ID: 1437978
Sample Name: bRlvBJEl6T.exe
Cookbook: default.jbs
Time: 09:28:08
Date: 08/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

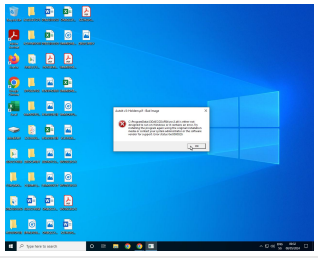
Windows Analysis Report

bRlvBJEl6T.exe

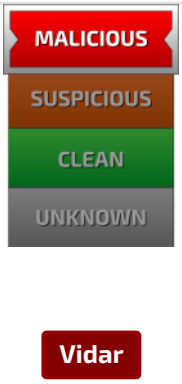
Overview

General Information

Sample name:	bRlvBJEl6T.exerenamed because original name is a hash value
Original sample name:	4efb38b934e42..
Analysis ID:	1437978
MD5:	4efb38b934e42..
SHA1:	121fe04be542a..
SHA256:	46b8ec4f65622..
Tags:	exe
Infos:	



Detection



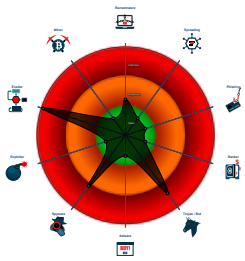
Vidar

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

Signatures

- Detected unpacking (creates a PE f…
- Found malware configuration
- Malicious sample detected (through…
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for subm…
- Sigma detected: Search for Antiviru…
- Yara detected AntiVM3
- Yara detected Vidar stealer
- C2 URLs / IPs found in malware con…
- Drops PE files with a suspicious file…
- Machine Learning detection for drop…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- bRlvBJEl6T.exe (PID: 916 cmdline: "C:\Users\user\Desktop\bRlvBJEl6T.exe" MD5: 4EFB38B934E4247C49AC1DE662B4FE2C)
  - cmd.exe (PID: 7180 cmdline: "C:\Windows\System32\cmd.exe" /k move Classics Classics.cmd & Classics.cmd & exit MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 7188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - tasklist.exe (PID: 7252 cmdline: tasklist MD5: 0A4448B31CE7F83CB7691A2657F330F1)
    - findstr.exe (PID: 7260 cmdline: findstr /I "wrsa.exe opssvc.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
    - tasklist.exe (PID: 7296 cmdline: tasklist MD5: 0A4448B31CE7F83CB7691A2657F330F1)
    - findstr.exe (PID: 7304 cmdline: findstr /I "avastui.exe avgui.exe nswscsvc.exe sophoshealth.exe" MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
    - cmd.exe (PID: 7340 cmdline: cmd /c md 334343 MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - findstr.exe (PID: 7356 cmdline: findstr /V "BbcAdvisorsAndaleNowhere" Lease MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
    - cmd.exe (PID: 7372 cmdline: cmd /c copy /b Pharmacy + Experiences + Creating 334343\e MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - Holdem.pif (PID: 7388 cmdline: 334343\Holdem.pif 334343\e MD5: 6EE7DDEBFF0A2B78C7AC30F6E00D1D11)
    - PING.EXE (PID: 7404 cmdline: ping -n 5 127.0.0.1 MD5: B3624DD758CCECF93A1226CEF252CA12)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	**http**://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

Threatname: Vidar


```
{
  "C2 url": [
    "https://steamcommunity.com/profiles/76561199680449169"
  ],
  "Botnet": "94a10776e7ea3334ad5fb8a76bbebf42",
  "Version": "9.3"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000003.3135450130.00000000038AB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0000000A.00000002.4096902193.00000000011D6000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0000000A.00000003.3135086350.00000000011D7000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0000000A.00000002.4096786614.00000000010B0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
0000000A.00000003.3135223602.0000000001141000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.Holdem.pif.1025bd8.1.raw.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
10.2.Holdem.pif.1025bd8.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x1f3f8:$s1: JohnDoe • 0x1f3f0:$s2: HAL9TH
10.2.Holdem.pif.1025bd8.1.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
10.2.Holdem.pif.1025bd8.1.unpack	INDICATOR_SUSPICIOUS_EXE_WindDefender_AntiEmaulation	Detects executables containing potential Windows Defender anti-emulation checks	ditekSHen	• 0x1e7f8:$s1: JohnDoe • 0x1e7f0:$s2: HAL9TH
10.2.Holdem.pif.38a0000.2.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 1 entries				

Sigma Signatures

System Summary

Sigma detected: Execution of Suspicious File Type Extension

HIPS / PFW / Operating System Protection Evasion

Sigma detected: Search for Antivirus process

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Compliance

Detected unpacking (creates a PE file in dynamic memory)

Networking

C2 URLs / IPs found in malware configuration

Uses ping.exe to check the status of other devices and networks

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (creates a PE file in dynamic memory)

Persistence and Installation Behavior

Drops PE files with a suspicious file extension

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Uses ping.exe to sleep

Stealing of Sensitive Information

Yara detected Vidar stealer

Tries to harvest and steal browser information (history, passwords, etc)

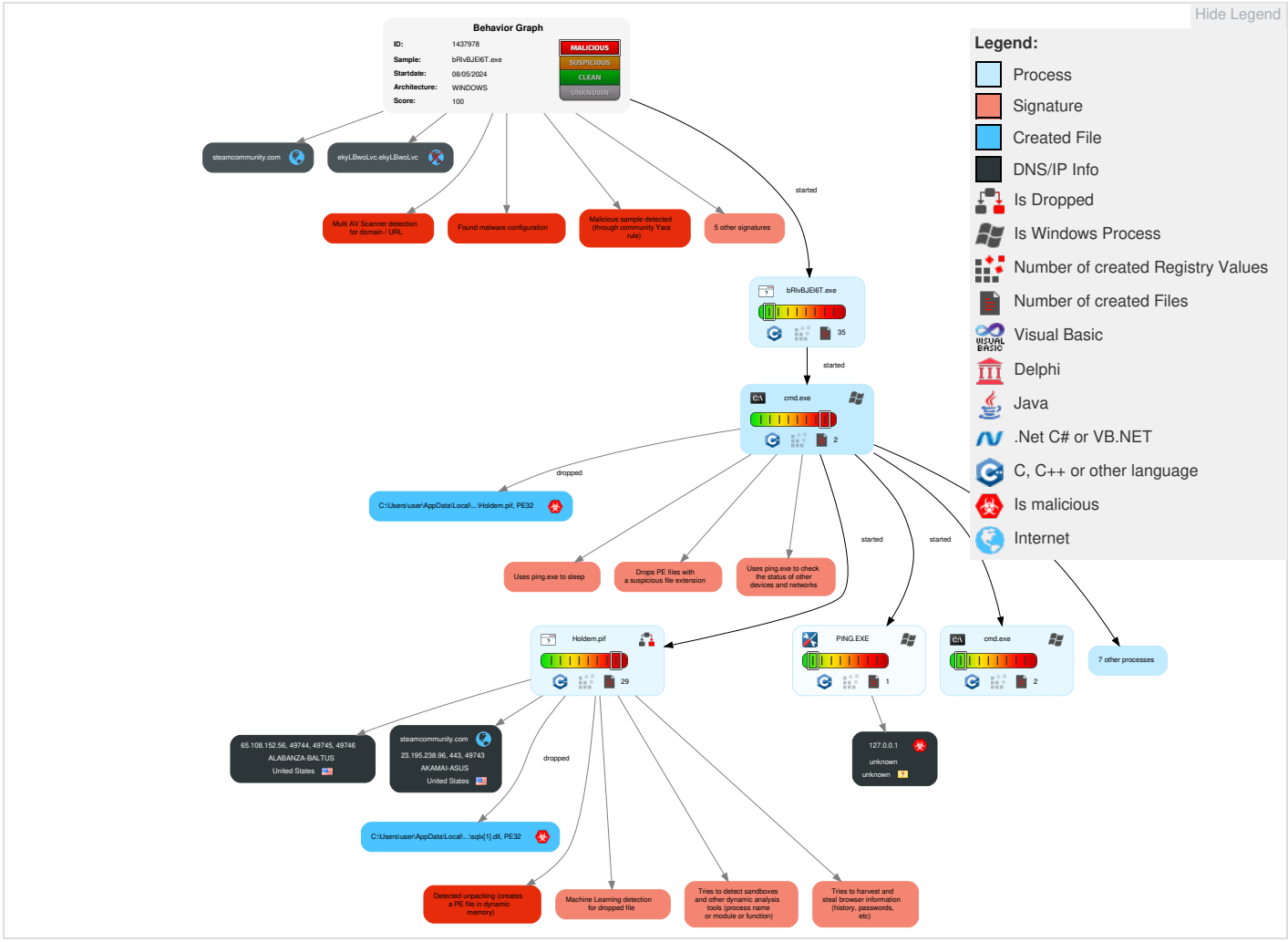
Remote Access Functionality

Yara detected Vidar stealer

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	2 Valid Accounts	1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	1 System Shutdown/Reboot
Credentials	Domains	Default Accounts	1 Native API	2 Valid Accounts	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	1 Data from Local System	1 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	2 Valid Accounts	2 Obfuscated Files or Information	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	2 1 Input Capture	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	2 1 Access Token Manipulation	1 Software Packing	NTDS	3 6 System Information Discovery	Distributed Component Object Model	3 Clipboard Data	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	1 2 Process Injection	1 DLL Side-Loading	LSA Secrets	1 5 1 Security Software Discovery	SSH	Keylogging	1 3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 1 Masquerading	Cached Domain Credentials	4 Process Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	2 Valid Accounts	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	2 1 Access Token Manipulation	Proc Filesystem	1 System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 2 Process Injection	/etc/passwd and /etc/shadow	1 Remote System Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	Dynamic API Resolution	Network Sniffing	1 System Network Configuration Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement

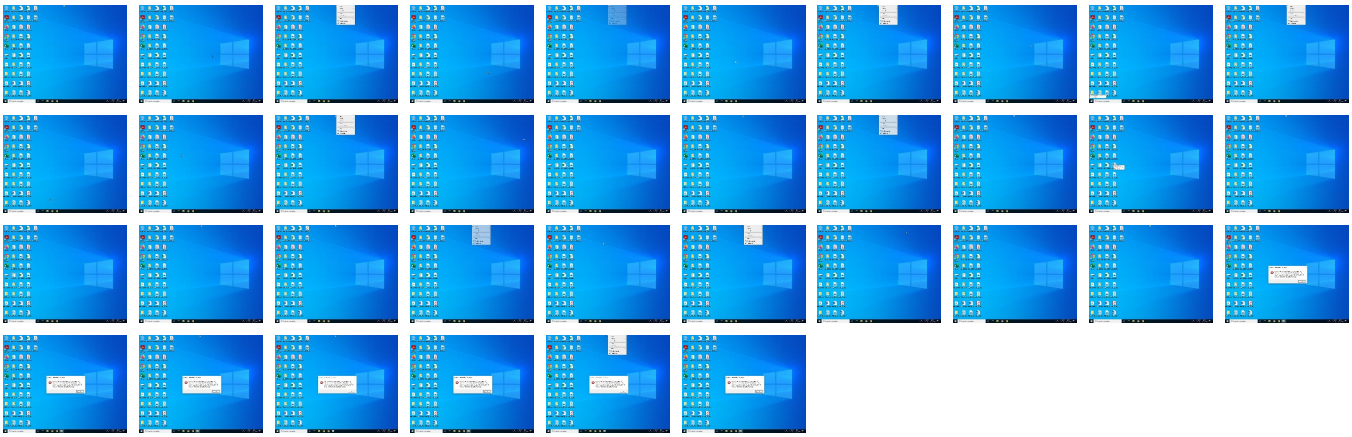
Behavior Graph



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
bRlvBJEl6T.exe	56%	Virustotal		Browse
bRlvBJEl6T.exe	39%	ReversingLabs	Win32.Trojan.Nekark	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	7%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://65.108.152.56:9000/(	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/mozglue.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/)	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/softokn3.dlldge	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://65.108.152.56:9000/nss3.dll_	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000	0%	Virustotal		Browse
http://https://65.108.152.56:9000/vcruntime140.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/(	11%	Virustotal		Browse
http://https://65.108.152.56:9000/vcruntime140.dllw	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/nss3.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/nss3.dllft	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000el	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/freebl3.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/i	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/f35bosoft	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/D	0%	Avira URL Cloud	safe	
http://https://community.akamai.steamstatic	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/soft	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/softokn3.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/mozglue.dllEdge	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/B	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/D	7%	Virustotal		Browse
http://https://65.108.152.56:9000/vcruntime140.dllser	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000ing	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/A	0%	Avira URL Cloud	safe	
http://https://65.108.152.56/	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/vcruntime140.dll_7)	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/vcruntime140.dll=cv6	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/freebl3.dllB	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/.152.56:9000/softokn3.dllessionKeyBackwarda_1	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000l	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/msvcp140.dll	0%	Avira URL Cloud	safe	
http://https://65.108.152.56:9000/	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
steamcommunity.com	23.195.238.96	true	false		high
ekyLBwoLvc.ekyLBwoLvc	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/profiles/76561199680449169	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	JJJKEHCA.10.dr	false		high
http://https://65.108.152.56:9000/(	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://65.108.152.56:9000/)	Holdem.pif, 0000000A.00000002.4096967324.0000000001273000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	JJJKEHCA.10.dr	false		high
http://https://steamcommunity.com/?subsection=broadcasts	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/mozglue.dll	Holdem.pif, 0000000A.00000002.4097499400.00000000039C8000.00000040.00001000.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/softokn3.dlldge	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000	76561199680449169[1].htm.10.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://store.steampowered.com/subscriber_agreement/	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/vcruntime140.dll	Holdem.pif, 0000000A.00000002.4096629893.000000000F32000.00000004.00000020.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097180640.00000000013F5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/libraries~b28b7af6	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/modalContent.js?v=L35TrLJDfqtD&l=engl	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/main.js?v=ZQOnBoEs	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://www.autoitscript.com/autoit3/	bRlvBJEl6T.exe, 00000000.00000003.1638072683.0000000002784000.00000004.00000020.00020000.00000000.sdmp, bRlvBJEl6T.exe, 00000000.00000002.1728936111.0000000000414000.00000004.00000001.01000000.00000003.sdmp, Holdem.pif.1.dr, Returned.0.dr	false		high
http://www.valvesoftware.com/legal.htm	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/css/promo/summer2017/stickers.css?v=HA2Yr5oy3FFG&	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/logo_valve_footer.png	Holdem.pif, 0000000A.00000002.4096850193.000000000114140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/applications/community/manifest.js?v=rG2l	Holdem.pif, 0000000A.00000002.4096850193.000000000114140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/nss3.dll_	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/vcruntime140.dllw	Holdem.pif, 0000000A.00000002.4097180640.00000000013F5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_menu_hamburger.png	Holdem.pif, 0000000A.00000002.4096850193.000000000114140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17rer.exe	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://65.108.152.56:9000/nss3.dll	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/nss3.dllft	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/global.js?v=B7Vsdo1okyaC&l=english	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_responsive.css?v=sHIlcMzCffX6&	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://www.valvesoftware.com/en/contact?contact-person=Translation%20Team%20Feedback	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/profile.js?v=Iy1ies1ROjUT&l=english	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=en	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000el	Holdem.pif, 0000000A.00000002.4097499400.0000000003A0C000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/javascript/scriptaculous/_combined.js?v=OeNIgrpEF8tL	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/freebl3.dll	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/J	bRlvBJEl6T.exe, 00000000.00000003.1633480344.00000000027A0000.00000004.00000020.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096293678.0000000000B69000.00000002.00000001.01000000.00000005.sdmp, Holdem.pif.1.dr, Supervision.0.dr	false		high
http://https://65.108.152.56:9000/i	Holdem.pif, 0000000A.00000002.4096967324.0000000001273000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/skin_1/header.css?v=NFoCa4OkAxRb&l=english	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://steamcommunity.com/q	Holdem.pif, 0000000A.00000002.4096786614.00000000010DF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://store.steampowered.com/privacy_agreement/	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://store.steampowered.com/points/shop/	Holdem.pif, 0000000A.00000002.4096850193.000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	JJJKEHCA.10.dr	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	bRlvBJEl6T.exe	false	• URL Reputation: safe	unknown
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp, FIJKEHJJ.10.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	bRlvBJEl6T.exe	false		high
http://https://steamcommunity.com/profiles/76561199680449169/badges	Holdem.pif, 0000000A.00000002.4096850193.000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://www.ecosia.org/newtab/	JJJKEHCA.10.dr	false		high
http://https://avatars.akamai.steamstatic.com/fef49e7fa7e1997310d705b2a6158ff8dc1cdfeb_full.jpg	76561199680449169[1].htm.10.dr	false		high
http://https://store.steampowered.com/privacy_agreement/	Holdem.pif, 0000000A.00000002.4096850193.000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high

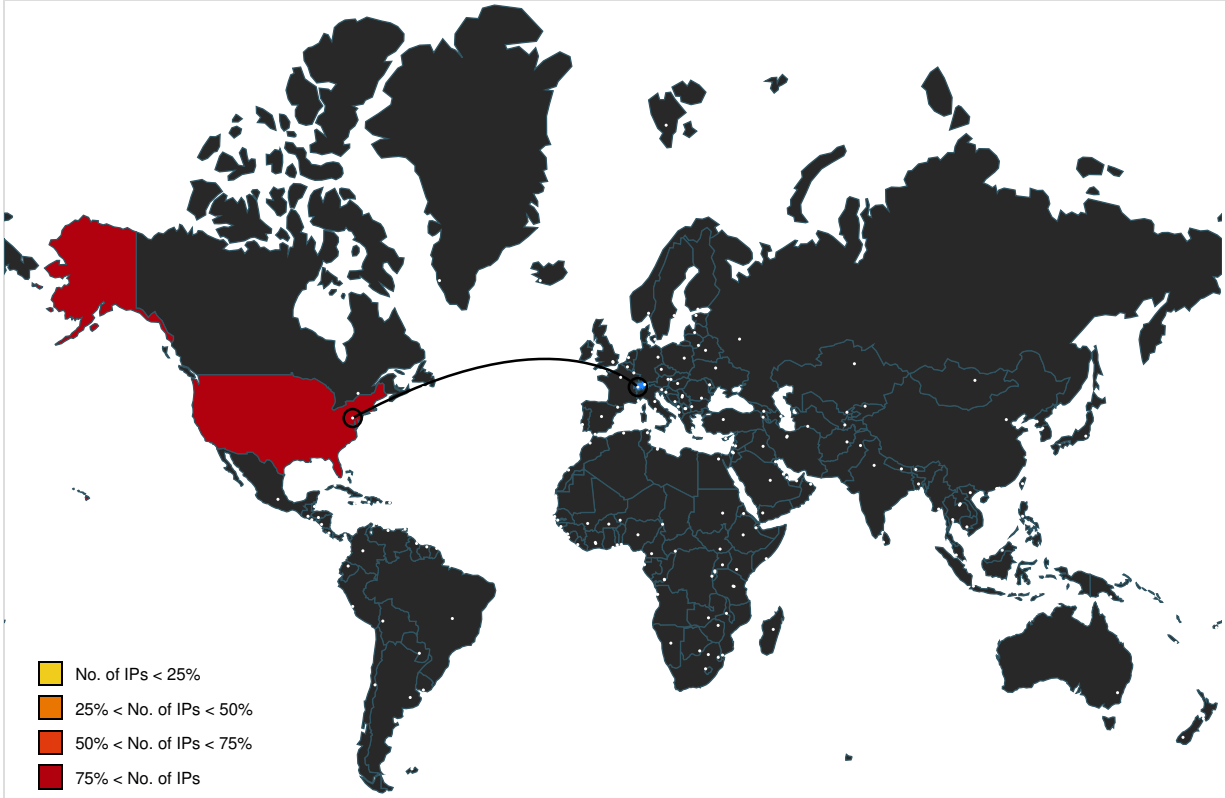
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/shared/javascript/tooltip.js?v=.zYHOpI1L3Rt0	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/f35bosoft	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/D	Holdem.pif, 0000000A.00000002.4097018307.000000000131C000.00000004.00000800.00020000.00000000.sdmp	false	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/profiles/76561199680449169l~	Holdem.pif, 0000000A.00000002.4096629893.0000000000F32000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://community.akamai.steamstatic	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/javascript/shared_global.js?v=REEGJU1hwkYI&am	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/soft	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/softokn3.dll	Holdem.pif, 0000000A.00000002.4096967324.0000000001273000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/modalv2.js?v=dfMhuy-Lrpyo&l=english	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/	Holdem.pif, 0000000A.00000002.4097018307.000000000131C000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/mozglue.dllEdge	Holdem.pif, 0000000A.00000002.4097499400.00000000039C8000.00000040.00001000.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/shared/images/responsive/header_logo.png	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://support.office.com/article/7D48285B-20E8-4B9B-91AD-216E34163BAD?wt.mc_id=EnterPK2016Examples	FIJKEHJJ.10.dr	false		high
http://https://www.valvesoftware.com/en/contact?contact-person=T	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://65.108.152.56:9000/B	Holdem.pif, 0000000A.00000002.4097018307.000000000131C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/vcruntime140.dllser	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000ing	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://65.108.152.56:9000/A	Holdem.pif, 0000000A.00000002.4097018307.000000000131C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/css/skin_1/profilev2.css?v=M_qL4gO2sKII&l=englis	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/jquery-1.11.1.min.js?v=.isFTSRckeNhC	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://store.steampowered.com/about/	76561199680449169[1].htm.10.dr	false		high
http://https://steamcommunity.com/my/wishlist/	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://ocsp.sectigo.com0	bRlvBJEl6T.exe	false	• URL Reputation: safe	unknown
http://https://65.108.152.56/	Holdem.pif, 0000000A.00000002.4096902193.0000000001205000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://65.108.152.56:9000/vcruntime140.dll_7)	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://help.steampowered.com/en/	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://steamcommunity.com/market/	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://store.steampowered.com/news/	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/vcruntime140.dll=cv6	Holdem.pif, 0000000A.00000002.4096629893.0000000000F32000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	JJJKEHCA.10.dr	false		high
http://store.steampowered.com/subscriber_agreement/	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://steamcommunity.com/login/home/?goto=profiles%2F76561199680449169	76561199680449169[1].htm.10.dr	false		high
http://https://steamcommunity.com/linkfilter/?u=http%3A%2F%2Fwww.geonames.org	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17	Holdem.pif, 0000000A.00000002.4097499400.00000000039CE000.00000040.00001000.00020000.00000000.sdmp, FIJKEHJJ.10.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	bRlvBJEl6T.exe	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://community.akamai.steamstatic.com/public/javascript/promo/stickers.js?v=upl9NJ5D2xkP&l=en	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://steamcommunity.com/discussions/	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/freebl3.dllB	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/r1g1o	Holdem.pif, 0000000A.00000002.4096902193.00000000011D6000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000003.3135450130.00000000038AB000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000003.3135086350.00000000011D7000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096786614.00000000010B0000.00000004.00000020.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000003.3135223602.0000000001141000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038A1000.00000040.00001000.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096629893.0000000001006000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://store.steampowered.com/stats/	Holdem.pif, 0000000A.00000002.4096850193.0000000001140000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/images/skin_1/footerLogo_valve.png?v=1	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://store.steampowered.com/steam_refunds/	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://65.108.152.56:9000/.152.56:9000/softokn3.dllessionKeyBackwarda_1	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://community.akamai.steamstatic.com/public/javascript/webui/clientcom.js?v=yXrh2LzpDwct&l=e	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://support.office.com/article/94ba2e0b-638e-4a92-8857-2cb5ac1d8e17Install	FIJKEHJJ.10.dr	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	JJJKEHCA.10.dr	false		high
http://https://65.108.152.56:9000l	Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://65.108.152.56:9000/msvcp140.dll	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://steamcommunity.com/A	Holdem.pif, 0000000A.00000002.4096786614.00000000010DF000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://steamcommunity.com/workshop/	Holdem.pif, 0000000A.00000002.4096850193.000000000114000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://store.steampowered.com/legal/	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high
http://https://community.akamai.steamstatic.com/public/javascript/reportedcontent.js?v=dAtjbcZMWhSe&l=e	Holdem.pif, 0000000A.00000002.4096850193.000000000114F000.00000004.00000800.00020000.00000000.sdmp, Holdem.pif, 0000000A.00000002.4097499400.00000000038D5000.00000040.00001000.00020000.00000000.sdmp, 76561199680449169[1].htm.10.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.108.152.56	unknown	United States		11022	ALABANZA-BALTUS	false
23.195.238.96	steamcommunity.com	United States		16625	AKAMAI-ASUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1437978
Start date and time:	2024-05-08 09:28:08 +02:00

Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	bRlvBJEl6T.exerenamed because original name is a hash value
Original Sample Name:	4efb38b934e4247c49ac1de662b4fe2c.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@22/22@2/3
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240000 for current running targets taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:28:59	API Interceptor	4630x Sleep call for process: Holdem.pif 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\FIJKEHJJ

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.7873599747470391
Encrypted:	false
SSDEEP:	96:pn6pld6px0c2EDKFm5wTmN8ewmdaDKFmJ4ee7vuejzH+bF+UIYysX0IxQzh/tsVL:8Ys3QMmRtH+bF+UI3iN0RSV0k3qLyj9v
MD5:	6A6BAD38068B0F6F2CADC6464C4FE8F0
SHA1:	4E3B235898D8E900548613DDB6EA59CDA5EB4E68
SHA-256:	0998615B274171FC74AAB4E70FD355AF513186B74A4EB07AAA883782E6497982
SHA-512:	BFE41E5AB5851C92308A097FE9DA4F215875AC2C7D7A483B066585071EE6086B5A7BE6D80CEC18027A3B88AA5C0A477730B22A41406A6AB344FCD9C659B9CB A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\ProgramData\GHJDGDBFCBKFHJKFHCBK

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 1, database pages 24, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8180424350137764
Encrypted:	false
SSDEEP:	96:uRMKLyeymwxCn8MZyFlSynlbiXyKwt8hG:uRkxGOXnlbibhG
MD5:	349E6EB110E34A08924D92F6B334801D
SHA1:	BDFB289DAFF51890CC71697B6322AA4B35EC9169
SHA-256:	C9FD7BE4579E4AA942E8C2B44AB10115FA6C2FE6AFD0C584865413D9D53F3B2A
SHA-512:	2A635B815A5E117EA181EE79305EE1BAF591459427ACC5210D8C6C7E447BE3513EAD871C605EB3D32E4AB4111B2A335F26520D0EF8C1245A4AF44E1FAEC4457 4
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

C:\ProgramData\IIIJECAEGDHIDHJKKKKFIEGIJK

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 11, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 11
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.5793180405395284
Encrypted:	false
SSDEEP:	96:/xealJiylsMjLslk5nYPphZEhcR2hO2mOeVgN8tmKqWkh3qzRk4PeOhZ3hcR1hOI:/xGZR8wbtxq5uWRHKloIN7YItnb6Ggz
MD5:	41EA9A4112F057AE6BA17E2838AEAC26
SHA1:	F2B389103BFD1A1A050C4857A995B09FEAFE8903

SHA-256:	CE84656EAEFC842355D668E7141F84383D3A0C819AE01B26A04F9021EF0AC9DB
SHA-512:	29E848AD16D458F81D8C4F4E288094B4CFC103AD99B4511ED1A4846542F9128736A87AAC5F4BFFBEFE7DF99A05EB230911EDCE99FEE3877DEC130C27819621(3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$.....

C:\ProgramData\JEBKJDAF

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 2, database pages 31, cookie 0x18, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	126976
Entropy (8bit):	0.47147045728725767
Encrypted:	false
SSDEEP:	96:/WU+bDoYysX0uhnyTpvVjN9DLjGQLBE3u:/l+bDo3irhnyTpvVj3XBBE3u
MD5:	A2D1F4CF66465F9F0CAC61C4A95C7EDE
SHA1:	BA6A845E247B221AAEC96C4213E1FD3744B10A27
SHA-256:	B510DF8D67E38DCAE51FE97A3924228AD37CF823999FD3BC6BA44CA6535DE8FE
SHA-512:	C571E5125C005EAC0F0B72B5F132AE03783AF8D621BFA32B366B0E8A825EF8F65E33CD330E42BDC722BFA012E3447A7218F05FDD4A5AD855C1CA22DFA2F79838
Malicious:	false
Preview:	SQLite format 3.....@ .....O}.....

C:\ProgramData\JJECAAEHCFIEBGCBGHIE

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwiI
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....

