ID: 753126
Sample Name: c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.exe
Cookbook: default.jbs
Time: 10:48:03
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

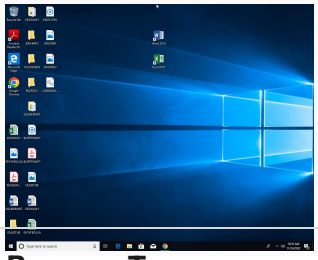
Windows Analysis Report

c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.exe

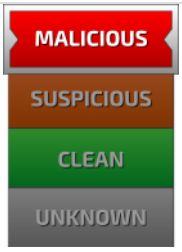
Overview

General Information

Sample Name:	c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.exe (renamed file extension from exe to dll)
Analysis ID:	753126
MD5:	590d96a7be5524.
SHA1:	2aaf8acb010dfe8..
SHA256:	846a8058cda542..
Tags:	exe
Infos:	



Detection



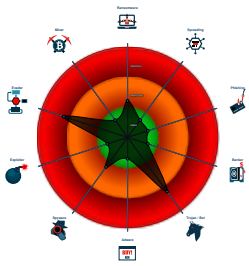
Ursnif

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Ursnif
- System process connects to networ…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Queries the volume information (nam…
- Tries to load missing DLLs
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…
- PE file contains sections with non-s…
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 2512 cmdline: loaddll64.exe "C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 5992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5972 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5932 cmdline: rundll32.exe "C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - cmd.exe (PID: 3308 cmdline: cmd /c "echo Commands" >> C:\Users\user~1\AppData\Local\Temp\AEC4.tmp MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 1716 cmdline: cmd /c "dir" >> C:\Users\user~1\AppData\Local\Temp\AEC4.tmp MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 5952 cmdline: regsvr32.exe /s C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5960 cmdline: rundll32.exe C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6072 cmdline: rundll32.exe C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll,FgnfMvSNFULXZx MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2668 cmdline: rundll32.exe C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll,KVpawdrrKTUjeZuk MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "c2_domain": [
    "https://higmon.cyou",
    "https://prises.cyou"
  ],
  "botnet": "202208151",
  "aes key": "VHpr3Unea0fVqBYc",
  "sleep time": "1",
  "request time": "10",
  "host keep time": "2",
  "host shift time": "1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: loaddll64.exe PID: 2512	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	
Process Memory Space: regsvr32.exe PID: 5952	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 5932	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 5960	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Observed DNS Query to Ursnif Domain (higmon .cyou) - Source IP: 192.168.2.7 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.78.8.8.860326532039637 11/24/22-10:49:03.324067
SID:	2039637
Source Port:	60326
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

Snort IDS alert for network traffic

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion

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

Stealing of Sensitive Information

Yara detected Ursnif

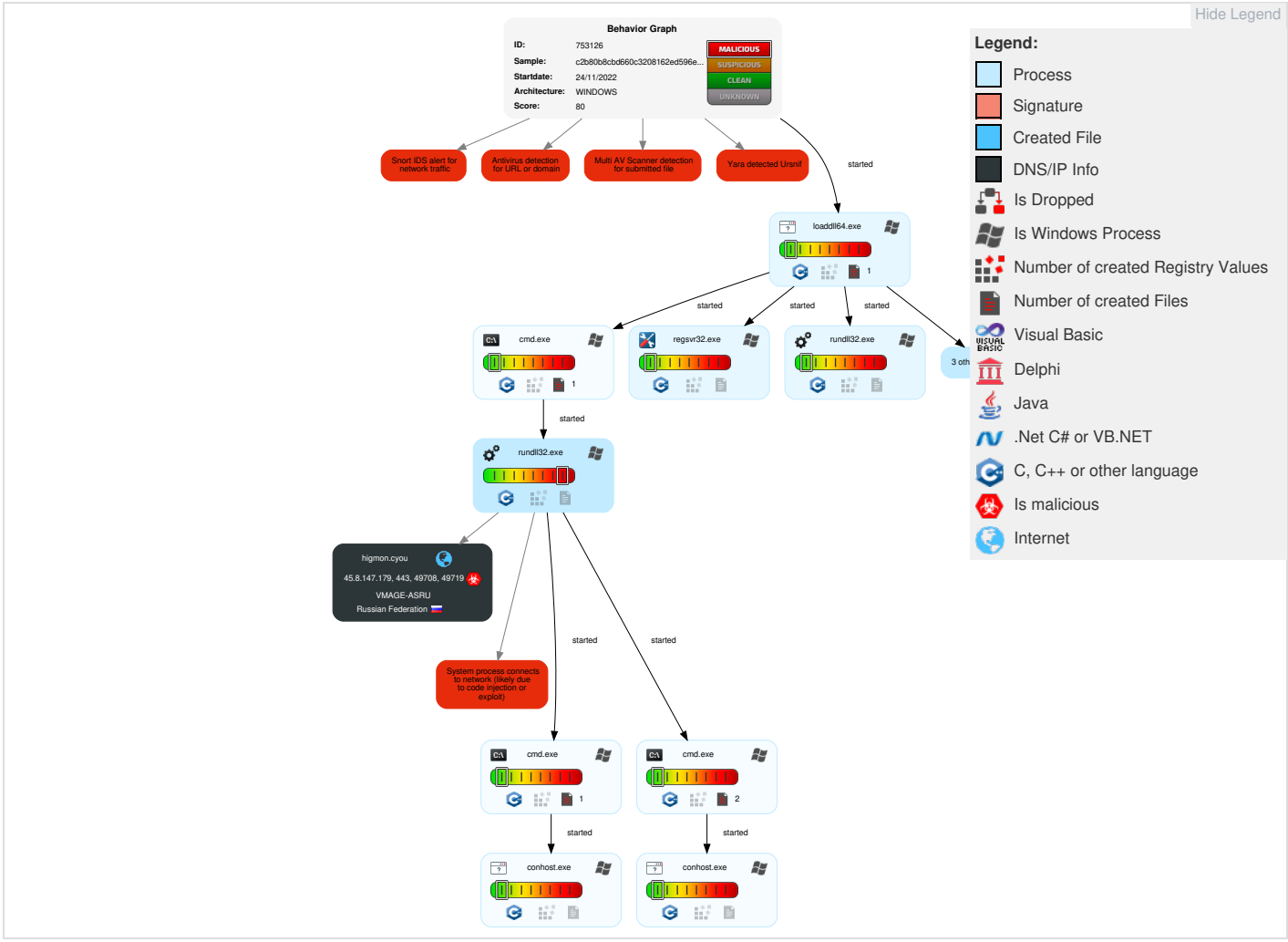
Remote Access Functionality

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 1 Process Injection	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Regsvr32	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

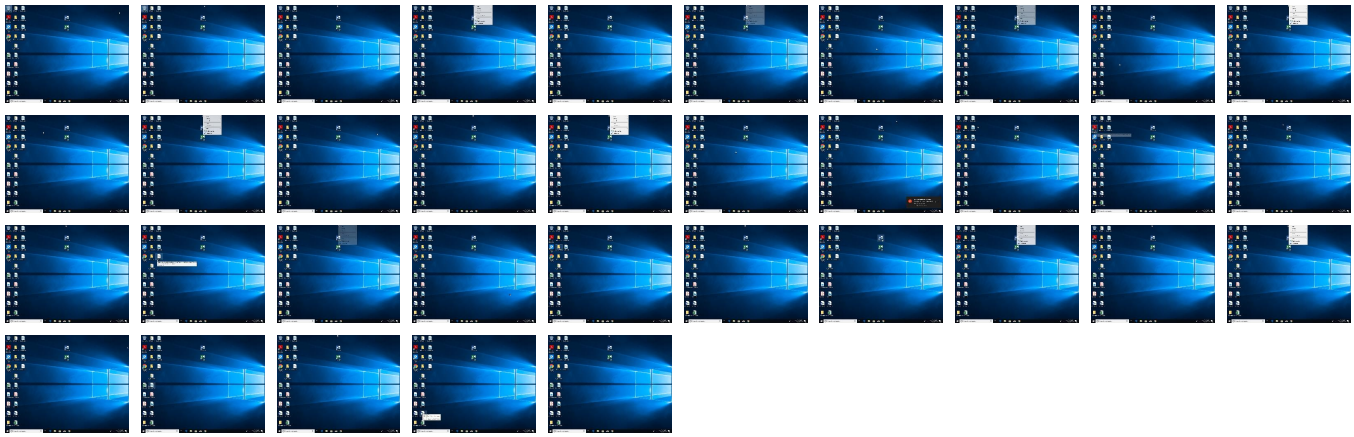
Behavior Graph



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
c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll	22%	ReversingLabs	Win64.Trojan.IcedID	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://higmon.cyou/index.html7b9a	100%	Avira URL Cloud	malware	
http://https://Mozilla/5.0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://higmon.cyouhttps://prises.cyouR	0%	Avira URL Cloud	safe	
http://https://higmon.cyou/index.html	100%	Avira URL Cloud	malware	
http://https://higmon.cyou	100%	Avira URL Cloud	malware	
http://https://higmon.cyou/	100%	Avira URL Cloud	malware	
http://https://prises.cyou	100%	Avira URL Cloud	malware	

Domains and IPs

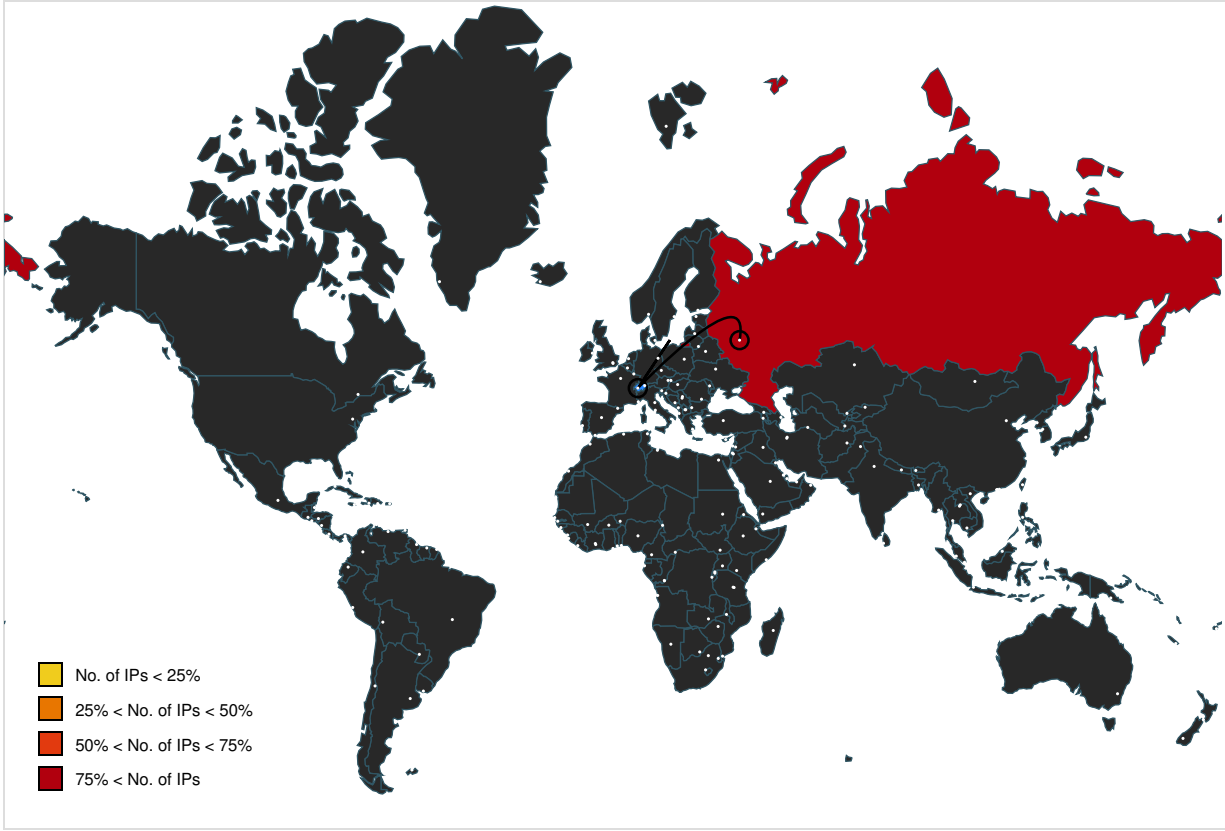
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
higmon.cyou	45.8.147.179	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://higmon.cyou/index.html7b9a	rundll32.exe, 00000004.00000002.76472393 4.000001C7146DB000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http:// https://my.tealiumiq.com/urest/legacy/tagcompanion/getProfile?utid=	rundll32.exe, rundll32.exe, 00000004.00000002.7653 46850.00007FFE35483000.00000008.00000001 .01000000.00000003.sdmp, c2b80b8cbd660c3 208162ed596e0443ea8f786b6fd1f809f2d2a1e0 7fe6475cd.dll	false		high
http://https://higmon.cyou/index.html	rundll32.exe, 00000004.00000002.76496117 8.000001C714740000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.764723934.000001C7146DB000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://Mozilla/5.0	loaddll64.exe, 00000000.00000002.2651718 62.000001FF43732000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0003.00000002.246612763.0000000002F42000 .00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.765260621.00000 1C716532000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000005.000 00002.247438709.000001817DA62000.0000000 4.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://higmon.cyou	loaddll64.exe, 00000000.00000002.2651650 48.000001FF43730000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0003.00000002.246608034.0000000002F40000 .00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.765253557.00000 1C716530000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000004.000 00002.765191980.000001C71618E000.0000000 4.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000002.247434802.000001817DA60 000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://higmon.cyouhttps://prises.cyouR	rundll32.exe, 00000004.00000002.76519198 0.000001C71618E000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://prises.cyou	loaddll64.exe, 00000000.00000002.2651650 48.000001FF43730000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0003.00000002.246608034.0000000002F40000 .00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.765253557.00000 1C716530000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000004.000 00002.765191980.000001C71618E000.0000000 4.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000002.247434802.000001817DA60 000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://higmon.cyou/	rundll32.exe, 00000004.00000002.76488286 3.000001C71471F000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.764961178.000001C714740000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.147.179	higmon.cyou	Russian Federation		44676	VMAGE-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753126
Start date and time:	2022-11-24 10:48:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.exe (renamed file extension from exe to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.evad.winDLL@20/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.5% (good quality ratio 19.5%) • Quality average: 40.1% • Quality standard deviation: 34.5%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll

Simulations

Behavior and APIs

Time	Type	Description
10:49:10	API Interceptor	1x Sleep call for process: loaddll64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\AEC4.tmp

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1558
Entropy (8bit):	4.6826840372617475
Encrypted:	false
SSDEEP:	48:kv2LdasaxnvlFaPMapaIaGaeau7agOV2av6Y8ZtaLaK:YlH
MD5:	7BEC34850EB3436F93D778F9C7353D0E
SHA1:	85BF8EE675F70D906E56E33442726602BDDACC27
SHA-256:	B779CF426802A01B413615C45A7730427AFB336C9BE53BD5B59D07AC2CAA4ED6
SHA-512:	8D44C53446E02FB053B6BEEB424C6C93F436695C87BCAF3C29543C55FBF18DB6D045FC9D80E62A55E48BF346093C3C4B241DAFFD8BA22E1F57D32B58866EA4AC

Malicious:	false
Preview:	Commands .. Volume in drive C has no label... Volume Serial Number is C820-F8D1.... Directory of C:\Users\user\Desktop....11/24/2022 10:48 AM <DIR> ...11/24/2022 10:48 AM <DIR> ....08/16/2022 02:37 PM 1,026 BJZFPPWAPT.mp3..08/16/2022 02:37 PM 1,026 BJZFPPWAPT.pdf..11/24/2022 10:48 AM 538,624 c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll..08/16/2022 02:37 PM <DIR> DUUDTUBZFW..08/16/2022 02:37 PM 1,026 DUUDTUBZFW.jpg..08/16/2022 02:37 PM <DIR> EEGWXUHVUG..08/16/2022 02:37 PM 1,026 EEGWXUHVUG.docx..08/16/2022 02:37 PM 1,026 EEGWXUHVUG.xlsx..08/16/2022 02:37 PM 1,026 EFOYFBOLXA.jpg..08/16/2022 02:37 PM 1,026 EFOYFBOLXA.xlsx..08/16/2022 02:37 PM 1,026 EWZCVGNOWT.mp3..07/23/2020 10:38 AM 2,660 Excel 2016.lnk..08/16/2022 02:37 PM 1,026 GRXZDKKVDB.png..08/16/2022 02:37 PM

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.822863121964014
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 77.79% • Windows Screen Saver (13104/52) 9.99% • Win64 Executable (generic) (12005/4) 9.16% • Generic Win/DOS Executable (2004/3) 1.53% • DOS Executable Generic (2002/1) 1.53%
File name:	c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll
File size:	538624
MD5:	590d96a7be55240ad868ebec78ce38f2
SHA1:	2aaf8acb010dfe83b808d7cc77f6821aaf44f3d2
SHA256:	846a8058cda54207aebb885f99dab0eab57529eb8dd94a3d57bbde2e93c4aad4
SHA512:	9360564b79909f934db9120315d981d3b2bf5e1f853baa0145d7ff9b0ac375d452d11d86f90dfe5547fdbd8f4f04a8f4fd2f73c50eab2df7bddb8207194d126a
SSDEEP:	6144:al+x6f16rj6MrQeQap0+TMPRxWer+YeZczE72q1i6qs6Yfs:a4416SCpXMPjWce+Eqq1i6qdas
TLSH:	D8B46D60B11030FFF6ABC039B1C66BD96279B113E9524DBEF05A98D48B8878B1177F19
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.}.1...1...1.....6...1...>.....0.....0.....0.....0...Rich1.....PE..d.....2c....." .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180001000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6332D8E8 [Tue Sep 27 11:05:12 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	16a8f4e2ed702e8523beef35ae5110a0

Entrypoint Preview

Instruction
jmp 00007FB3A0A0DDFCh
mov eax, 00000001h

Instruction
add eax, 00000000h
jmp 00007FB3A0A0DDE2h
dec eax
add esp, 18h
ret
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 18h
jmp 00007FB3A0A0DDEDh
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
jmp 00007FB3A0A0DDCCh
mov eax, dword ptr [esp+28h]
mov dword ptr [esp], eax
jmp 00007FB3A0A0DDB4h
jmp 00007FB3A0A0DF88h
mov byte ptr [esp+67h], 0000000Ah
add byte ptr [esp+67h], 00000066h
jmp 00007FB3A0A0DDFAh
mov byte ptr [esp+64h], 00000012h
add byte ptr [esp+64h], 00000026h
jmp 00007FB3A0A0DE34h
mov byte ptr [esp+66h], 0000000Dh
add byte ptr [esp+66h], 00000062h
jmp 00007FB3A0A0DDBEh
mov byte ptr [esp+68h], 00000034h
add byte ptr [esp+68h], 00000030h
jmp 00007FB3A0A0DE04h
add dx, 000Ah
xor ecx, ecx
jmp 00007FB3A0A0DFD3h
mov byte ptr [esp+6Bh], 0000001Eh
add byte ptr [esp+6Bh], 00000055h
jmp 00007FB3A0A0DDE2h
mov byte ptr [esp+6Ch], 00000000h
mov dx, 0011h
jmp 00007FB3A0A0DDC0h
mov byte ptr [esp+69h], 00000032h
add byte ptr [esp+69h], 00000047h
jmp 00007FB3A0A0DDE2h
mov byte ptr [esp+6Ah], 00000004h
add byte ptr [esp+6Ah], 00000070h
jmp 00007FB3A0A0DDB3h
mov byte ptr [esp+65h], 00000041h
add byte ptr [esp+65h], 0000002Bh
jmp 00007FB3A0A0DD84h
call 00007FB3A0A0DFD3h
xor eax, eax
jmp 00007FB3A0A0DEE0h
call dword ptr [00000F5Bh]
test eax, eax
jne 00007FB3A0A0DDD1h
jmp 00007FB3A0A0DF71h
call dword ptr [00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2090	0x144	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x21d4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x85000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	0x2000	0x90	.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	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xfe0	0x1000	False	0.59130859375	DOS executable (COM)	5.742356131814896	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x41a	0x600	False	0.380859375	COM executable for DOS	3.47027698168912	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sedt	0x3000	0x81ad6	0x81c00	False	0.3247832369942196	data	5.775703252117877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x85000	0x1e0	0x200	False	0.52734375	data	4.719348272345726	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x85060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	VirtualAlloc, GetConsoleMode, PeekConsoleInputA, ReadConsoleA, FlushConsoleInputBuffer, GetConsoleScreenBufferInfo, SetConsoleCursorPosition, SetConsoleTextAttribute, ReadConsoleOutputA, GetCurrentConsoleFont
USER32.dll	GetScrollBarInfo, DefMDIChildProcW
USP10.dll	ScriptXtoCP, ScriptString_pSize, ScriptTextOut

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180001030
FgnfMvSNFULXZx	2	0x180001e60
KVpawdrrKTUjeZuk	3	0x180001e3c
LaEiyoOgoiNTr	4	0x180001f5c
WOlqmpYHUmo	5	0x180001e84
XEuCWLzwGSc	6	0x180001ea8
ZdXkUtuwLqhmt	7	0x180001f38
aLcPpKozZltuf	8	0x180001f14
cNtNVfZnIZvqyMq	9	0x180001ecc
hbOlyYikdaBLyqU	10	0x180001ef0
zJhDuUvYOmGa	11	0x180001e18

Possible Origin

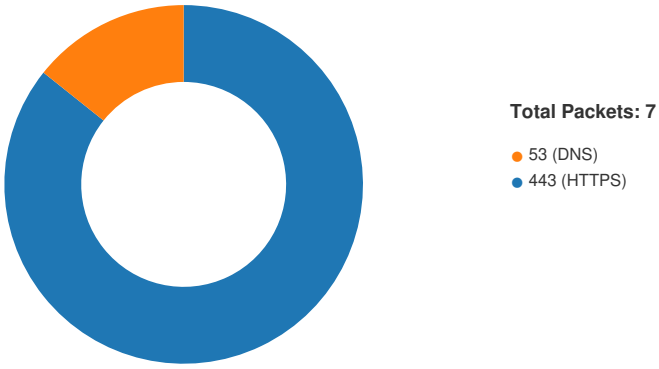
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.78.8.8.8.8603265 32039637 11/24/22-10:49:03.324067	UDP	2039637	ET TROJAN Observed DNS Query to Ursnif Domain (higmon .cyou)	60326	53	192.168.2.7	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 10:49:03.362545013 CET	49708	443	192.168.2.7	45.8.147.179
Nov 24, 2022 10:49:03.362597942 CET	443	49708	45.8.147.179	192.168.2.7
Nov 24, 2022 10:49:03.362678051 CET	49708	443	192.168.2.7	45.8.147.179
Nov 24, 2022 10:49:03.368077993 CET	49708	443	192.168.2.7	45.8.147.179
Nov 24, 2022 10:49:03.368100882 CET	443	49708	45.8.147.179	192.168.2.7
Nov 24, 2022 10:51:14.267262936 CET	443	49708	45.8.147.179	192.168.2.7
Nov 24, 2022 10:51:14.270287037 CET	49719	443	192.168.2.7	45.8.147.179
Nov 24, 2022 10:51:14.270345926 CET	443	49719	45.8.147.179	192.168.2.7
Nov 24, 2022 10:51:14.270559072 CET	49719	443	192.168.2.7	45.8.147.179
Nov 24, 2022 10:51:14.272161007 CET	49719	443	192.168.2.7	45.8.147.179
Nov 24, 2022 10:51:14.272178888 CET	443	49719	45.8.147.179	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 10:49:03.324067116 CET	60326	53	192.168.2.7	8.8.8.8
Nov 24, 2022 10:49:03.342747927 CET	53	60326	8.8.8.8	192.168.2.7

DNS Queries

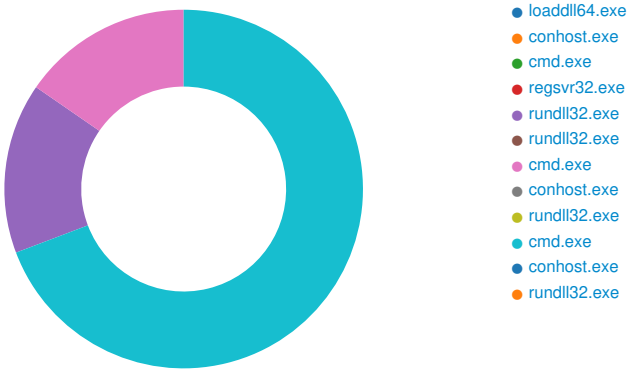
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 10:49:03.324067116 CET	192.168.2.7	8.8.8.8	0xe611	Standard query (0)	higmon.cyou	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 10:49:03.342747927 CET	8.8.8.8	192.168.2.7	0xe611	No error (0)	higmon.cyou		45.8.147.179	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 2512, Parent PID: 3320

General

Target ID:	0
Start time:	10:49:00
Start date:	24/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll"
Imagebase:	0x7ff6962f0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5992, Parent PID: 2512

General

Target ID:	1
Start time:	10:49:00
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5972**, Parent PID: **2512**

General

Target ID:	2
Start time:	10:49:00
Start date:	24/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll",#1
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5952**, Parent PID: **2512**

General

Target ID:	3
Start time:	10:49:00
Start date:	24/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll
Imagebase:	0x7ff7ccb40000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **5932**, Parent PID: **5972**

General

Target ID:	4
Start time:	10:49:00
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll",#1
Imagebase:	0x7ff739200000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEC4.tmp	success or wait	1	180001A45	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEC4.tmp	unknown	1558	success or wait	1	1800010A5	ReadFile

Analysis Process: rundll32.exe PID: **5960**, Parent PID: **2512**

General

Target ID:	5
Start time:	10:49:00
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll,DllRegisterServer
Imagebase:	0x7ff739200000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **3308**, Parent PID: **5932**

General

Target ID:	6
Start time:	10:49:03
Start date:	24/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c "echo Commands" >> C:\Users\user~1\AppData\Local\Temp\AEC4.tmp
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\AEC4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7651BC614	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEC4.tmp	0	11	43 6f 6d 6d 61 6e 64 73 20 0d 0a	Commands	success or wait	1	7FF7651C275B	WriteFile

Analysis Process: conhost.exe PID: **3828**, Parent PID: **3308**

General	
Target ID:	7
Start time:	10:49:03
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **6072**, Parent PID: **2512**

General	
Target ID:	8
Start time:	10:49:03
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll,FgnfMvSNFULXZx
Imagebase:	0x7ff739200000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1716**, Parent PID: **5932**

General	
Target ID:	9
Start time:	10:49:04
Start date:	24/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c "dir" >> C:\Users\user~1\AppData\Local\Temp\AEC4.tmp
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEC4.tmp	11	34	20 56 6f 6c 75 6d 65 20 69 6e 20 64 72 69 76 65 20 43 20 68 61 73 20 6e 6f 20 6c 61 62 65 6c 2e 0d 0a	Volume in drive C has no label.	success or wait	1	7FF7651C275B	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	45	36	20 56 6f 6c 75 6d 65 20 53 65 72 69 61 6c 20 4e 75 6d 62 65 72 20 69 73 20 43 38 32 30 2d 46 38 44 31 0d 0a	Volume Serial Number is C820-F8D1	success or wait	1	7FF7651C275B	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	81	2	0d 0a		success or wait	1	7FF7651C6729	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	83	44	20 44 69 72 65 63 74 6f 72 79 20 6f 66 20 43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 0d 0a 0d 0a	Directory of C:\Users\user\Desktop	success or wait	1	7FF7651C275B	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	127	40	31 31 2f 32 34 2f 32 30 32 32 20 20 31 30 3a 34 38 20 41 4d 20 20 20 20 3c 44 49 52 3e 20 20 20 20 20 20 20 20 20 20 2e	11/24/2022 10:48 AM <DIR> .	success or wait	24	7FF7651C275B	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	167	2	0d 0a		success or wait	24	7FF7651C6729	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	1459	47	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 31 36 20 46 69 6c 65 28 73 29 20 20 20 20 20 20 20 20 35 35 37 2c 36 38 31 20 62 79 74 65 73 0d 0a	16 File(s) 557,681 bytes	success or wait	1	7FF7651C275B	WriteFile
C:\Users\user\AppData\Local\Temp\AEC4.tmp	1506	52	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 38 20 44 69 72 28 73 29 20 20 38 35 2c 38 39 38 2c 33 30 31 2c 34 34 30 20 62 79 74 65 73 20 66 72 65 65 0d 0a	8 Dir(s) 85,898,301,440 bytes free	success or wait	1	7FF7651C275B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEC4.tmp	unknown	1	success or wait	1	7FF7651BC762	ReadFile

Analysis Process: conhost.exe PID: **4248**, Parent PID: **1716**

General

Target ID:	10
Start time:	10:49:04
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **2668**, Parent PID: **2512**

General	
Target ID:	11
Start time:	10:49:07
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\c2b80b8cbd660c3208162ed596e0443ea8f786b6fd1f809f2d2a1e07fe6475cd.dll,KVpawdrrKTUjeZuk
Imagebase:	0x7ff739200000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly