834.flv	
SHA-256:	F164F9BB2D9FABB549AAB68819C3255F34BEAB75E0DDFA618B059EE0C6C65369
SHA-512:	E559E6AC52DD6BC01CC1191314A214216F5FCBE86C4B311171D0AA60EB4DDDB528D228248FDBF0D824144599A54F701AB78808BA38C7493E265E1327FADCE2 6
Malicious:	false
Preview:	TEuFFrWroyowKnTNDLzsCD

C:\Users\user\AppData\Local\Temp\legion.dxf	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	4.1219280948873624
Encrypted:	false
SSDEEP:	3:WJWd:WJWd
MD5:	DD24671D9404E9C36CA2D0728F0CF615
SHA1:	3B73D1D1287704B1C8D7A97E7999E57B3E4C65E6
SHA-256:	611ABFA58D9883BE637F93A6FD23A252721AEF5AB5D5581BA43C0A7061455F5E
SHA-512:	3C503C3FD023BF949F193BDFBAC261BB03F902CA72DBADA2736F27AA6AE26034786ADC424620D4904C30B85086F659D6AE5BD100E2B8303B2E1065E32DE59B 0
Malicious:	false
Preview:	UXTrMEtRJSRqufisIYjj

C:\Users\user\AppData\Local\Temp\manufacture.jpeg	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.41189187902552
Encrypted:	false
SSDEEP:	3:JGLtaQApdLBon:2tson
MD5:	1B763728C91574A0122FB0A343902049
SHA1:	F2E5A437F933663D0FD76E835E6686C5978EB9C7
SHA-256:	CA9ED7892C09527B07317AB1499A4AC047FCDE0851CCA110D062CABA044EA331
SHA-512:	ECB4AF02FB7A52530BB62AAE2394CE969BCF5D35FDF9035608D99851098D51F1BF7A2030AD3C2D2C1FDB8D5F4BA4F28B19FAF099B08F99A6D66732087D4D2F 3
Malicious:	false
Preview:	uFOrcyVeeGHVyuYdcnHjhuueEEDHxZSQdiSLs

C:\Users\user\AppData\Local\Temp\nowhere.avchd	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	4.209867121904035
Encrypted:	false
SSDEEP:	3:axRPi2tsn:ax1q
MD5:	F8BC2F62C3C91AE51ECFAF2F7A2FCF5E
SHA1:	C4279B768DA0B257C09A9D264DC4EAF409533E32
SHA-256:	7FF369BFE78742ED731BA80D19F48EB6F2DD050DA4B4A92E3131F911E87B9AD7
SHA-512:	B6A87962E5EC455F56CA05BCD4F33B065D4B7B9F762428F302E59EA1635C442769B890F0F04504A9AEEA91E1A31FFDBFA135C522771DC680036A2005E4842706
Malicious:	false
Preview:	zwTyeEqTLrOiwJBwdjJSpYPGOG

C:\Users\user\AppData\Local\Temp\preferential.qt	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	5.106092007632401
Encrypted:	false
SSDEEP:	3:YmV0z5awWuBy8hvPpgFQZeOv9Pvg:YmV0z51x7XC6eOvG
MD5:	18140628248CBBD9016D35781288BB87
SHA1:	9C139E62099A1D6A2E1CF055930DA0CE61904013

C:\Users\user\AppData\Local\Temp\preferential.qt	
SHA-256:	6A839A398ADBB2CE4C8EBC06BBB83157099C24EBC03D2A0EE4119B1C6993E86F
SHA-512:	5A81AC280C6477FA18D5123A550BD80147D698F640602384D401E3F6CE486FE4AB4E8104C82CDDAD5D3DA161EF9F251D42E1C2D1362CC2152C9B93B28A4F2E
Malicious:	false
Preview:	zQNhjaLODlspXAFVfkyDwLxWsPAMgmrWVxTANxJzkDJjLEWJqCQeKuadVsaIAlwZSXAzJxjiKE

C:\Users\user\AppData\Local\Temp\prestige.zip	
Process:	C:\Windows\System32\wscript.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	262198
Entropy (8bit):	**7.994396440050114**
Encrypted:	**true**
SSDEEP:	6144:7e/3xyCNPKhR+lFedsL6uEcTEXFIqkoOY7+1HC:LYUMaT7X2/4n
MD5:	056CFF5AB72065AD83271A7CC577DB20
SHA1:	A999541AF64F34CB8A112062244971101763 31CE
SHA-256:	E660AE12199521288D039C5594A8FF803D0C82B005223CAC05ABA12F43B24729
SHA-512:	40E6917DF21F0B4DD09C603226150B48FF3082923766F2D4FCBD30065BBCDE90CE5A192DD2A8D88996EF9512E54991DAC8DB907ECFCFAEEAA68AA08E930F6D0
Malicious:	**true**
Preview:	PK.....P..Q..2.....`.....Oxnard.rb..XSK.8....`P.^.....]:(%B"`....(...P.....=vT...g.....{...}..'.g.....x.2:.h.B...CH.a/;.2.z...#y.g..pDg...G....._.p..._.!.....B.....1V..?..H...+A.....^.X.w..u...U..i...z..`.....}D.o.....K...:U...G..r.!..Zf.....?.4m...;1.V.....U.....x.../h.OUDj*Q..k@Hr}BZ...?..4&...{....h...=V.U.....2.....'.....[.5"2....PZ.?..u.....imX.9.....e..B!.h. .i.....l.8.p...@.....x.#...!.....5...o.~.....c.+.w.....6.....`(.X.0.Y...2...\.(.....@W.....!.s.....l...8.p.....: ....`..;@..T.D.u.[...\..... ~...NU.<..v<..<..2..$.A.p^..;...`.}u~G.:.*.*.|a(.....x....[...F..v.t.K,...&._.....>...Ni..T85..)/)Q1..C..).4%.....A+{,k7...N%*...k1*U.!y.yB.FE..qI.?.....h..f.2.2.....JF....y%.I..;c.b.L.;..<~~Y.E..?n.....g.....<..r.....>..h}Sq#..#..r....Tr{.....Z.!....bYk.Vs.u.n..Gr&..+A.....F8..."@..0..9.*9...tV~H.s.....7...P1Z...8.+Q.

C:\Users\user\AppData\Local\Temp\programmed.3gp	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	47
Entropy (8bit):	4.713955340947276
Encrypted:	false
SSDEEP:	3:FATWUa/xHsk1RLn:FATWv1RLn
MD5:	470239F8744F989F7DC05CE1A6B673ED
SHA1:	BC2C4C5FA8812618386E2398C61068BEA1FEDD70
SHA-256:	E484636BDC32A9983DE6655BFF77C085C946AB651E14A6D8C129BCA120129AC2
SHA-512:	2B2041426237AC9CD4ADAFDEDF0457FC5BA243753C0462C43040BDEDAF9E43CCB10C75E81EAD8B1DC5A6378804A9531C5DE7E36E832A4AB2CC9D56B18F97536
Malicious:	false
Preview:	WcAOBevuiPOFbVmxsxZTbfTBZfkkSrUgziFlNndOgZPOezF

C:\Users\user\AppData\Local\Temp\rectifier.xcodeproj	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	4.209867121904035
Encrypted:	false
SSDEEP:	3:AgFeso0o:/Cl
MD5:	942E89877F6401D47FA2915AA8FD7EAD
SHA1:	30598B643B438725CEA08E125AEA38A9B15B70C4
SHA-256:	052832F9CA187A3786EC79BD5EE1C3AA5DF067BC1599F0ED31769E63AB239481
SHA-512:	AA17D2628B8572F69837D6550B8D8F9FBFB3AA94104DA9DA79A249C81F551C000C6A10B0BF4177A253FA0BEFAB683C03902C9E9CFB1C7BD6861950019FCC69E7
Malicious:	false
Preview:	SuUwxmPStrpIgGujBMPeJjgsRg

C:\Users\user\AppData\Local\Temp\rustic.tbz2	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.084962500721157

C:\Users\user\AppData\Local\Temp\rustic.tbz2	
Encrypted:	false
SSDEEP:	3:R2xlS0:wu0
MD5:	C97A0A530A9912484E17E4E1AB6B601E
SHA1:	3338E31D8547A4B4F59B694BBB4B78374F6E3348
SHA-256:	3071FBFCE721232FF91C7148854533A0F45AEF024A204C1612BCA4CD6BA00CF8
SHA-512:	D687F9C0027C06178DF52E91BB90E839C1392EE92240F245F7CA547FC4C63B2201CB048F57874616266C5A3360748AD32762AA5BF8BD9CA9F527FBC7155CC1C
Malicious:	false
Preview:	lKdoHRZkaRbxRWBgIlyeRPlM

C:\Users\user\AppData\Local\Temp\shimmy.py	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.9690016298759936
Encrypted:	false
SSDEEP:	3:gz9OxOC:ggxOC
MD5:	ED0EEA1BCBCBFDD03A904212D7F8D114
SHA1:	7DB8BE121D194FF99A641664C8C93466FD65CCCC
SHA-256:	40CA1795953988C8A19F5492136018BBC3594B23C71782165095E4AD310BDD9F
SHA-512:	9E27828D384837874B83245B5112220E5DC612A91132DF13138A263642EE8D23D81D4E87EFCE33549B0C8F730AA168AD81FA38F85F58D92E27A3C4E685BDCD5E
Malicious:	false
Preview:	NJGrVQakGwlXlwaltSQMivT

C:\Users\user\AppData\Local\Temp\signify.tif	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	5.169146220500345
Encrypted:	false
SSDEEP:	3:bnIZ0GJq8GCDJ6QPVWTGn:EKeqdQtln
MD5:	FEEF16A74C73940EFB42E59907B9EA65
SHA1:	39D209EF251A38F09D8B57FD5A456880546F32FB
SHA-256:	40EB90E5A53FA84209B10D596D4DC390A6D1372B1CCF83D2F241521108D7CC56
SHA-512:	8A4887DECF4A0A4E2F8A47D96EBA05890B51A1855D1C08B08BC4B4D394696F7AFF952B4808F2F9A5054FB40E981BE33C6FE20AEEB331CC85FA47E226706EE05 2
Malicious:	false
Preview:	bFbnlprZeOGQCOalDyTaFBcnSseDuEvCWVQbvNjgWhtJfFIHXpiMPtyCirAj

C:\Users\user\AppData\Local\Temp\switchblade.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	4.186704345910023
Encrypted:	false
SSDEEP:	3:UkD+:UkD+
MD5:	1B9DEAFFEAB94DC6200DC5F8E979FB65
SHA1:	0A805113E7015386199996FA5791BDAE0669A444
SHA-256:	BD1B8E317206E55D54175BDAC393D1DA4883216095F70012B9F4F88A09A13B92
SHA-512:	C0A574E8E46D1D360D317E1EAAC453027A876D194696C525D57B5377E32DB374D6B6530C8FB4751665CA9C6F384CDBF728ED2CEA7ACB6D6160CFB5366BFBD9 C
Malicious:	false
Preview:	pcPSYkuHEhRIYWSaXiOjjb

C:\Users\user\AppData\Local\Temp\taro.mov	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	83

C:\Users\user\AppData\Local\Temp\taro.mov	
Entropy (8bit):	5.0856472625679645
Encrypted:	false
SSDEEP:	3:3+jUUra8xS0BwLSn2O9n:3+oya6B/
MD5:	D12760FD1671E768A2B2D38C58C06F90
SHA1:	F401A0DA110A554C911D1016E25C530D69A735C2
SHA-256:	7ED4EC3376B7EBA348C1D5295F4A115444B3DCC14E1C5380FEF16B4AA503A2D9
SHA-512:	6D9E5AF277CB98D6E68B679FACD485A6D314FD171A74EFC7FA02E68BA9B0DCDEE3545DE66B5D09E6D20575FAD99047ADAF7C4D73DB589EA0E02F98B9F9DA4DA9
Malicious:	false
Preview:	GuowRHWeEpOFzRlbSNsCAUqqNqAjFoKGqsaGcUvBFXqwBeRcCvBjvoVZGUnHzrKRFKkKYBIivqPoAnbOQxQ

C:\Users\user\AppData\Local\Temp\triode.sh	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.838562939644916
Encrypted:	false
SSDEEP:	3:KKHC0KeOg3ZJH3mrFLn:KkBLR3Z5mrFL
MD5:	E9D578EB7D721DD650F08EF8FA196FF9
SHA1:	D3B988DF1A625F3CDB1DC1B9D232B335BA42D1AB
SHA-256:	238AD1BB3A413AAF0BCA367BF41FCE2AE056A40C50876A5B99A36BB6A21B9027
SHA-512:	83CA7BD1A65A266021F3D8A80E95FB6C7B26E02F471D36FAB93C757144766308C982B38D29A6B0671F833160C47CBEF7C2E6B63CFFDFCB02D3BA92E42906085
Malicious:	false
Preview:	BotSHieTVBSQfBPJwILgLNYBkgFZhYELPesfAIlbRXnmNtFFoI

C:\Users\user\AppData\Local\Temp\wildfire.md	
Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	3.459431618637298
Encrypted:	false
SSDEEP:	3:rsQo:y
MD5:	7750CEE87A9AF0A3CC291199AD65D278
SHA1:	2580B8ED57C97C6505CA3281A220CA3536BA3E94
SHA-256:	19E318B5517FD99B458A48FCA73BF9FB4C6B332FC815F590FE9170A9BE3F9398
SHA-512:	ED085B9155DD9C5A5B5F84A83B7EF53EDE1B1C02CAC081DD2601A36F9DD2FAF00267C1AC2F72A070DE772CA011A14E735C6B15E140B11936F49F0556525E122
Malicious:	false
Preview:	dRxESlluLBC

C:\Users\user\AppData\Local\Temp\~DF86F75BB46A075095.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933
Entropy (8bit):	0.4066799289052363
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRRJF9l8fRRL9lTqRhLPX8qUPc:c9lLh9lLh9lln9lln9loB9loh9lWfj7Z
MD5:	72571B70D43DBBF3F16DD8DF576A9A0C
SHA1:	F13021A674330CC7999888A9C512B7E0A84F352A
SHA-256:	A294E8BDB9B485B0BD5BEB402645F162A7DE542938C72487634D26700384A0E1
SHA-512:	E47350DB78599C9FED0047E12A9B502C6DC657FACBBFD09BCB8E0033882D515576E1F9AF6E30E248CFC28A900074213232DD4ABA3F0C860F8A8AAC699B0BC1E
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFCE3CEB3DA92FCDD0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Temp\~DFCE3CEB3DA92FCDD0.TMP	
File Type:	data
Category:	dropped
Size (bytes):	40273
Entropy (8bit):	0.6944984738201564
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+QWMNW/SWny47Uj9x0SWny47Uj9hSWny47Uj9C:kBqoxKAuqR+QWMNW/S2SyS2ShS2SC
MD5:	C468E90E5C41BFDABF93EE54FE326E8C
SHA1:	C6699276B88E5C2DD5B9A95163C91080685BA9A8
SHA-256:	BE53EF5B8B010D83AA6A8938B01F932C943EF96AF62913AC59637BFFFFD0D835
SHA-512:	D7546ADF180CBD51DEF94C22C8A0C20518E6A599ECE02FBF0F5E10A821ABC4AD17876D30C0CA068379908B19F71EB1DF1A1B793CDA0ADDDA324562ECCF302D3
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.492441125094552
TrID:	
File name:	view_attach_72559.vbs
File size:	1478801
MD5:	29933320f02dfc13999ff70cd960a291
SHA1:	29db771aef8cfe3231e5f1b077bf49c096777043
SHA256:	7c4f0d072bdbf9aaba20f96173a9274376d589a171ff96d4bfbb56427ea17f7c
SHA512:	087d7429d11b1352da4e196737b9c8967cd69bc119ca72d40c6a4e1ebf72cc05a8686466aedbd2c090f5d4d57cd85a0a8df7e259e31bd9e6d0582d32cc6365d1
SSDEEP:	12288:zVc6VAbGS/oDhshU7IUjDmllrwvcW+LWZBD3yvONpgJJ6khEtCeiy9ZNeq2C/kyp:pBGuhMUsUvmHVWZBD9ABMywsk
File Content Preview:	' monkeyflower, Pitney amongst pestilent schizoid Schiller Protophyta biscuit tolerate Libreville Ann drill imbue, 9900734 arithmetic. argillaceous inculpable, 4346106 adduce Carrie Goldman Detroit ..' diverse assassinate stadium Beckman, inexorable Sun

File Icon



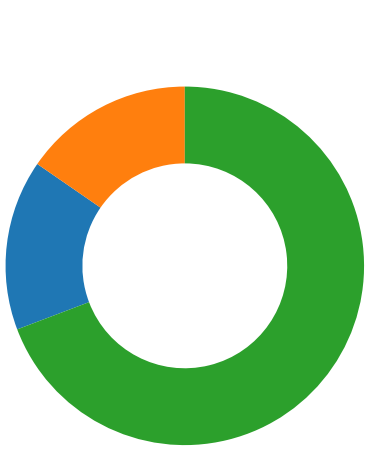
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Network Port Distribution

Total Packets: 65

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 20:41:23.238269091 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.260381937 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.260512114 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.262553930 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.284806967 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.287451029 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.287473917 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.287493944 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.287514925 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.287527084 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.287575960 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.332202911 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.355103016 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.444277048 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.475173950 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:23.507332087 CET	443	49753	88.99.66.31	192.168.2.4
Dec 16, 2020 20:41:23.553630114 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:41:38.434016943 CET	49753	443	192.168.2.4	88.99.66.31
Dec 16, 2020 20:42:23.770611048 CET	49771	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:23.771327019 CET	49772	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:23.824987888 CET	80	49771	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:23.825148106 CET	49771	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:23.825511932 CET	80	49772	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:23.825583935 CET	49772	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:23.826311111 CET	49771	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:23.922852993 CET	80	49771	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:24.061244011 CET	80	49771	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:24.061439991 CET	49771	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:24.063460112 CET	49771	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:24.117839098 CET	80	49771	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:24.332195044 CET	49772	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:24.426537991 CET	80	49772	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:24.534838915 CET	80	49772	46.173.218.93	192.168.2.4
Dec 16, 2020 20:42:24.535032988 CET	49772	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:24.536889076 CET	49772	80	192.168.2.4	46.173.218.93
Dec 16, 2020 20:42:24.591003895 CET	80	49772	46.173.218.93	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 20:40:50.726007938 CET	63153	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:50.750422001 CET	53	63153	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:51.717070103 CET	52991	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:51.744180918 CET	53	52991	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:52.738962889 CET	53700	53	192.168.2.4	8.8.8.8

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 20:40:52.766078949 CET	53	53700	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:54.042150974 CET	51726	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:54.079418898 CET	53	51726	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:55.356266975 CET	56794	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:55.380563974 CET	53	56794	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:56.389739990 CET	56534	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:56.417006016 CET	53	56534	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:57.437122107 CET	56627	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:57.464571953 CET	53	56627	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:58.553380013 CET	56621	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:58.577672005 CET	53	56621	8.8.8.8	192.168.2.4
Dec 16, 2020 20:40:59.530651093 CET	63116	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:40:59.554965973 CET	53	63116	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:00.513315916 CET	64078	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:00.540585041 CET	53	64078	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:01.485591888 CET	64801	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:01.509982109 CET	53	64801	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:02.473906040 CET	61721	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:02.498377085 CET	53	61721	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:13.906704903 CET	51255	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:13.931055069 CET	53	51255	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:18.972353935 CET	61522	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:19.005130053 CET	53	61522	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:23.192785978 CET	52337	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:23.230571032 CET	53	52337	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:36.757635117 CET	55046	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:36.795226097 CET	53	55046	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:37.248379946 CET	49612	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:37.272828102 CET	53	49612	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:37.686522007 CET	49285	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:37.725173950 CET	53	49285	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:38.175614119 CET	50601	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:38.200042963 CET	53	50601	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:38.405529022 CET	60875	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:38.440915108 CET	53	60875	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:38.533036947 CET	56448	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:38.565752029 CET	53	56448	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:38.914482117 CET	59172	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:38.947454929 CET	53	59172	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:39.349355936 CET	62420	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:39.384587049 CET	53	62420	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:39.715612888 CET	60579	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:39.748270035 CET	53	60579	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:39.987878084 CET	50183	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:40.020840883 CET	53	50183	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:40.585829020 CET	61531	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:40.621351957 CET	53	61531	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:41.328526974 CET	49228	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:41.355667114 CET	53	49228	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:41.706912994 CET	59794	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:41.742779970 CET	53	59794	8.8.8.8	192.168.2.4
Dec 16, 2020 20:41:54.936301947 CET	55916	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:41:54.973997116 CET	53	55916	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:22.291284084 CET	52752	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:22.328221083 CET	53	52752	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:23.441163063 CET	60542	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:23.758465052 CET	53	60542	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:25.879936934 CET	60689	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:25.907159090 CET	53	60689	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:27.752015114 CET	64206	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:27.787190914 CET	53	64206	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:52.288115025 CET	50904	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:52.315593958 CET	53	50904	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:53.282437086 CET	50904	53	192.168.2.4	8.8.8.8

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 16, 2020 20:42:53.309823036 CET	53	50904	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:54.280514956 CET	50904	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:54.308274984 CET	53	50904	8.8.8.8	192.168.2.4
Dec 16, 2020 20:42:56.303597927 CET	50904	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:42:56.331151009 CET	53	50904	8.8.8.8	192.168.2.4
Dec 16, 2020 20:43:00.312500000 CET	50904	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:43:00.347820044 CET	53	50904	8.8.8.8	192.168.2.4
Dec 16, 2020 20:45:37.628688097 CET	57525	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:45:37.653048038 CET	53	57525	8.8.8.8	192.168.2.4
Dec 16, 2020 20:45:37.834352970 CET	53814	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:45:37.858638048 CET	53	53814	8.8.8.8	192.168.2.4
Dec 16, 2020 20:45:38.259187937 CET	53418	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:45:38.299994946 CET	53	53418	8.8.8.8	192.168.2.4
Dec 16, 2020 20:45:41.458463907 CET	62833	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:45:41.502763033 CET	53	62833	8.8.8.8	192.168.2.4
Dec 16, 2020 20:45:44.932238102 CET	59260	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:45:44.956572056 CET	53	59260	8.8.8.8	192.168.2.4
Dec 16, 2020 20:45:45.273381948 CET	49944	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:45:45.306265116 CET	53	49944	8.8.8.8	192.168.2.4
Dec 16, 2020 20:47:59.014956951 CET	63300	53	192.168.2.4	8.8.8.8
Dec 16, 2020 20:47:59.039118052 CET	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 16, 2020 20:41:23.192785978 CET	192.168.2.4	8.8.8.8	0x2683	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Dec 16, 2020 20:42:23.441163063 CET	192.168.2.4	8.8.8.8	0xeddc	Standard query (0)	golang.feel500.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 16, 2020 20:41:23.230571032 CET	8.8.8.8	192.168.2.4	0x2683	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Dec 16, 2020 20:42:23.758465052 CET	8.8.8.8	192.168.2.4	0xeddc	No error (0)	golang.feel500.at		46.173.218.93	A (IP address)	IN (0x0001)
Dec 16, 2020 20:45:37.653048038 CET	8.8.8.8	192.168.2.4	0xcee7	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- golang.feel500.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49771	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 20:42:23.826311111 CET	6437	OUT	GET /api1/DIwBQ8Rv7j7xfqFjg4_2BA9/g0fzfaOWqj/Y_2BPGiAPfzGcs2Be/I_2BUuYEc0ea/KBkab56Bm_2/FWmqnzUOX9_2B0/YbRWfB6IMq7TSr21K5FNM/xWmFuq_2FeEONGMO/1ZuPh_2FNFAeM3T/FM11WlspOeJ_2FqYpl/U_2F6jwXu/YXiyreYoS1UAkST_2FVa/JT_2Fx9W7QvoG6HJsdC/ExFIoNdpiPpyKG7cmJGp40/huNnlqBJ9uVVH/QyyRFE1b/30os8htaDb_2FAitT_2BOsm/SKMxwp3_0A/_0DyvsrFrDpoMB3eg/_2BPhnWhGFuU/FPA93GCv8Zd/FBoszW1uVg1_2B/gtKiRyRf4RAjLF4_2F0P1/_2FR HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: golang.feel500.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 20:42:24.061244011 CET	6437	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 16 Dec 2020 19:42:24 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	192.168.2.4	49772	46.173.218.93	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 16, 2020 20:42:24.332195044 CET	6438	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: golang.feel500.at Connection: Keep-Alive
Dec 16, 2020 20:42:24.534838915 CET	6438	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 16 Dec 2020 19:42:24 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

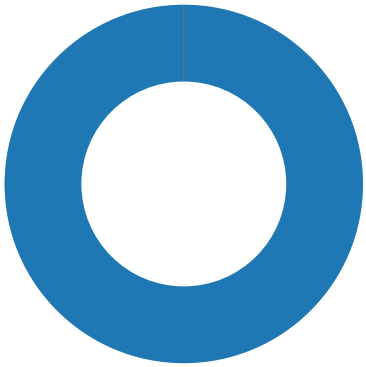
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 16, 2020 20:41:23.287514925 CET	88.99.66.31	443	192.168.2.4	49753	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020	Sun Nov 21 00:59:59 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 960 Parent PID: 3424

General

Start time:	20:40:55
Start date:	16/12/2020
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\view_attach_72559.vbs'
Imagebase:	0x7ff6270c0000
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\prestige.zip	success or wait	1	7FFA9A0B721F	DeleteFileW
C:\Users\user\Desktop\view_attach_72559.vbs	success or wait	1	7FFA9A0B721F	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\view_attach_72559.vbs	unknown	128	success or wait	11554	7FFA9A0A17B5	ReadFile

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\view_attach_72559.vbs	unknown	128	end of file	1	7FFA9A0A17B5	ReadFile

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: 5528 Parent PID: 800

General

Start time:	20:42:21
Start date:	16/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff67fea0000
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	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: 5500 Parent PID: 5528

General

Start time:	20:42:22
Start date:	16/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5528 CREDAT:17410 /prefetch:2
Imagebase:	0x1020000
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