C:\ProgramData\JJJKEHCA

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.1358696453229276
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c5/w4:MnlyfnGtxnfVuSVumEH544
MD5:	28591AA4E12D1C4FC761BE7C0A468622
SHA1:	BC4968A84C19377D05A8BB3F208FBFAC49F4820B
SHA-256:	51624D124EFA3EE31EF43CB3D9ECFE98254D629957063747F4CA7061543B14B9
SHA-512:	5DDC8C36538AB1415637B2FF6C35AED3A94639A0C2B0A36E256A1C4477AA5A356813D1368913BA3B6E8B770625CDCB94EE7BFC17FD7D324982CFE3BDEC2D3EB
Malicious:	false

Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\ProgramData\KKJJEBFC

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 2, database pages 56, cookie 0x24, schema 4, UTF-8, version-valid-for 2
Category:	modified
Size (bytes):	114688
Entropy (8bit):	0.9746603542602881
Encrypted:	false
SSDEEP:	192:CwbUJ6IH9xhomnGCTjHbRjCLqtzKWJaW:CfJ6a9xpnQLqtzKWJn
MD5:	780853CDDEAEE8DE70F28A4B255A600B
SHA1:	AD7A5DA33F7AD12946153C497E990720B09005ED
SHA-256:	1055FF62DE3DEA7645C732583242ADF4164BDCFB9DD37D9B35BBB9510D59B0A3
SHA-512:	E422863112084BB8D11C682482E780CD63C2F20C8E3A93ED3B9EFD1B04D53EB5D3C8081851CA89B74D66F3D9AB48EB5F6C74550484F46E7C6E460A8250C9B1D8
Malicious:	false
Preview:	SQLite format 3.....@ .....8.....$.....O}.....4.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	893608
Entropy (8bit):	6.620254876639106
Encrypted:	false
SSDEEP:	12288:DpVWeOV7GtINsegA/hMyyzIcqikvAfcN9b2MyZa31troPTdFqgaAV2M0L:DT3E53MyyzI0hMf1te7xaA8M0L
MD5:	6EE7DDEBFF0A2B78C7AC30F6E00D1D11
SHA1:	F2F57024C7CC3F9FF5F999EE20C4F5C38BFC20A2
SHA-256:	865347471135BB5459AD0E647E75A14AD91424B6F13A5C05D9ECD9183A8A1CF4
SHA-512:	57D56DE2BB882F491E633972003D7C6562EF2758C3731B913FF4D15379ADA575062F4DE2A48CA6D6D9241852A5B8A007F52792753FD8D8FEE85B9A218714EFD0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 7%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R.+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L.....Z....."....@.....Jo....@...@.....@.....|.....P.....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<....@..@.reloc...q...p...r.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	data
Category:	dropped
Size (bytes):	311820
Entropy (8bit):	**7.99945664422248**
Encrypted:	**true**
SSDEEP:	6144:umgBywAo0a8WsSp1uOUF2BlfoIiq0xzMDa9PQ/K9mZJ/uBwDLQq0:aTt8Wsg19tHfobq0xqoYJWBeLs
MD5:	6A9A08A897FD2567F2BE8A37AF9409C7
SHA1:	D5905D73D5113BF28E95E387F5A885F2DC4DF670
SHA-256:	58F7AEDBF5B73B0AD71FCFDDE89E30BF4F6CF5F1A4AA8EDCCC7DA92A81300235
SHA-512:	841F7BBEF006D50E97D7B068A45F11E9F5DF7CA75A9C23C7C7B0DB2867B13AF01C3195A7972EF450C25FB9493CD09D0AF4C858DF0ACEB3397B851134AFAA11E3
Malicious:	false
Preview:	.)..G..C..xn.k.d..z.Q..)@...~./.....`;.Eu...9..ep....%.....J(H.dP...,%?...w8Y..."...B.n.!q...M.....9._.....j...2..@..Yl.....#....K.u|..\e".F"..y....:...$..SnR^*....WZ.G..N"..H...B..$7.u..v.C...S..u.Xrp.....u^.... vh.....MI.D..o.(O.k8..+d4.z.3(w.....<w.Y.d+s..@.2.&.fw..mm..6<.!s.....).:;.=...j.3#PJ...}O.T.O.T.....h.. .c...s.H}.Zo....N/.....+.7..k.L.yL.....fq\|6...{rK.m.{F.P..wE3...l<240l?.2.K...Z..Hk.\|U.3Kv$..B2.xU...GA.o....{.....7Gd.#..GA..N}.5,..t..L...9."h.H.0.vp.^.....|n.....%.F7...D.V.....s.` L...c.5F.I.E~qU_....K y..d.....>L.....'..+ ...7Y.$.....NZ...d.....2..ML...Dj.....u..F.x.....^....*..Aa>..S....y...{(.....n.G.....&...I.U.....I.>.}.....}..h.!.F.....K.X.....mA..;.E.@..F..&t.J.H!H].Cl...@....k...*....[F.,w<c;...l?..5C.....H.5)"..C.?...?..I+.K..EG..hK.....$z.J..Fc...F...S...zI.....'."....",....@..RJr-&!....<.BNb...?.qn..Zu..i.?H.....h.....92.Z.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	ASCII text, with very long lines (1426), with CRLF line terminators
Category:	dropped
Size (bytes):	28159
Entropy (8bit):	5.022030688278114
Encrypted:	false
SSDEEP:	768:JE/QndS3hiWIS+e57WB3hvghsNIfuj1mGBqGBBWYt6:JJdSQ7S+epWLvEkIGxJt6
MD5:	8F7F76574B4EA462583D058F32D53442
SHA1:	F09D455F80917CFFB3AFAE4DC7918E70F22FA62F
SHA-256:	DBB0AB5B95732C6704495DF674A66D09B69638F1F6DC96CD4A6B02D98D678224
SHA-512:	5607A45B3197BE7F590920247F1701B2631B77AF97CED09B28A744306E089527E5E84E95B3F4D3B9E1C48CE1E5440A98034510E4099501A821AD0469CAB7D641
Malicious:	false
Preview:	Set Become=i..EKMedian Mercury Cups Prague ..JDIMeditation Nato Mutual Suspected Mardi Developing Taught Lil Absent ..rTTrEntities Gl ..JCHMouth Conditioning Ho Tolerance Committee Villa Criterion Workshops Broke ..BMMVCulture Accurate Pixel Contribute Council ..KGPokemon Know Apps Generators Alike ..UyPair Actively Gr oss ..HrWAdjusted Roller Description ..ushCitizen Guru Ae Flow Http Timber Talks Merchant ..Set Tanzania= ..VRXSHeroes Kenya Bleeding Tn Billing Routines Fundam ental Nepal Drive ..qWxlClient Screensavers Millennium Summary Suit ..NRMuMissile Hammer Gifts Advert Instances Arrived Transparency Eur ..HkaLAlphabetical Hold er Bandwidth Lighter ..XoJJBrutal Dover Bids Wma Ate ..laOContinuous War Cottage ..Set Disciplinary=t..qrgUIde Stat Janet Spanking Indigenous Ppc Establish Soon Competition ..ULSComparisons Voices Uncertainty Developmental Divisions Wichita Suck Monster Interpreted ..rlAsks Violent Type Bloggers Halfcom Scales Motherbo ard Postage ..GiFFla Machines Nations Na

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd (copy)

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with very long lines (1426), with CRLF line terminators
Category:	dropped
Size (bytes):	28159
Entropy (8bit):	5.022030688278114
Encrypted:	false
SSDEEP:	768:JE/QndS3hiWIS+e57WB3hvghsNIfuj1mGBqGBBWYt6:JJdSQ7S+epWLvEkIGxJt6
MD5:	8F7F76574B4EA462583D058F32D53442
SHA1:	F09D455F80917CFFB3AFAE4DC7918E70F22FA62F
SHA-256:	DBB0AB5B95732C6704495DF674A66D09B69638F1F6DC96CD4A6B02D98D678224
SHA-512:	5607A45B3197BE7F590920247F1701B2631B77AF97CED09B28A744306E089527E5E84E95B3F4D3B9E1C48CE1E5440A98034510E4099501A821AD0469CAB7D641
Malicious:	false
Preview:	Set Become=i..EKMedian Mercury Cups Prague ..JDIMeditation Nato Mutual Suspected Mardi Developing Taught Lil Absent ..rTTrEntities Gl ..JCHMouth Conditioning Ho Tolerance Committee Villa Criterion Workshops Broke ..BMMVCulture Accurate Pixel Contribute Council ..KGPokemon Know Apps Generators Alike ..UyPair Actively Gr oss ..HrWAdjusted Roller Description ..ushCitizen Guru Ae Flow Http Timber Talks Merchant ..Set Tanzania= ..VRXSHeroes Kenya Bleeding Tn Billing Routines Fundam ental Nepal Drive ..qWxlClient Screensavers Millennium Summary Suit ..NRMuMissile Hammer Gifts Advert Instances Arrived Transparency Eur ..HkaLAlphabetical Hold er Bandwidth Lighter ..XoJJBrutal Dover Bids Wma Ate ..laOContinuous War Cottage ..Set Disciplinary=t..qrgUIde Stat Janet Spanking Indigenous Ppc Establish Soon Competition ..ULSComparisons Voices Uncertainty Developmental Divisions Wichita Suck Monster Interpreted ..rlAsks Violent Type Bloggers Halfcom Scales Motherbo ard Postage ..GiFFla Machines Nations Na

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Creating

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	104972
Entropy (8bit):	**7.998384885619153**
Encrypted:	**true**
SSDEEP:	1536:CPxRRKh5gbmwTTIdDNXVAXZe0+TvwHEkP/ey0FEUruz1GGkO/Uweef2eYSAZoaa0:k/K7cuVVmZJEvEuyKZslMgDLQXa0
MD5:	3174E5C547EC44D9E422845F62E95B6B
SHA1:	B02BE201156CD93436BFEE9B1D8E363B14C51707
SHA-256:	8145F63CCC2C07ED746DB82F8421E629735F6E69A4F605ABB5CF1212EDE8FCBD
SHA-512:	80134B58FE675194BED7E9F493ABCFC804DD596C0C2EF7CB93B81A9FD1CFEB9461BFE6023B25883006A320AE49B341D8A3B0EF7618E994139AA76162CBC3498A
Malicious:	false
Preview:	...n>...U|9..'y=q1.7"W.h..+.,J.h...K..6R..W..Z..[.....tN.q.EG.{...Q&h....h.O5..U.....1.)..].5^.D.......?.......H......R..K\QZ..A..g..E.....i..?h...D.N.....G,..v..|/..,.....&.'......h..B|7g9_ ^}..P.s..7c..6+.8..;?~@.b....iR....A^.*..T.....v..>.....;...tW.....{..c.o.M`.....,..N.R...QO.E.....:..zHS....&.pZz.hf.zL.cm.T..C.(z.O.I7.0a.go1.D..B.:.n$.....`...By...4hz.Vs...w.V8..cj .....~O3].$.....[..@F)OK.....k>{M....D...v.>.....$...<%.3;.....".f...'6.T....'.D>.....}km..k....i=?.Qy.&%C....s@..M.....R&?,....Q....8....F...\|.....gY.8wA...f.....B....n..K..J.K.I. *..eu[c5...{..b6,\|.^Lk....}..&k...\.....N.V.....?....I.L..y.....*..AS....[...i$.7..*.:./..}...v.. i5.n|/n._wD.Q.. .$]X-..3[v...0 .6.s.UQU>.s....7.P..:....PO!!Pm.L.I...u.....f..-..P.b}&..$..."....k.. V...x...(..T.d...?...R...w..}2...u...{RYR.nB.[..^.L.Y`8.....G...^....!.9.e.]..D....v..G.#u..v.B.n..l....h.....H{F.....F..u...H4..6..;..;....5.Z...hm..-(#..F..h|.,..B$....x.Wgd.Q..{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Experiences

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	181248
Entropy (8bit):	**7.999061896550611**
Encrypted:	**true**
SSDEEP:	3072:IzAfkCB1op89a8YnYH7f+PpHVufdUULRuTBlfEVpmiqlqkEfA+MTf8rz5UfLqL:4Ao0a8WsSp1uOUF2BlfoIiq0xzMDa9PL
MD5:	0131A04280608465EF6A189301961FCE
SHA1:	3E0A81F593CBE518C96D675917922F3A1D20309D
SHA-256:	43A07113368DEAF916127480450B1B19C22EED4F367CF73B20B6BF6685D014DD
SHA-512:	039AB3FCF9DAABEED49CE654F43CB5A7AD3CB51DCFB2293C3C028C5DF4DA29F9D2491DD69594F7F3A6C9C45106FE5240F16D5F7AA68CF19993333606BF7BDFC8
Malicious:	false
Preview:	._(....e..0....H.....w..uJ...j...w...KN..]4G;....$'..;....1.r.1gu....T.>.a/.:...Z.?..E..... G..a.thr..l..w.2. cY.1.q..L.^-..H.D.n..j.....m.*.....j;..B.2^b_..!C2.w.5..0.)...noK...9..a.l.z"l....)?.. ....8..W+.....h.....~[.".E&..l.V5..u9x40.?D..S.l.B..g.y....}..2...B(j.[0iRC.S-@hT.0...1.D>..a.....f:.z.FO..n]Q.....<....Mb.W.l..[/...W.d.V..i.@Y.t;..Q..GO7e..h..y..J>.{.....c. (.up.7m..Z..E[.A....}..;.\4|...)....^M....w..Z....v.U......"N#..<.T5.6.WJ0i...eM.K..h.....%..4..`..J....7.M...q.D..#m.C.;.h.....I...g,.5R..+!N...U.m...k....C....._...v1...r....[...K..1 .5Wp..n;~.....I...L)69..[5.-.#ukZ."....I#.".1..*.."sW3...kg..0.~_w.s'/..M...6.M.6MQ...=2....e....n..G..].) .....$..J....._..[o*N.....#=...(.....F.r...=>.8<KJ..{.xf.....ab'Z...Z.G..ZR.. {.....L.%.+.w.<r.....2. ..nrsM..@U.|<9.B..B..+c.|.....va./' ..*w.....'LOHv.H...{.$.s..c.....> .t*./...j.....X..0.3?...u..z.L...D.un~..tf. .N4<=...{v7i.a:.4.....cVLW...R.?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3D003UC5\76561199680449169[1].htm

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (2969), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	34791
Entropy (8bit):	5.385516925635591
Encrypted:	false
SSDEEP:	768:Tdpqm+0Ih3YAA9CWGI+fcDAGPzzgiJmDzJtxvrfJkPVoEAdmPzzgiJmDzJtxvJ2E:Td8m+0Ih3YAA9CWGI+FGPzzgiJmDzJt3
MD5:	8040A93DFD9A45D15AD3B7F63F66BB21
SHA1:	81893F5C3BC08407441CA79FCED36A428342B7DC
SHA-256:	A813D344FA3863810AD75CFC863CAFE246CF8C4912D14C3D3580EF3EE843D6B6
SHA-512:	5E2346AAD0C70BA503BE86FB410E81BA4E418A34102F4B5AFC1C47E04A8FEB973B868201C7BA938D1D4F5DC855DE392483FB72E67E23785A6BDFD65E8EC5304D
Malicious:	false
Preview:	<!DOCTYPE html>..<html class=" responsive" lang="en">..<head>...<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.....<meta name="viewport" content="width=device-width,initial-scale=1">....<meta name="theme-color" content="#171a21">....<title>Steam Community :: p__o https://65.108.152.56:9000|</title>...<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon">.....<link href="https://community.akamai.steamstatic.com/public/shared/css/motiva_sans.css?v=-DH0xTYpnVe2&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/buttons.css?v=PUJIfhtcQn7W&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/shared/css/shared_global.css?v=SPpMitTYp6ku&l=english" rel="stylesheet" type="text/css" >.<link href="https://community.akamai.steamstatic.com/public/css/globalv2.css?v=PAcV2zMBzzSV&l=english" rel="stylesheet" type="text/css" >.<lin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\YLNGKWRH\sqlx[1].dll

Process:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2459136
Entropy (8bit):	6.052474106868353
Encrypted:	false
SSDEEP:	49152:WHoJ9zGioiMjW2RrL9B8SSpiCH7cuez9A:WHoJBGqabRnj8JY/9
MD5:	90E744829865D57082A7F452EDC90DE5
SHA1:	833B178775F39675FA4E55EAB1032353514E1052
SHA-256:	036A57102385D7F0D7B2DEACF932C1C372AE30D924365B7A88F8A26657DD7550
SHA-512:	0A2D112FF7CB806A74F5EC17FE097D28107BB497D6ED5AD28EA47E6795434BA903CDB49AAF97A9A99C08CD0411F1969CAD93031246DC107C26606A898E570323
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.Z.Y.Z.Y.Z.Y...Z.n.Y...\..Y...]...Y...X.Y.Y.Z.X..Y.O.\.E.Y.O.].U.Y.O.Z.L.Y.l3].[.Y.l3Y.[.Y.l3..[.Y.l3[.[.Y.RichZ.Y.....PE..L...i.`e.....!...%.. .....{D..... .....%.....@.....#..6....$.(....$..... .....$....`.#.8.....x.#.@.....$.....text...G. ....`.rdata..."..... ..$.... .....@..@.data...4|... $..b....#.....@....idata.... ....$.....^$.....@..@.00cfg.....$.....p$.....@..@.rsrc.....$.....r$.....@..@.reloc..5....$.....$.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Lease

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe

File Type:	data
Category:	dropped
Size (bytes):	123
Entropy (8bit):	3.9361447888719114
Encrypted:	false
SSDEEP:	3:BMWXjQoucUqt/vllpfrYZcFTSn:BXTsHqjvVS
MD5:	98E87874165393607B54818EA0CC0813
SHA1:	DDDEDD925A309CB2B359EB08E678F4829EE26632
SHA-256:	C0D3B1DBBBF02073B0E60D6CA6294C97134D13017E6332D1EE49918A4FF94A1B
SHA-512:	127C1F7978F6C8CF321B62B5F45766A81807CEC5F778231950CA3362201CEEB914D6A84D97D1F57FF14AA34BA12C83E29B1A51B564649D0754E692EBA2DD7F8
Malicious:	false
Preview:	BbcAdvisorsAndaleNowhere..MZ.....@.....!..L.!This program cannot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Oil

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	6.688977511438296
Encrypted:	false
SSDEEP:	6144:5/12vk6AQzyMfA+eyVPlcBgtoTqnvAfcaGM:5/hMyyzlcqikvAfcNM
MD5:	CCFF4D45B31B96AD3BFDAEE364B88C66
SHA1:	8594F9FCD10C3BA98529175EEEB7F00B17F17F17
SHA-256:	C1E5F515F73058A6A4AB02C95B7111001A10F933F51542258B97A53A3E56B354
SHA-512:	DC18CAAEEA264DA603BA77C4878F260F84AC60908D41360D3DB131687C210C67AF22E77675C9ECF0C253F59386D8D0BE6CAEAA0C80D88BBADE7445939E545 1C
Malicious:	false
Preview:	....t....G..j0Z..@I....U.....x..?5|.....0H.89t....>1u..B...S....@PSV.c.....3.[_^].U..QQ.E.SVW..x.....P.....}...E...t.....t....<...%.....!..u...u..E.!P.!.f.x..X...<..3.....M .....E..]..s.....x&.....y.}..}..E..s...f.{._^[..].U....0.P.L.3.E..E.S.].V.E.E.WP.E.P.....YY.E.Pj.j.....u....f.."....u.C...E....E..C..E.P.u.V.....$..u..M..._.s.3.^[.*2....] .3.PPPPP.....WVU3.3.D$...}.GE.T$.....D$..T$..D$...}.G.T$.....D$..T$...u(.L$..D$.3....D$.....d$.....d$....G..L$..T$..D$.....u.....d$...D$.....r.;T$.w.r.;D$.v.N+D$. .T$.3.+D$..T$.My.....Ou.....]^_...U..M..E.....#.V.u.....t$..t.j.j..J...YY...7...j.^.0.....Q.u...t..&.....YY3.^].U...$.M..u..H....E...t..M....E.SVW..t..}...t....\|...$~.....R..... ..}.p.3.]....t.~..E.P...j.P..&...}.....H.....t...F..E..]...-u.....F.M.....+t.M..}..].E.....C.....:....$..1.....u...0t.j._.0..<xt.<Xt.j...j._.....u...0u..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Pharmacy

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	25600
Entropy (8bit):	**7.99391195789994**
Encrypted:	**true**
SSDEEP:	768:NPteSp4vUNy+Cy73dv6tamehP+JkMtXCU9y:uvyt73V6A9+JkcyU9y
MD5:	A47F571CA70AD97D1EA1435F098A3E6C
SHA1:	DA0F173DBF68004BF0B101A7F1B044144F707C52
SHA-256:	EB99BFA316742ED21FA831B87DEADE8DBCD28337C6DDC77682A3E93F97B2F47E
SHA-512:	EAB604201412F6440CD091ADF83A1E85C98BA712E61B037107A70D49D4BEBF7D60F4CD375009F8E3F1671A2D7ADF17757A04F4B6B58B401E142AC3F73BCE085 8
Malicious:	false
Preview:	.)..G..C..xn.k.d..z.Q..)@...~./.....`;.Eu...9..ep....%.....J(H.dP..,.%?...w8Y..."...B.n.!q...M.....9._.....j...2..@..Yl.....#....K.u|..\e".F"..y....:...$..SnR^*....WZ.G..N"..H...B..$7.u ..v.C...S..u.Xrp.....u^.... vh.....MI.D..o.(O.k8..+d4.z.3(w.....<w.Y.d+s..@.2.&.fw..mm..6<.!s.....).:.=...j.3#PJ...}O.T.O.T.....h.. .c...s.H}.Zo....N/.....+.7..k.L.yL.....fq\|6... {rK.m.{F.P..wE3...l<240l?.2.K...Z..Hk.\|U.3Kv$..B2.xU...GA.o....{.....7Gd.#..GA..N}.5,..t..L...9."h.H.0.vp.^.....|n.....%.F7...D.V.....s.` L...c.5F.I.E~qU_....K y..d.....>L... .....'..+ ...7Y.$.....NZ...d.....2..ML...Dj.....u..F.x.....^....*..Aa>..S....y...{(.....n.G.....&...I.U.....I.>.}.....}..h.!.F.....K.X.....mA..;.E.@..F..&t.J.H!H].Cl...@....k...*....[F .,w<c;...l?..5C.....H.5)"..C.?...?..I+.K..EG..hK.....$z.J..Fc...F...S...zI.....'."....",....@..RJr-&!....<.BNb...?.qn..Zu..i.?H.....h.....92.Z.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Relatives

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	256000
Entropy (8bit):	6.5083855315988846
Encrypted:	false
SSDEEP:	3072:CDqeb2Xo2IkVvh8p65Nu+dVtqi/x4Rqf21Rgat0g/bZaUAg0FuPOKBNEBNUGXEyc:8b2M8JTDD/xcq21R1p/rAOPOei7TdFU
MD5:	CD818EE7F8BD1F1BAE4E1822C4E41541

SHA1:	5CC00D959325F119B026ED0E330D57FDFEE543A2
SHA-256:	421E5FCF6246FAAE145237DAA2A0542E7A45AEA01BE75C5070770DE93CB1644F
SHA-512:	87C34F4AD54B139DD4312C598E155A534AAFE2F408D20C13805764CB1D4AB641E300A6145E4CA2E2919D883C89600E567DF377C9C9A52DDD7438A6A1FCC667
Malicious:	false
Preview:	..H...[....t........G..H..[....t........}....$......$....P..........I...........$.................d9..Y..$.....L$\...[%....$.......3..2P.=9...L$\..$..K.....#....$.....L$\..#....$.........p..$....f9.u..M..D$XP..Z...L$X.v' ...,....I...t...$.....M..=Z....3.P..j..H.....{...D$...u.P.....Y.t$......Y.D$0..u.P.....Y.t$,....Y.L$8..'...L$...'...L$h..&...L$H..&...L$x..&.._^3.[..]...U...\...SVW.=..I.......P.u..M.2.......tq......h ..I.P.iA..YY..tH......hx.K.P.RA..YY..t1......P....I...E..M...#......QP....I.................PV....I...u.V....I..}..............Php.K.......ty.=..I..]........tU......h..I.P..@..YY..t>......hx.K.P.@..YY..t'...... P...u....u..u..u........t8hx.K........PV....I...u...V....I..._^[..]...V....I.2...3...U...\...SVW.=..I.......P.u..M.2.......t\......h..I.P..@..YY..t3......hx.K.P..?..YY..t..u..U.........P..Y................PV... .I...u.V....I..}..............Php.K.......ty.=..I..]........tU......h..I.P.x?..YY..t>......hx.K.P.a?..YY..t'......P...u....u..u..u........t8hx.K...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Returned

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	44615
Entropy (8bit):	6.996943182721781
Encrypted:	false
SSDEEP:	768:09BSCVoyO15DuOKHnrxbxZiUCu2iPaLTQ7Q1tCwqVLwQVn8qT4O:09BBVgCOa1ZBPaPQaEwo0yv
MD5:	F791D2356005E6538629B3BDE88B0BDC
SHA1:	EC5EECB9515DDA66CEC06D81B2595906E5454A1A
SHA-256:	B27657C27B957B8794EC2A6644D75578A620A0EC413E1BE8B961D0152E12BC48
SHA-512:	0BE50D77EA1920052734BCC7319DECE0C4A741556BE621BF41B7CAC88C03497C8ADE3DF1582CDFC479AAE48278FB9DCC28EC1CF619ABE1F8F12175586229 6A
Malicious:	false
Preview:	....$.......................................\...\...$..0..........................e. ..]...]...]...]...]...]...]...]...e...........................0..............................%.....................g...]...]...]...]...]...]...]...]...]...]...]...]...f.......................%...]...]...]...]...]. ..]...]...]...]...]...]...]...]...]...]..]...]...]...]...]...]...]...]...]...]...]...]...]...]...]...]...]..................................%................]...]...]...]...]...]...]...]...]. ..]...]...]...]...]...]...]...]...]...]...................%........................g...]...f....................................

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Rolled

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	231424
Entropy (8bit):	6.583065790073281
Encrypted:	false
SSDEEP:	3072:GCV26MqgQTc5F446iYNpK5SB7BJBzLZDKJtIs8di/37EM/j2xQeixW:Gi2VWTyFsJ8gNJBnGtINsegW
MD5:	0FA84A1591EF7ED70FB17E1701CE0E8C
SHA1:	3E2E21E13F1CDFA6684063BA1150251B5B2AFB0D
SHA-256:	95DD465FA97618639D0D11556DBAA8A5F50484ADA6CF46D82B6B832CC6C2E81D
SHA-512:	FFA3C5F8EF264CFFE1552CFD7A0BF5775E308B3392BD7E175580EA3C66FD7B508EE9D8FDE9FEBA1708172BF33B36E2AF8D5952E81B66713D7A513C3FC53E26 2C
Malicious:	false
Preview:	be run in DOS mode....$........sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R.+.r.*......*....S.*._@..S.*.R...P.*....S.*.RichR.*.........................PE..L...... Z.........".............................@................................Jo....@...@.......@.........................|.......P....................p...q...;.............................. [..@..te xt.............................. ..`.rdata.............................@..@.data...t........R.................@....rsrc...P............<..............@..@.reloc...q...p...r.................@..B................................ ....DaL.....h..C..\...Y...L..h..C..K...Y..N..h..C..:...Y.h..C......Y..<C..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Supervision

Process:	C:\Users\user\Desktop\bRlvBJEl6T.exe
File Type:	data
Category:	dropped
Size (bytes):	140288
Entropy (8bit):	5.233137662978611
Encrypted:	false
SSDEEP:	1536:K+l6JPTcUNx6/xhgariwYLTN3EfrDWyu0uZo2x:n6i/xhgariwYLTNaWy4ZNx
MD5:	9F30E95A4B07C6DE10CBD2361B682751
SHA1:	D01CD024A1AC849E97A5217368AC6C1EB4FE6CDD
SHA-256:	B4873B854CD42B8E5CF792C368043BB24427045FC41B22C6AE977CC342CEC1CF
SHA-512:	A0249A4106CBE0C087906ADB6402B5AD5A536B83676D5AF10258B76A0E64935A3483A988DFA0FC221DAA681E815D2B118A2F094BDBD4E7426B785BA0DA116A 0
Malicious:	false

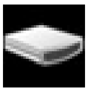
Preview:	....r.r... ....r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.!.!.!.!.!.!.!.r.r.r.r.r.r.r.r.r.r.r.r.r..........r.r.r.r.r.......................)...... ....r..........r...r.....r.....r... .......*.*.*.*.*.*.*.*.*.*.*.*.*.*.*.*.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r.r..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.978295271509072
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	bRlvBJEl6T.exe
File size:	784'214 bytes
MD5:	4efb38b934e4247c49ac1de662b4fe2c
SHA1:	121fe04be542a55b4ce6716d792e9ce4e8a5c0ae
SHA256:	46b8ec4f65622595233743e8277a2980f69f866e6edd3a2ec610d0f2872a1e5f
SHA512:	8ced1adc480693b2d5daf4013317118c2794c8840d617aa4e30a50fa0b1d8ab5aa3bb2bb2b241c672debb477ee756afcda48e9dc163a5cbb362a5d95f73c50ed
SSDEEP:	12288:AXyWGSXbu0jblSgRI4/8Xg/38hMK6JZB2L7IflVlkKWm9A/Hu5ya/8p/ryr:AXyubu0jbIg8Q8t0yElkKWUGHu5yYoyr
TLSH:	4AF423522200B983EC239A31B5E55BF2BE92B95003C467E72390754C7FB5792EE5F683
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........1 ..PN..PN..PN.*_...PN..PO.JPN.*_...PN..s~..PN..VH..PN.Rich.PN.........................PE..L....C.f.................f...".....

File Icon



Icon Hash:	c610f8e6f8f803c8

Static PE Info

General

Entrypoint:	0x40351c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x660843F3 [Sat Mar 30 16:55:15 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f4639a0b3116c2cfc71144b88a929cfd

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 25/03/2021 00:00:00 24/03/2024 23:59:59
Subject Chain	• CN="IObit CO., LTD", O="IObit CO., LTD", STREET=45 Renmin South Road, STREET="No. 605, 6th Floor, Unit 1, Building 1", L=Chengdu Shi, S=Sichuan Sheng, PostalCode=610042, C=CN

Version:	3
Thumbprint MD5:	8AD2A09EBDD6E8444414E1FFE7FC9683
Thumbprint SHA-1:	145D90AD3134C665246DC1C93CD3E2D8C69E9231
Thumbprint SHA-256:	12DBEE7AA5DBB550CEEDC6172E5C34BA577759D8926AAFF08A781552B7FABDE9
Serial:	008BA1F172FD50BA8D4C11B74FFAC8A282

Entrypoint Preview

Instruction
sub esp, 000003F8h
push ebp
push esi
push edi
push 00000020h
pop edi
xor ebp, ebp
push 00008001h
mov dword ptr [esp+20h], ebp
mov dword ptr [esp+18h], 0040A2D8h
mov dword ptr [esp+14h], ebp
call dword ptr [004080A4h]
mov esi, dword ptr [004080A8h]
lea eax, dword ptr [esp+34h]
push eax
mov dword ptr [esp+4Ch], ebp
mov dword ptr [esp+0000014Ch], ebp
mov dword ptr [esp+00000150h], ebp
mov dword ptr [esp+38h], 0000011Ch
call esi
test eax, eax
jne 00007FC54C50550Ah
lea eax, dword ptr [esp+34h]
mov dword ptr [esp+34h], 00000114h
push eax
call esi
mov ax, word ptr [esp+48h]
mov ecx, dword ptr [esp+62h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [esp+0000014Eh], 00000004h
not eax
and eax, ecx
mov word ptr [esp+00000148h], ax
cmp dword ptr [esp+38h], 0Ah
jnc 00007FC54C5054D8h
and word ptr [esp+42h], 0000h
mov eax, dword ptr [esp+40h]
movzx ecx, byte ptr [esp+3Ch]
mov dword ptr [00429AD8h], eax
xor eax, eax
mov ah, byte ptr [esp+38h]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [esp+00000148h]
movzx ecx, cx
shl eax, 10h
or eax, ecx
movzx ecx, byte ptr [esp+0000004Eh]

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3a000	0x1890	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xbab6e	0x4be8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2a8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6576	0x6600	1e4066ed6e7440cc449c401dfd9ca64f	False	0.6663219975490197	data	6.461246686118911	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1358	0x1400	f0b500ff912dda10f31f36da3efc8a1e	False	0.44296875	data	5.102094016108248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1fb38	0x600	2e1d49b2855a89e6218e118f0c182b81	False	0.5026041666666666	data	4.044293204800279	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2a000	0x10000	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3a000	0x1890	0x1a00	717af41bcb52dc6df2fff9551871a540	False	0.34314903846153844	data	3.878406451504744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x3a190	0x1128	Device independent bitmap graphic, 32 x 64 x 32, image size 4352	English	United States	0.3035063752276867
RT_DIALOG	0x3b2b8	0x100	data	English	United States	0.5234375
RT_DIALOG	0x3b3b8	0x11c	data	English	United States	0.6056338028169014
RT_DIALOG	0x3b4d8	0x60	data	English	United States	0.7291666666666666
RT_GROUP_ICON	0x3b538	0x14	data	English	United States	1.05
RT_MANIFEST	0x3b550	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States	0.5542168674698795

Imports

DLL	Import
ADVAPI32.dll	RegEnumValueW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, RegOpenKeyExW, RegCreateKeyExW
SHELL32.dll	SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW, ShellExecuteExW
ole32.dll	CoCreateInstance, OleUninitialize, OleInitialize, IIDFromString, CoTaskMemFree

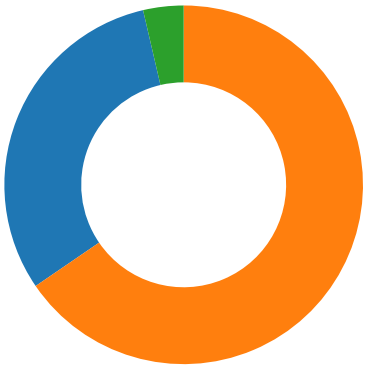
DLL	Import
COMCTL32.dll	ImageList_Destroy, ImageList_AddMasked, ImageList_Create
USER32.dll	MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, CreatePopupMenu, AppendMenuW, TrackPopupMenu, OpenClipboard, EmptyClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, IsWindowEnabled, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CharPrevW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndPaint, CharNextA, wsprintfA, DispatchMessageW, CreateWindowExW, PeekMessageW, GetSystemMetrics
GDI32.dll	GetDeviceCaps, SetBkColor, SelectObject, DeleteObject, CreateBrushIndirect, CreateFontIndirectW, SetBkMode, SetTextColor
KERNEL32.dll	lstrcmpiA, CreateFileW, GetTempFileNameW, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, WriteFile, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, Sleep, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW, MulDiv, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, SetEnvironmentVariableW

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 9000 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 09:31:29.344923973 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:29.344953060 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:29.345041990 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:29.357156992 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:29.357173920 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:29.691910982 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:29.691982985 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:29.744905949 CEST	49743	443	192.168.2.4	23.195.238.96

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 09:31:29.744923115 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:29.745232105 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:29.745434046 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:29.748830080 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:29.792121887 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.250761032 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.250787973 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.250804901 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.250895023 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.250910044 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.251010895 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.411726952 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.411777973 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.411787987 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.411798954 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.411823034 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.411837101 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.440304995 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.440342903 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.440376997 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.440385103 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.440401077 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.440401077 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.440413952 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.440440893 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.440788984 CEST	49743	443	192.168.2.4	23.195.238.96
May 8, 2024 09:31:30.440802097 CEST	443	49743	23.195.238.96	192.168.2.4
May 8, 2024 09:31:30.451261997 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:30.779889107 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:30.780081034 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:30.780483961 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:31.110310078 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:31.135783911 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:31.135798931 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:31.135839939 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:31.164895058 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:31.494023085 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:31.494112015 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:31.497009993 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:31.865464926 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:32.162692070 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:32.162776947 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:32.392467022 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:32.721417904 CEST	9000	49745	65.108.152.56	192.168.2.4
May 8, 2024 09:31:32.721541882 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:33.069592953 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:33.398488998 CEST	9000	49745	65.108.152.56	192.168.2.4
May 8, 2024 09:31:33.398776054 CEST	9000	49745	65.108.152.56	192.168.2.4
May 8, 2024 09:31:33.398850918 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:33.536468029 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:33.538692951 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:33.867552042 CEST	9000	49745	65.108.152.56	192.168.2.4
May 8, 2024 09:31:34.242244005 CEST	9000	49745	65.108.152.56	192.168.2.4
May 8, 2024 09:31:34.242360115 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.274626970 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.275043964 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.602979898 CEST	9000	49744	65.108.152.56	192.168.2.4
May 8, 2024 09:31:34.603096008 CEST	49744	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.603509903 CEST	9000	49746	65.108.152.56	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 09:31:34.603609085 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.603969097 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.932466030 CEST	9000	49746	65.108.152.56	192.168.2.4
May 8, 2024 09:31:34.932687998 CEST	9000	49746	65.108.152.56	192.168.2.4
May 8, 2024 09:31:34.932756901 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.933145046 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:34.934863091 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.263421059 CEST	9000	49746	65.108.152.56	192.168.2.4
May 8, 2024 09:31:35.644841909 CEST	9000	49746	65.108.152.56	192.168.2.4
May 8, 2024 09:31:35.644865036 CEST	9000	49746	65.108.152.56	192.168.2.4
May 8, 2024 09:31:35.644906998 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.644948006 CEST	49746	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.646229029 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.646677017 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.976767063 CEST	9000	49745	65.108.152.56	192.168.2.4
May 8, 2024 09:31:35.976846933 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:35.976958036 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.976959944 CEST	49745	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:35.977267027 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:36.305816889 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:36.306113005 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:36.306220055 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:36.306579113 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:36.308301926 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:36.636828899 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:37.033458948 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:37.033477068 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:37.033488035 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:37.033513069 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:37.033524990 CEST	9000	49747	65.108.152.56	192.168.2.4
May 8, 2024 09:31:37.033541918 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:37.033597946 CEST	49747	9000	192.168.2.4	65.108.152.56
May 8, 2024 09:31:37.091283083 CEST	49746	9000	192.168.2.4	65.108.152.56

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 09:29:00.342344046 CEST	65129	53	192.168.2.4	1.1.1.1
May 8, 2024 09:29:00.540509939 CEST	53	65129	1.1.1.1	192.168.2.4
May 8, 2024 09:31:29.171299934 CEST	52101	53	192.168.2.4	1.1.1.1
May 8, 2024 09:31:29.334323883 CEST	53	52101	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 8, 2024 09:29:00.342344046 CEST	192.168.2.4	1.1.1.1	0x423c	Standard query (0)	ekyLBwoLvc.ekyLBwoLvc	A (IP address)	IN (0x0001)	false
May 8, 2024 09:31:29.171299934 CEST	192.168.2.4	1.1.1.1	0x48af	Standard query (0)	steamcommunity.com	A (IP address)	IN (0x0001)	false

DNS Answers

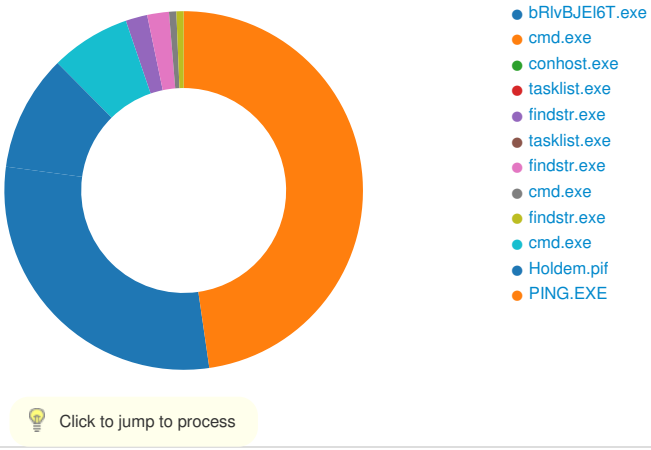
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 8, 2024 09:29:00.540509939 CEST	1.1.1.1	192.168.2.4	0x423c	Name error (3)	ekyLBwoLvc.ekyLBwoLvc	none	none	A (IP address)	IN (0x0001)	false
May 8, 2024 09:31:29.334323883 CEST	1.1.1.1	192.168.2.4	0x48af	No error (0)	steamcommunity.com		23.195.238.96	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- steamcommunity.com

Statistics

Behavior



System Behavior

Analysis Process: bRlvBJEl6T.exe PID: **916**, Parent PID: **2580**

General

Target ID:	0
Start time:	09:28:54
Start date:	08/05/2024
Path:	C:\Users\user\Desktop\bRlvBJEl6T.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bRlvBJEl6T.exe"
Imagebase:	0x400000
File size:	784'214 bytes
MD5 hash:	4EFB38B934E4247C49AC1DE662B4FE2C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: cmd.exe PID: **7180**, Parent PID: **916**

General

Target ID:	1
Start time:	09:28:56
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k move Classics Classics.cmd & Classics.cmd & exit
Imagebase:	0x240000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	250605	CreateFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	success or wait	1	2453F6	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	97	512	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 16 73 44 fd 52 12 2a fd 52 12 2a fd 52 12 2a fd 14 43 fd fd 50 12 2a fd 32 fd fd 53 12 2a fd 5f 40 fd fd 61 12 2a fd 5f 40 fd fd fd 12 2a fd 5f 40 fd fd 67 12 2a fd 5b 6a fd fd 5b 12 2a fd 5b 6a fd fd 77 12 2a fd 52 12 2b fd 72 10 2a fd fd fd fd 02 12 2a fd fd fd fd 53 12 2a fd 5f 40 fd fd 53 12 2a fd 52 12 fd fd 50 12 2a fd fd fd fd 53 12 2a fd 52 69 63 68 52 12 2a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 12 fd fd 5a 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0c 00 00 fd 08 00 00 fd 04 00 00 00 00 00 fd 7f 02 00 00 10 00 00 00 00 09 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00	be run in DOS mode.$sDR*R*R*C P*S*_@a*_@*_@g*[j[* [jw*R+r**S* _@S*RP*S*RichR*PELZ" @	success or wait	21	269830	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	10	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	27	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	9	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	37	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	2	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	27	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	12	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	11	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	25	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	29	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	4	24D737	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	4	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	17	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	8	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	3	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	7	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	9	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	3	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	4	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	4	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	4	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	6	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	10	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	2	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	2	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	20	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	7	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	8	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	18	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	37	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	9	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	2	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	17	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	12	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	5	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	9	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	6	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	6	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	5	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	129	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	4	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	0	65024	success or wait	1	269535	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Rolled	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Rolled	0	65024	success or wait	4	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Rolled	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Oil	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Oil	0	65024	success or wait	4	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Oil	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Relatives	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Relatives	0	65024	success or wait	4	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Relatives	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Supervision	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Supervision	0	65024	success or wait	3	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Supervision	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Returned	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Returned	0	65024	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Returned	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	success or wait	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	end of file	1	24D737	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Classics.cmd	0	8191	end of file	1	24D737	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7188**, Parent PID: **7180**

General

Target ID:	2
Start time:	09:28:56
Start date:	08/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: tasklist.exe PID: **7252**, Parent PID: **7180**

General

Target ID:	3
Start time:	09:28:57
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\tasklist.exe
Wow64 process (32bit):	true
Commandline:	tasklist
Imagebase:	0xd30000
File size:	79'360 bytes
MD5 hash:	0A4448B31CE7F83CB7691A2657F330F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **7260**, Parent PID: **7180**

General

Target ID:	4
Start time:	09:28:57
Start date:	08/05/2024

Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /I "wrsa.exe opssvc.exe"
Imagebase:	0x410000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	0	8192	success or wait	1	413A11	ReadFile
stdin	0	8192	success or wait	2090	41305F	ReadFile
stdin	0	8192	pipe broken	1	41305F	ReadFile

Analysis Process: tasklist.exe PID: **7296**, Parent PID: **7180**

General

Target ID:	5
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\tasklist.exe
Wow64 process (32bit):	true
Commandline:	tasklist
Imagebase:	0xd30000
File size:	79'360 bytes
MD5 hash:	0A4448B31CE7F83CB7691A2657F330F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **7304**, Parent PID: **7180**

General

Target ID:	6
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /I "avastui.exe avgui.exe nswscsvc.exe sophoshealth.exe"
Imagebase:	0x410000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	0	8192	success or wait	1	413A11	ReadFile
stdin	0	8192	success or wait	2090	41305F	ReadFile
stdin	0	8192	pipe broken	1	41305F	ReadFile

Analysis Process: cmd.exe PID: **7340**, Parent PID: **7180**

General

Target ID:	7
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c md 334343
Imagebase:	0x240000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	245A76	CreateDirectoryW

Analysis Process: findstr.exe PID: **7356**, Parent PID: **7180**

General

Target ID:	8
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /V "BbcAdvisorsAndaleNowhere" Lease
Imagebase:	0x410000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif	0	97	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 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	MZ@!L!This program cannot	success or wait	1	413359	WriteFile

Analysis Process: cmd.exe PID: **7372**, Parent PID: **7180**

General

Target ID:	9
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c copy /b Pharmacy + Experiences + Creating 334343\e
Imagebase:	0x240000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	2565DD	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	0	512	fd 29 fd fd 47 04 02 43 fd 7b 78 6e fd 6b fd 64 fd c6 7a fd 51 fd fd 29 40 13 fd fd 7e fd 2f fd fd 1b fd fd fd fd 60 3b fd 45 75 09 fd fd 39 fd fd 65 70 fd fd fd fd 25 1b 1d fd fd fd 4a 28 48 fd 64 50 fd fd 2c fd 25 3f fd 0b 1c 77 38 59 60 15 18 22 fd fd fd 42 fd 6e fd 21 71 7f fd fd 4d fd 15 fd fd 07 fd 39 fd 5f fd fd fd 09 fd fd 6a 15 1a fd 32 06 fd 40 fd 0d 59 6c fd f4 fd 1a 10 f7 23 fd fd 2e 97 4b fd 75 7c a4 fd 5c 65 22 fd 46 22 34 ed 79 fd 2b fd 3c 3a fd fd fd 24 fd fd 53 6e 52 5e 2a fd 62 fd 0b 57 5a fd 47 fd fd 4e 22 15 fd 48 e0 fd f9 42 fd fd 24 37 fd 75 fd fd 76 fd 43 fd 97 fd 53 fd fd 75 fd 58 72 70 0f fd fd 0a fd fd 75 5e 9b fd 1c fd 20 76 68 70 fd 18 fd 1c 71 12 4d 49 fd	)GCxnkdzQ)@~/`;Eu9ep %J(HdP,%?w 8Y"Bn!qM9_j2@Yl#.Ku|\e "F"y:$Sn R^*WZGN"HB$7uvCSuXr pu^ vhMl	success or wait	9	269830	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Pharmacy	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Pharmacy	0	65024	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Pharmacy	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Experiences	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Experiences	0	65024	success or wait	3	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Experiences	0	65024	end of file	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Creating	0	512	success or wait	1	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Creating	0	65024	success or wait	2	254CD0	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Creating	0	65024	end of file	1	254CD0	ReadFile

Analysis Process: Holdem.pif PID: **7388**, Parent PID: **7180**

General

Target ID:	10
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\Holdem.pif
Wow64 process (32bit):	true
Commandline:	334343\Holdem.pif 334343\e
Imagebase:	0xaa0000
File size:	893'608 bytes
MD5 hash:	6EE7DDEBFF0A2B78C7AC30F6E00D1D11
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000003.3135450130.00000000038AB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000002.4096902193.00000000011D6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000003.3135086350.00000000011D7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000002.4096786614.00000000010B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000003.3135223602.0000000001141000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000003.3135523275.00000000013A5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000002.4097499400.00000000038A1000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000003.3135596733.0000000001141000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000003.3135031847.00000000013A5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000000A.00000002.4096629893.0000000001006000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 7%, ReversingLabs
Reputation:	moderate
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	0	65536	success or wait	1	AD12FD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	0	4096	success or wait	1	AD12FD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	0	512	success or wait	2	AD12FD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	0	512	success or wait	1	AD12FD	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\334343\e	0	309760	success or wait	1	AD12FD	ReadFile
C:\ProgramData\IIIJECAEGDHIDHJKKKKFIEGIJK	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\FIJKEHJJ	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\FIJKEHJJ	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\JJECAAEHCFIEBGCBGHIE	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\JJJKEHCA	0	100	success or wait	9	1000FE09	ReadFile
C:\ProgramData\JJJKEHCA	0	100	success or wait	9	1000FE09	ReadFile
C:\ProgramData\JJJKEHCA	0	100	success or wait	9	1000FE09	ReadFile
C:\ProgramData\JEBKJDAF	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\JEBKJDAF	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\GHJDGDBFCBKFHJKFHCBK	0	100	success or wait	6	1000FE09	ReadFile
C:\ProgramData\KKJJEBFC	0	100	success or wait	20	1000FE09	ReadFile

Analysis Process: PING.EXE PID: **7404**, Parent PID: **7180**

General

Target ID:	11
Start time:	09:28:58
Start date:	08/05/2024
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping -n 5 127.0.0.1
Imagebase:	0xe70000
File size:	18'944 bytes
MD5 hash:	B3624DD758CCECF93A1226CEF252CA12
Has elevated privileges:	true

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly