ID: 553121
Sample Name:
urMpgNNXPM.exe
Cookbook: default.jbs
Time: 10:50:44
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

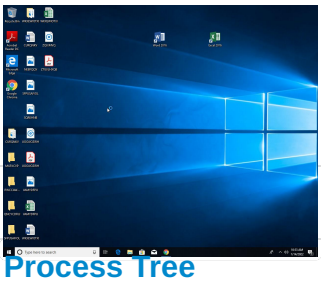
Windows Analysis Report urMpgNNXPM.exe

Overview

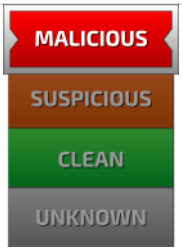
General Information

Sample Name:	urMpgNNXPM.exe
Analysis ID:	553121
MD5:	c94a5671588abb..
SHA1:	a04fe7f0944c051..
SHA256:	50bee5c11d3905..
Tags:	exe RaccoonStealer
Infos:	

Most interesting Screenshot:



Detection



Amadey Raccoon RedLine SmokeLoader Tofsee Vidar

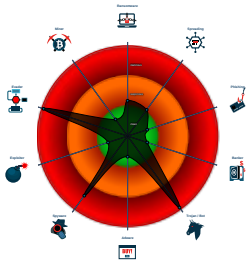
Score: 100
Range: 0 - 100

Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e.…
- Yara detected Amadeys stealer DLL
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- Yara detected Amadey bot
- System process connects to networ…
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Sigma detected: Suspect Svchost A…

Classification



Process Tree

- **System is w10x64**
- urMpgNNXPM.exe (PID: 7052 cmdline: "C:\Users\user\Desktop\urMpgNNXPM.exe" MD5: C94A5671588ABB64EAB63DB753FF3DDE)
  - urMpgNNXPM.exe (PID: 7120 cmdline: "C:\Users\user\Desktop\urMpgNNXPM.exe" MD5: C94A5671588ABB64EAB63DB753FF3DDE)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 7CF6.exe (PID: 6592 cmdline: C:\Users\user\AppData\Local\Temp\7CF6.exe MD5: 277680BD3182EB0940BC356FF4712BEF)
        - WerFault.exe (PID: 5900 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6592 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - 8D62.exe (PID: 6784 cmdline: C:\Users\user\AppData\Local\Temp\8D62.exe MD5: 69D8C52799339ABA9407830AB8AA210B)
      - F9FC.exe (PID: 6248 cmdline: C:\Users\user\AppData\Local\Temp\F9FC.exe MD5: 8B25D9317E18654C3F83EF8630D1DE16)
        - cmd.exe (PID: 4624 cmdline: "C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\cnuxfiv\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 3576 cmdline: "C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\mtkthtmd.exe" C:\Windows\SysWOW64\cnuxfiv\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 6068 cmdline: C:\Windows\System32\sc.exe" create cnuxfiv binPath= "C:\Windows\SysWOW64\cnuxfiv\mtkthtmd.exe /d\"C:\Users\user\AppData\Local\Temp\F9FC.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 4216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5400 cmdline: C:\Windows\System32\sc.exe" description cnuxfiv "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 4272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 660 cmdline: "C:\Windows\System32\sc.exe" start cnuxfiv MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 4860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 5356 cmdline: "C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - conhost.exe (PID: 400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 4BB.exe (PID: 5128 cmdline: C:\Users\user\AppData\Local\Temp\4BB.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
        - 4BB.exe (PID: 6040 cmdline: C:\Users\user\AppData\Local\Temp\4BB.exe MD5: D7DF01D8158BFADDC8BA48390E52F355)
      - 6DF6.exe (PID: 6548 cmdline: C:\Users\user\AppData\Local\Temp\6DF6.exe MD5: 852D86F5BC34BF4AF7FA89C60569DF13)
      - 8DA4.exe (PID: 7060 cmdline: C:\Users\user\AppData\Local\Temp\8DA4.exe MD5: 8B239554FE346656C8EEF9484CE8092F)
        - mjlooy.exe (PID: 4684 cmdline: "C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe" MD5: 8B239554FE346656C8EEF9484CE8092F)
          - cmd.exe (PID: 5820 cmdline: "C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\82aa4a6c48\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - B169.exe (PID: 1684 cmdline: C:\Users\user\AppData\Local\Temp\B169.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
      - D1D3.exe (PID: 5400 cmdline: C:\Users\user\AppData\Local\Temp\D1D3.exe MD5: 5800952B83AECEFC3AA06CCB5B29A4C2)
- svchost.exe (PID: 4708 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3640 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5620 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- brgebic (PID: 5636 cmdline: C:\Users\user\AppData\Roaming\brgebic MD5: C94A5671588ABB64EAB63DB753FF3DDE)
  - brgebic (PID: 6596 cmdline: C:\Users\user\AppData\Roaming\brgebic MD5: C94A5671588ABB64EAB63DB753FF3DDE)
- svchost.exe (PID: 6848 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6908 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6592 -ip 6592 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6684 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- mtkthtmd.exe (PID: 528 cmdline: C:\Windows\SysWOW64\cnuxfiv\mtkthtmd.exe /d"C:\Users\user\AppData\Local\Temp\F9FC.exe" MD5: 6697E6F7370892D5B7251882BEDAD002)
  - svchost.exe (PID: 5920 cmdline: svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 6732 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000002F.00000002.626880122.000000000738000.00000004.00000001.sdmp	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
00000014.00000002.490147726.000000000630000.00000040.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	

Source	Rule	Description	Author	Strings
0000002A.00000002.638483235.0000000004D1 0000.00000040.00000001.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
00000005.00000000.392146415.0000000002E3 1000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000002.00000002.407856003.000000000058 0000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.urMpgNNXPM.exe.5615a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
13.1.brgebic.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
37.3.mtkthtmd.exe.650000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
39.2.svchost.exe.2e90000.0.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
37.2.mtkthtmd.exe.740000.2.raw.unpack	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
Click to see the 38 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity
Sigma detected: Copying Sensitive Files with Credential Data
Sigma detected: Suspicious Svchost Process
Sigma detected: Netsh Port or Application Allowed
Sigma detected: New Service Creation

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara detected Raccoon Stealer
Antivirus detection for URL or domain
Antivirus detection for dropped file
Multi AV Scanner detection for submitted file
Multi AV Scanner detection for domain / URL
Machine Learning detection for sample
Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
System process connects to network (likely due to code injection or exploit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara detected Raccoon Stealer

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains method to dynamically call methods (often used by packers)

Persistence and Installation Behavior:

Yara detected Amadey bot

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

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

Found evasive API chain (may stop execution after checking locale)

Tries to detect virtualization through RDTSC time measurements

Checks if the current machine is a virtual machine (disk enumeration)

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Contains functionality to detect sleep reduction / modifications

Found evasive API chain (may stop execution after checking computer name)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Raccoon Stealer

Yara detected Vidar stealer

Yara detected Tofsee

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

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

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected Raccoon Stealer

Yara detected Vidar stealer

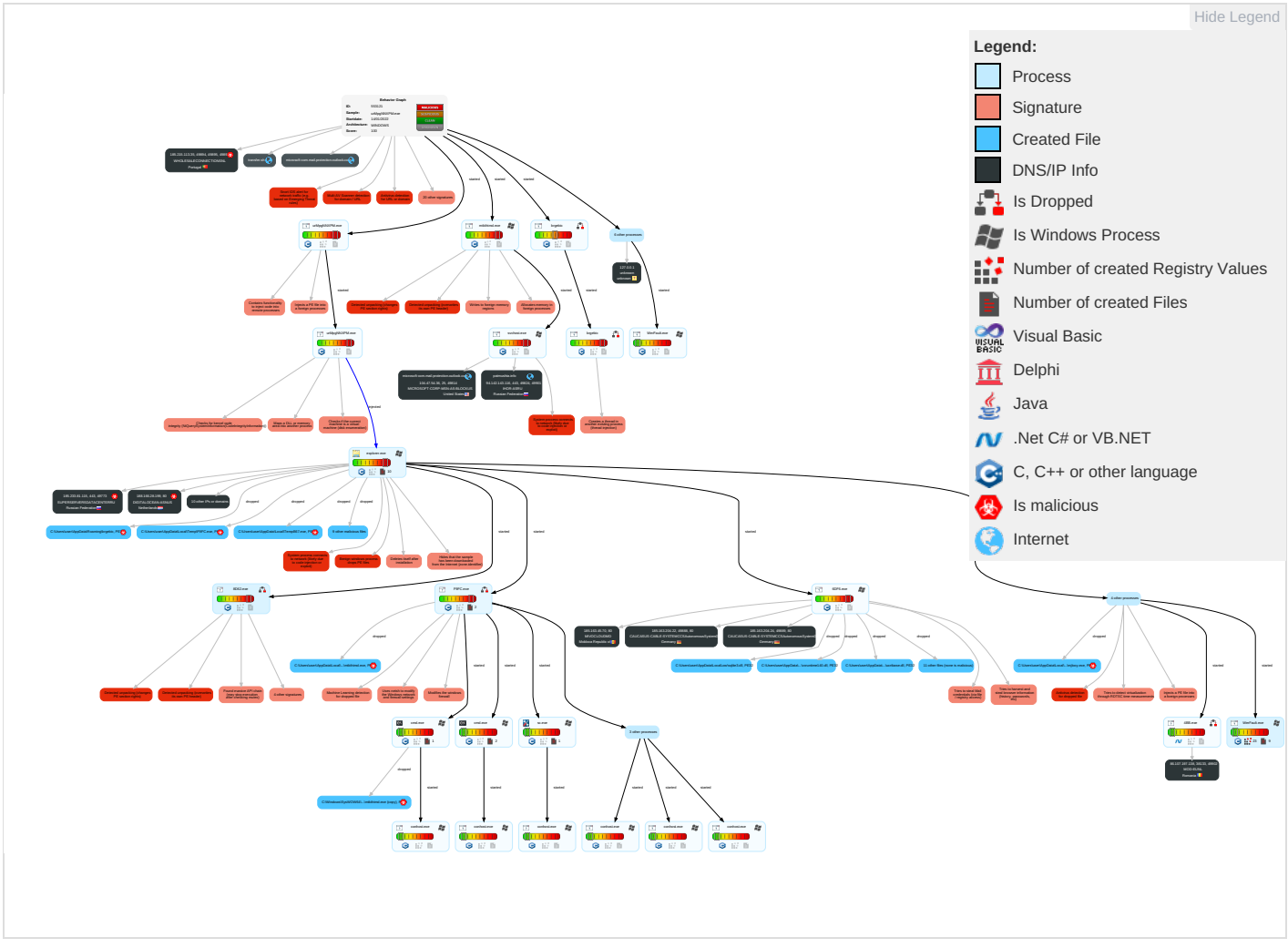
Yara detected Tofsee

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Native API 5 3 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Exploitation for Client Execution 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	Command and Scripting Interpreter 3	Windows Service 1 4	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Sta Port 1
Local Accounts	Service Execution 3	Logon Script (Mac)	Windows Service 1 4	Software Packing 3 3	NTDS	System Information Discovery 3 3 8	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Non-Applicat Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Process Injection 7 1 3	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Applicat Layer Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 5 7 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multibar Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Pc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 4 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Valid Accounts 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Virtualization/Sandbox Evasion 2 4 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 7 1 3	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Hidden Files and Directories 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

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
urMpgNNXPM.exe	40%	ReversingLabs	Win32.Trojan.Generic	
urMpgNNXPM.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\4BB.exe	100%	Avira	HEUR/AGEN.1211353	
C:\Users\user\AppData\Local\Temp\F9FC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7CF6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8D62.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\EB67.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\F432.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B169.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8DA4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D1D3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4BB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6DF6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	2%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\nssdbm3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\nssdbm3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.8D62.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.1.brgebic.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.3.7CF6.exe.600000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.4BB.exe.ea0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.2.4BB.exe.ea0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
42.3.6DF6.exe.4d10000.2.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
13.0.brgebic.400000.2.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
14.2.7CF6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.brgebic.400000.3.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
2.0.urMpgNNXPM.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.3.mtkthtmd.exe.650000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.4BB.exe.ea0000.7.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.4BB.exe.ea0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.4BB.exe.ea0000.11.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.3.F9FC.exe.660000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.4BB.exe.ea0000.5.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
2.0.urMpgNNXPM.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.brgebic.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.4BB.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
20.2.F9FC.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
45.2.8DA4.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143239		Download File
42.2.6DF6.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1127993		Download File
40.0.4BB.exe.ea0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
13.0.brgebic.400000.0.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
37.2.mtkthtmd.exe.740000.2.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
39.2.svchost.exe.2e90000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
13.0.brgebic.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.mtkthtmd.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.2.brgebic.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.7CF6.exe.5d0e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.4BB.exe.cd0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
21.0.4BB.exe.cd0000.2.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.4BB.exe.ea0000.3.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
40.0.4BB.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
40.0.4BB.exe.ea0000.9.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
20.2.F9FC.exe.630e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.4BB.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
21.2.4BB.exe.cd0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
0.2.urMpgNNXPM.exe.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.0.brgebic.400000.1.unpack	100%	Avira	HEUR/AGEN.1123244		Download File
17.2.8D62.exe.560e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
40.0.4BB.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
13.0.brgebic.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.brgebic.5615a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.urMpgNNXPM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.4BB.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
14.0.7CF6.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.mtkthtmd.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
21.0.4BB.exe.cd0000.0.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.0.7CF6.exe.5d0e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.4BB.exe.ea0000.13.unpack	100%	Avira	HEUR/AGEN.1211353		Download File
14.0.7CF6.exe.5d0e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.3.8D62.exe.580000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.1.urMpgNNXPM.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.0.4BB.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1145065		Download File
2.0.urMpgNNXPM.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.7CF6.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.0.4BB.exe.cd0000.1.unpack	100%	Avira	HEUR/AGEN.1211353		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://185.163.204.24/n	0%	Avira URL Cloud	safe	
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	13%	Virustotal		Browse
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	0%	Avira URL Cloud	safe	
http://185.163.204.24/	4%	Virustotal		Browse
http://185.163.204.24/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/bbdc967e1854b9bf89347672adc7c62bedc561f8	0%	Avira URL Cloud	safe	
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	100%	Avira URL Cloud	malware	
http://178.62.113.205/capibar	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://185.163.45.70/capibar	100%	Avira URL Cloud	phishing	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/8bcad42ad965e4d081164a067770c0c3dfa4b869	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://185.163.204.24:80//l/f/N2z-VH4BZ2GIX1a33Fax/8bcad42ad965e4d081164a067770c0c3dfa4b869pkedcjkde	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	false		high
host-data-coin-11.com	8.209.70.0	true	false		high
patmushta.info	94.142.143.116	true	false		high
cdn.discordapp.com	162.159.133.233	true	false		high
microsoft-com.mail.protection.outlook.com	104.47.54.36	true	false		high
goo.su	104.21.38.221	true	false		high
transfer.sh	144.76.136.153	true	false		high
a0621298.xsph.ru	141.8.194.74	true	false		high
data-host-coin-8.com	8.209.70.0	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://185.215.113.35/d2VxjasuwS/index.php?scr=1	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.163.204.24/	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/bbdc967e1854b9bf89347672adc7c62bedc561f8	false	• Avira URL Cloud: safe	unknown
http://a0621298.xsph.ru/9.exe	false		high
http://data-host-coin-8.com/files/9030_1641816409_7037.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/game.exe	false	• URL Reputation: safe	unknown
http://185.163.204.24//l/f/N2z-VH4BZ2GIX1a33Fax/8bcad42ad965e4d081164a067770c0c3dfa4b869	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.163.45.70	unknown	Moldova Republic of		39798	MIVOCLOUDMD	false
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	true
8.209.70.0	host-data-coin-11.com	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
54.38.220.85	unicupload.top	France		16276	OVHFR	false
104.47.54.36	microsoft-com.mail.protection.outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
185.7.214.171	unknown	France		42652	DELUNETDE	true
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.142.143.116	patmushta.info	Russian Federation		35196	IHOR-ASRU	false
185.215.113.35	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
104.21.38.221	goo.su	United States		13335	CLOUDFLARENETUS	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
141.8.194.74	a0621298.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false
185.163.204.22	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false
185.163.204.24	unknown	Germany		20771	CAUCASUS-CABLE-SYSTEMCCSAutonomousSystemGE	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553121
Start date:	14.01.2022
Start time:	10:50:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	urMpgNNXPM.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	51
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@57/48@84/19
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 21.2% (good quality ratio 15.1%) • Quality average: 54.9% • Quality standard deviation: 40.5%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:52:25	Task Scheduler	Run new task: Firefox Default Browser Agent 90D5EFE22E129C95 path: C:\Users\user\AppData\Roaming\brg ebic
10:52:37	API Interceptor	1x Sleep call for process: 8D62.exe modified
10:52:49	API Interceptor	10x Sleep call for process: svchost.exe modified
10:52:56	API Interceptor	1x Sleep call for process: WerFault.exe modified
10:53:26	API Interceptor	4x Sleep call for process: 6DF6.exe modified
10:53:36	Task Scheduler	Run new task: mjlooy.exe path: C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe
10:53:36	API Interceptor	227x Sleep call for process: mjlooy.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24859994025015605
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4W:BJiRdwfu2SRU4W
MD5:	AC367059D85C19D65E1221B971055F62
SHA1:	B34049C90C193F63A4B598A0F085704DC3BFD4CA
SHA-256:	29450451094914E92DBC39735111EC861C260F94CC3E141144ECDCE7D3F1514A
SHA-512:	7A6976084EAB6480DDC8EFFCB91AF8AC2518F27275B0FFE9469079C583BEBA1186B978B47D9AE05BDA4D8DD02EE86298E10FB2107FFFEE84E89B385C98E9C3A
Malicious:	false
Reputation:	unknown
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x4164f616, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25071296422546385
Encrypted:	false
SSDEEP:	384:c+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:DSB2nSB2RSjlK/+mLesOj1J2
MD5:	D81540271B94FD78C71B0EC4BEC2F235
SHA1:	EDB485D896DC2FD20329400C91D34279FCB595E9
SHA-256:	6CA6F1058DB6024C1F8897D1D8A33F600DAD22099EA7730A0125CC5663457AEB
SHA-512:	2A3CC56F0300C03C8B089E5060F5E229BF7680EC9BFBB831C5AB777CBC70C28032BC5DFAF32128017FEF95D3D961DC0E8F0F9A179322CE4242C8FD38A53B4E A
Malicious:	false
Reputation:	unknown
Preview:	Ad..... .....e.f.3...w.....&.....w...5...z..h.(.....3...w.....B.....@..... ....3...w..... .....5...z.u.....S=...5...z..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07714613233559794
Encrypted:	false
SSDEEP:	3:VSF/TEvmQ6Tlc8l/bJdAtiRkpw/toll3VkttlmlnI:QymQwq8t4TF3
MD5:	B29185C7F66EA1FBBC7DD51B41F9A44D
SHA1:	C6650EA32FF1E126FA7C4CFB9CD7B8116CF3444A
SHA-256:	34994D447A739A27994CFB1793CF95ABDE0354FA982E4A0E860C4855346710D3
SHA-512:	1ED8D56101248B3E0724DFD43FD62ABA7832844F7E0BFAF46134CEBED52335659D8D2F02C25AF646147E8144871C0B1CB8683414FD74BE5BE6493F6D49F60EE
Malicious:	false
Reputation:	unknown
Preview:	ue.....3...w...5...z.....w.....w.....w....:O.....w.....S=...5...z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_7CF6.exe_e1efabdc86e5e7d27089b1be821981d81068140_37bb2cbe_1696affc\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8147997216185958
Encrypted:	false
SSDEEP:	96:MpFi5bGLFhsZOQoJ7R3V6tpXIQcQec6tycEfcw3e+HbHg/8BRTf3o8Fa9iVfOyWJ:A0b4Fhd8HQ0lTjIq/u7sfS274ItXTI
MD5:	0789809B5656946BC4B617B5D49AFAC7
SHA1:	8CA546120998988E5DD00D1A2A1A67E0C19C34AF
SHA-256:	A09AE961CCCF5523B30CAAB726EBF03925DF2A9ACA2AE5BB6052BCBC1B4F7DF1
SHA-512:	99A7B1450F24CCCE71D13868811929D611DAD3DCA4DD4C22B864A675D97A76B7482D8C77F9BB93A2687F26251D29F49187E9C4C2A638036BF6C1E2FCC03D925
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.5.9.9.5.9.6.0.6.9.5.2.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.5.9.9.7.2.6.5.3.5.5.5.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.5.c.4.e.9.f.e.-.0.e.1.0.-.4.5.3.f.-.8.d.e.1.-.f.3.d.f.3.6.a.7.c.4.d.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.1.5.9.9.a.9.2.-.8.1.e.3.-.4.e.f.8.-.9.c.e.6.-.e.4.9.b.3.4.c.4.f.c.2.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.7.C.F.6...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.c.0.-.0.0.0.1.-.0.0.1.7.-.e.d.c.f.-.3.4.e.1.7.7.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.2.f.d.e.4.a.7.b.2.8.8.2.e.4.b.f.5.1.5.1.9.5.1.a.a.9.e.1.d.a.c.f.0.0.0.0.2.9.0.1.!.0.0.0.0.5.9.9.5.a.e.9.d.0.2.4.7.0.3.6.c.c.6.d.3.e.a.7.4.1.e.7.5.0.4.c.9.1.3.f.1.f.b.7.6.!.7.C.F.6...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.1././.1.2.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2481.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	50476
Entropy (8bit):	3.0523985593958183

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2481.tmp.csv	
Encrypted:	false
SSDEEP:	1536:keHNMSSBGgc4kLeT7AP2g3TdqFomx8Drv:keHNMSSBGgc4kLeT7AP2g3TdWomx8Drv
MD5:	2EB648534D00CDD243D390FE62F70159
SHA1:	BD543E0239537364AEE7C00DEB4A688BD8C0D2D9
SHA-256:	D362CB5537348A35AEF4334E06489EE8426DDC0D37B80D5EF0B35C34D09E5773
SHA-512:	79515603E3CA2DDD5373CC5AB13B1256427F624B0ECFA109E1741E51C0450CE97ADFC339EC38B521A98B7BF2B088FF357384E7A6EDD4D1CFE0AEB33F4CF554AC
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2935.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696586626327966
Encrypted:	false
SSDEEP:	96:9GiZYWtxGTRYNYTVHWaH5UYEZKqtMiFzFe+XwiinKa8+ZndfklvSq3:9jZDgaGjAiKa8+5dfT6q3
MD5:	ECEB6ED4FDDCDF16AB0DCCC5AF4CB070
SHA1:	3FC6BD931132C6ED8C949CAA59B0FD62F86763F7
SHA-256:	C121DE8363D92FCE189435145A2F32397440538EBBE0BBB1ACE76EEAE197E151
SHA-512:	DDAA6A33A1F59991A6543D5363BA4703BA72EE68BDEF700161EABB12CB38378EAFC1A018510BDEAD0752BB5779DAC88B914B3962F47972F552180B2CF253B5D0
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6DD3.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jan 14 18:52:41 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	36668
Entropy (8bit):	2.1135885608896916
Encrypted:	false
SSDEEP:	192:gyvrDSOeh0kCfd2qziCI1bu6WBo3x22O8MCTDYN:3edogoyOiYN
MD5:	95132D5DB94CE6C1CADD400AA7FCB6F0
SHA1:	605CBB0D261E035B5EC3292EEBF1CC4C533B68D0
SHA-256:	89D86EA8E1CDFE5341C2CB42536B6116C95025531C7678596E0E141682EE531B
SHA-512:	B998B66D9953D201E73D51F7577F6C4B0370F76A35ADD16E4804CA426F09D6A1E2E617C2CBA2EEA12F4F14EB76A2E19FA4374EFC08EECEDD6F45F7C3F908907
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....y..a.....z%.....T.....8.....T.....z.....H.....4.....U.....B.....GenuineIntelW.....T.....m..a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7565.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8390
Entropy (8bit):	3.70079908120978
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNilQH6OK6YJsSUsgmfFRSVWnCpDh89bP/sffbtFm:RrlsNiC6OK6YCSUsgmfFRSVWJPkffbu
MD5:	A6A96D7F78EF275D0AB3C7723EE925C0

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7565.tmp.WERInternalMetadata.xml	
SHA1:	4D6B7ABE79FB3B519F51D2C87728E417DAF6CBEE
SHA-256:	192D860E8F6D5D2C77C174B7331E6B6BF5D3D3FB9580930EB94FA60A3EDD787C
SHA-512:	85530541DC793D20D0EE7015CC601E3BA5AC7E6827F3608783BAD621B956022383EB8ED48D04CE6F17DE6AF7ABEF27BD6415DC6D0459E78B1663AF1B7688E1C
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.5.9.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER78F0.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.477939604568014
Encrypted:	false
SSDEEP:	48:cvIwSD8zsCJgtWI99pWSC8B5d8fm8M4JN8qFO+q8vq8XzLr2jLd:uITfQmYSNmJoK73r2jLd
MD5:	33EA9F72655C73181478E361DCEC4474
SHA1:	D5CBD08306BFE1AD6FA57C445D30FA9427788BCF
SHA-256:	7E49968F726285EE4C31C58CC9B75694F2B1447868C8650611F8949FCF89919F
SHA-512:	24C0640C0877E15F870DAC3E9D2A676C49F41AFB9A346AC45422760B8AA7E85645D9BB4352C3C756848209B1E7B3CDCAE6AD7CA9841827177ABEFF0BC0B992B7
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1342323" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoplvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBoplvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleHandler.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z../{.. ..../{...../{...../{b...../{.....Rich.....PE..L...C@.\.....''!.....b.....0.....~p....@.....p.....h.....0...T..... .....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\AccessibleMarshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA 70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T.. .U..T...U...U...U..T...URich...U.....PE..L...<@.\.....''!.....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T..... .....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....* .....@..@.reloc..<.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\IA2Marshal.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5 A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&|.J...K&|.J...K&|uK...K&|.J...KRich...K.....PE..L...J@.\.....''!.....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false

C:\Users\user\AppData\LocalLow\sG8rM8v\breakpadinjector.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+l.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A.{*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L...@.\.....!.....t.....0.....S....@.....P...P.....(.....`...T.....@.....0..D.....text..... ..`.rdata...l...0...n... .....@..@.data.....@....rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\dI3hX2r.zip	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Reputation:	unknown
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o.....[.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`.M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\.../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.|k.5...XF.Y..lVVW..C..|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..|!.....O....M....>.>.$\.%..L.zF.l...3

C:\Users\user\AppData\LocalLow\sG8rM8v\freebl3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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....@.\.....!.....f.....p.....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false

C:\Users\user\AppData\LocalLow\sG8rM8v\ldap60.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\.....'!.....f..... .....0.....@..... x..... ....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...I.....@....rsrc...x.... .....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ldif60.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich..j.....PE..L....<.\.....'!.....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@..... ....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0..... .@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\nssdbm3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E5E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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....@.\.....'!.....0.....0.....*q....@..... ?.....(@.....`..x.....L.....p.....:.T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsrc...x....`.....@.....@..@.reloc.....p.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9

C:\Users\user\AppData\LocalLow\sG8rM8v\prldap60.dll	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[.$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\.....!.... ... .....%.....0.....p...../....@.....5.....p7..x....P..x.....@.....`..$...`1..T.....1..@.....0..,.....text...2..... ..... ..`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc...x....P.....8.....@..@.reloc..$....`.....<.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\qipcap.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91A9E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W..7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\.....!..... .....`.....r....@.....$..P....@..x.....".....P.. ....T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\softokn3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...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....@.\.....!.....b.....P.....|....@.....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\LocalLow\sG8rM8v\ucrtbase.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.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:FBmF2IIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\LocalLow\sG8rM8v\ucrtbase.dll	
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.....l.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\sG8rM8v\vcruntime140.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.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:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Reputation:	unknown
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\LocalLow\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\6DF6.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z..... .....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... .....".....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsrc..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4BB.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\4BB.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4BB.exe.log	
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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\4BB.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	537088
Entropy (8bit):	5.840438491186833
Encrypted:	false
SSDEEP:	12288:SV2DJxKmQESnLJYydpKDDCrqXSIXcZD0sgbxRo:nK1vVYcZyXSY
MD5:	D7DF01D8158BFADDC8BA48390E52F355
SHA1:	7B885368AA9459CE6E88D70F48C2225352FAB6EF
SHA-256:	4F4D1A2479BA99627B5C2BC648D91F412A7DDDDF4BCA9688C67685C5A8A7078E
SHA-512:	63F1C903FB868E25CE49D070F02345E1884F06EDEC20C9F8A47158ECB70B9E93AAD47C279A423DB1189C06044EA261446CAE4DB3975075759052D264B020262A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?y*.....0..*.....I... ...`....@.. ..... ..@.....`I..K....`..... ..... ..H.....text....).. ...*..... ..`.rsrc.....`.....,.....@....reloc..... .....0.....@..B.....I.....H.....?.....hX..}.....(....*..0..,.....(d...8....*.~....u....s....z&8.....8.....*.....*....(d...(....*...j*..... ..*.....*.....*.....*....(....*.~(....(^...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....z.A.....z.A..... .....*.....*.....*.....*.....

C:\Users\user\AppData\Local\Temp\6DF6.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.I....v....h.....E....x.....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P\|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata.."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\7CF6.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	301056
Entropy (8bit):	5.192330972647351
Encrypted:	false
SSDEEP:	3072:4/ls8LAAkcooHqeUolNx8IA0ZU3D80T840yWrxpzbgqruJnfed:Ils8LA/oHbbLAGOfT8auzbgwuJG
MD5:	277680BD3182EB0940BC356FF4712BEF
SHA1:	5995AE9D0247036CC6D3EA741E7504C913F1FB76
SHA-256:	F9F0AAF36F064CDFC25A12663FFA348EB6D923A153F08C7CA9052DCB184B3570
SHA-512:	0B777D45C50EAE00AD050D3B2A78FA60EB78FE837696A6562007ED628719784655BA13EDCBBEE953F7EEFADE49599EE6D3D23E1C585114D7AECDDDA9AD1D0ECB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\7CF6.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2t..v.i.v.i.v.i.hG..i.i.hG....i.hG..[.i.Q...q.i.v.h...i.hG..w.i.hG..w.i.hG..w.i.Richv.i.....PE..L.....b_.....-.....0....@..... .....e..P.....2..... Y..@.....0.....text..... ..`.rdata..D?...0...@..."....@..@.data...X....p...$...b.....@....rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\82aa4a6c48\mjlooy.exe

Process:	C:\Users\user\AppData\Local\Temp\8DA4.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..U(...(...(...6.).1...6.?.W....l..+...(.....6.8.....6.(.)...6.-.)...Rich(.....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8.....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|.....@..@.reloc..4F...0...H...l.....@..B.....

C:\Users\user\AppData\Local\Temp\8D62.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	323072
Entropy (8bit):	6.713255694252631
Encrypted:	false
SSDEEP:	6144:9AYrD4IBVd8itceyXcaf4bIrehvYrcGYC5L2aQzKPkS:9trD4IBVmBbc70KhOY22aQYk
MD5:	69D8C52799339ABA9407830AB8AA210B
SHA1:	41D1E25A0844778B09CD7733786FFA244FCFF827
SHA-256:	D6F20AD67B08F29828C05878F4381065D8634085129D70D637EFFAE9E6226A1A
SHA-512:	447109CFAFD0F7881A131DE0A26E2EB7A5F8DB9AF8912659F481216951B280471199B28D71B7023BC94D251D20F231EE3205077C50E5E91DD43322327FC7E6B7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R.....PE..L.....`..... .....@.....A.....D...(.....0...@.....D.....text..... ..`.data.....@....yazoj.....@....nukomap.....@....tomoyic.....@....rsrc....."....@..@.reloc..dF.....H.....@..B.....

C:\Users\user\AppData\Local\Temp\8DA4.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373760
Entropy (8bit):	6.990411328206368
Encrypted:	false
SSDEEP:	6144:GszrgLWpo6b1OmohXrIdF5SpBLE4Hy+74YOAnF3YFUGFHWEZq:Gsgq3b1Omsb7pBLEazsYOSGFHFHW
MD5:	8B239554FE346656C8EEF9484CE8092F
SHA1:	D6A96BE7A61328D7C25D7585807213DD24E0694C
SHA-256:	F96FB1160AAAA0B073EF0CDB061C85C7FAF4EFE018B18BE19D21228C7455E489
SHA-512:	CE9945E2AF46CCD94C99C36360E594FF5048FE8E146210CF8BA0D71C34CC3382B0AA252A96646BBFD57A22E7A72E9B917E457B176BCA2B12CC4F662D8430427D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\8DA4.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..U(...(...(...6.).1...6.?.W....l..+...(.....6.8....6.(.)...6.-.)...Rich(..... .....PE..L...a.R`.....v.....@.....@.....&.....(.....{.....0.....@.....8..... .....text..... ..`.data.....@....gizi.....@....bur.....@....wob.....@....rsrc....{.....|..... @..@.reloc..4F...0...H...l.....@..B..... .....

C:\Users\user\AppData\Local\Temp\B169.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3576320
Entropy (8bit):	**7.9976863291960605**
Encrypted:	**true**
SSDEEP:	49152:Y+RSFqeQKgdJee+ntOkgd+TuRCg+687ZEYNFvKfDIcK8nAONaGGh:Yb8eQKg+tOV0T0z875NFKfDPK8nASA
MD5:	5800952B83AECEFC3AA06CCB5B29A4C2
SHA1:	DB51DDBDF8B5B1ABECD6CFAB36514985F357F7A8
SHA-256:	B8BED0211974F32DB2C385350FB62954F0B0F335BC592B51144027956524D674
SHA-512:	2A490708A2C5B742CEB14DE6E2180C4CB606FCCEB5F17DE69249CF532EDC37B984686B534A88AE861CC38471C5892785C26DA68C4F662959542458C583E77E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....!7. .....|.N. .... M..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....x+...P.....@.....1.....@....rsrc..... M.....L0.....@....28gybOo.....N.....1.....@....ada ta.....pS.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\D1D3.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3576320
Entropy (8bit):	**7.9976863291960605**
Encrypted:	**true**
SSDEEP:	49152:Y+RSFqeQKgdJee+ntOkgd+TuRCg+687ZEYNFvKfDIcK8nAONaGGh:Yb8eQKg+tOV0T0z875NFKfDPK8nASA
MD5:	5800952B83AECEFC3AA06CCB5B29A4C2
SHA1:	DB51DDBDF8B5B1ABECD6CFAB36514985F357F7A8
SHA-256:	B8BED0211974F32DB2C385350FB62954F0B0F335BC592B51144027956524D674
SHA-512:	2A490708A2C5B742CEB14DE6E2180C4CB606FCCEB5F17DE69249CF532EDC37B984686B534A88AE861CC38471C5892785C26DA68C4F662959542458C583E77E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....S.....!7. .....|.N. .... M..... .....@.....0.....@.....@ ...z.....@..... ...0.....@.....x+...P.....@.....1.....@....rsrc..... M.....L0.....@....28gybOo.....N.....1.....@....ada ta.....pS.....6.....@..... .....

C:\Users\user\AppData\Local\Temp\EB67.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	905216
Entropy (8bit):	7.399713113456654
Encrypted:	false
SSDEEP:	12288:KoXpNqySLyUDd48BpBIfj2ucA0ZeEbVkw+lMbguodE1z0oLxCZJ9tzj8kpcunn:KoO9FDZpBIMR/4Mzv2Jnp
MD5:	852D86F5BC34BF4AF7FA89C60569DF13
SHA1:	C961CCD088A7D928613B6DF900814789694BE0AE
SHA-256:	2EAA2A4D6C975C73DCBF251EA9343C4E76BDEE4C5DDA8D4C7074078BE4D7FC6F
SHA-512:	B66B83D619A242561B2A7A7364428A554BB72CCC64C3AC3F28FC7C73EFE95C7F9F3AC0401116AE6F7B41B960C323CC3B7ADAC782450013129D9DEC49A81DCE 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\EB67.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g.....q.l....v....h.....E....x....f.....c...Rich.....PE..L....[._. ....2.....0.....0....@.....P|.....q.....Xf..(....p.. .....1.....@Y..@.....0.....text..... .. ..`.rdata.."?...0...@...$.....@..@.data...8....p.....d.....@....rsrc... .n..p.....@..@..... .....

C:\Users\user\AppData\Local\Temp\F432.exe

Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	557664
Entropy (8bit):	7.687250283474463
Encrypted:	false
SSDEEP:	12288:fWxcQhhhhhn8bieAtJlllLtrHWnjkQrK8iBHZkshvesxViA9Og+:fWZhhhhhUATlLtrUbK8oZphveoMA9
MD5:	6ADB5470086099B9169109333FADAB86
SHA1:	87EB7A01E9E54E0A308F8D5EDFD3AF6EBA4DC619
SHA-256:	B4298F77E454BD5F0BD58913F95CE2D2AF8653F3253E22D944B20758BBC944B4
SHA-512:	D050466BE53C33DAAF1E30CD50D7205F50C1ACA7BA13160B565CF79E1466A85F307FE1EC05DD09F59407FCB74E3375E8EE706ACDA6906E52DE6F2DD5FA3ED CD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....5.....0..$...*..... ...`....@.....0.....@....@.....p.....P)..... ..idata...`.....`.pdata.....p.....@....rsrc...P).....0.....@..@.didata.....x.....@..... .....g..L.r9..v9.<iP.hL[Kc...",..

C:\Users\user\AppData\Local\Temp\F9FC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.693203776268283
Encrypted:	false
SSDEEP:	6144:ea1ijIN+Aee6+saxCBxHoM3sDKOd4xncb3wQ:eag8N+Ae2sTvIM5OYncb
MD5:	8B25D9317E18654C3F83EF8630D1DE16
SHA1:	B4503FB92DCB9B4B90E2CD2A534AE38C08F0589A
SHA-256:	1BE428F924402D7CC4586CA37A9E843C869B394F85085DB5E4E85D150AA87E04
SHA-512:	36AD3AD9E9DF0D52DEB4F350880BAEFA3F6871945D566118573AD1511F9CCDE55A5EC205AADCB7ACA156AAFC881587551996BBE27A47B27F8BD596CBCE04E 7B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...5._..... .....@.....D...(.....0...@.....D..... text..... ..`.data.....@....nife.....@....kiza.....@....lagoti.....@....rsrc.....@..@. reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Local\Temp\mtkthtmd.exe

Process:	C:\Users\user\AppData\Local\Temp\F9FC.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14881792
Entropy (8bit):	3.781178022928025
Encrypted:	false
SSDEEP:	6144:Aa1ijIN+Aee6+saxCBxHoM3sDKOd4xncb3wQ:Aag8N+Ae2sTvIM5OYncb
MD5:	6697E6F7370892D5B7251882BEDAD002
SHA1:	31F9BCE889CD859126FC323D7ABBD155FDDF41F2
SHA-256:	44E305DB99461F07B7CFF6648B50531771361A4DFAFA69991527D3963EB88DD2
SHA-512:	1D8E6A71CC886250D6191788C828B3A134C5AAF8E48786CA6E6808802BA74A2902840185690B683E4B3336FF2C0E74E142442B87CBC95A1BABC4B07C4CE94E0
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\mtkthtmd.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...5._.....@.....D...(.....0...@.....D..... text..... ..`.data.....@....nife.....@....kiza.....@....lagoti.....@....rsrc.....@..@. reloc..ZF.....x.....@..B..... .....

C:\Users\user\AppData\Roaming\brgebic	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	319488
Entropy (8bit):	6.693501670017806
Encrypted:	false
SSDEEP:	6144:RnueuQuWjRKidSSUeE+XaiDiGvDvi00bbVzTN119N7ZM69A:R1uejdSSUcX3HrvEbRN11z6
MD5:	C94A5671588ABB64EAB63DB753FF3DDE
SHA1:	A04FE7F0944C051D9EB60A53E321BAE5AD139912
SHA-256:	50BEE5C11D3905157AA3AA461B9DA69CC05C90D748330E98324CC36815610BC0
SHA-512:	9BC30BBD2E6C0C28223050BA939E2C89B77F4C89991FB59D101C026058563A5F3ADEE5B851173541735BADC83E419FE5F3AF81CAD2F53C36BB417BBD93E365(
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L.....`_.....@.....4...(.....0...@.....D..... .text..... ..`.data.....@....duduti.....@....xibasej.....@....kak.....@....rsrc..... .....@..@.reloc..ZF.....H.....@..B..... .....

C:\Users\user\AppData\Roaming\brgebic:Zone.Identifier	
Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\SysWOW64\cnuxfiv\mtkthtmd.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14881792

C:\Windows\SysWOW64\cnuxfiv\mtkthtmd.exe (copy)	
Entropy (8bit):	3.781178022928025
Encrypted:	false
SSDEEP:	6144:Aa1ijIN+Aee6+saxCBxHoM3sDKOd4xncb3wQ:Aag8N+Ae2sTvIM5OYncb
MD5:	6697E6F7370892D5B7251882BEDAD002
SHA1:	31F9BCE889CD859126FC323D7ABBD155FDDF41F2
SHA-256:	44E305DB99461F07B7CFF6648B50531771361A4DFAFA69991527D3963EB88DD2
SHA-512:	1D8E6A71CC886250D6191788C828B3A134C5AAF8E48786CA6E6808802BA74A2902840185690B683E4B3336FF2C0E74E142442B87CBC95A1BABC4B07C4CE94E0E
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R..R..R.....R....g.R..])..R..S...R.....R.....R.....R.Rich.R..... ..PE..L...5._..... .....@.....D...(.....0...@.....D..... text..... ..`.data.....@....nife.....@....kiza.....@....lagoti.....@....rsrc.....@..@. reloc..ZF.....x.....@..B..... .....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2145513326304425
Encrypted:	false
SSDEEP:	12288:o2/MzhXk/6YRpDb8iy/5Lf3I1P4hlzbS9uInO1mzIgtEWBTvbCMnLt:x/MzhXk/6YDDb8/6c12x
MD5:	22B88C2FDA467A47C4365A499E29E137
SHA1:	FC0C6466C2F4F44EFE181770C981B9101C546E34
SHA-256:	17DBC65F8B6FC5084855B092B2037BD16B94A7FCA6CA92A4C5D771205DC29FFA
SHA-512:	42E0F91F307C61C5FB290F3A86232B76B8F4242A27E1A56C211BD4D327288F587FDA6DBC1E176DBFA693051A5A2565C3176E31C82F2BB32DBAA795F9A239E32E
Malicious:	false
Reputation:	unknown
Preview:	regfV...V...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.QW.w..... ....\..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.4632131310057863
Encrypted:	false
SSDEEP:	384:tYR5uoIpnc8VTVgGmKAXDmnnkp3cs87W/:+P9Sc8ZVgGlAXqnnkh87W
MD5:	357B15203E7BE7E756BEF482EB0EC3C9
SHA1:	13E2AEDA79A34DC32E5A8C6EB27D8325D4ED7305
SHA-256:	A140ECD3A614C842BD0126F73EDE3677E3C9D15A3973E5B32B3F25AD71D3B10D
SHA-512:	542FAA36E972469C8930049B6D62DCF0E8BE2856D1C21092DAAA97AF36252747BD131AFA3D3A50BB790F98E45CBDA55E852FD0EB5283EBC45429E3C520F7F64 5
Malicious:	false
Reputation:	unknown
Preview:	regfU...U...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm.QW.w..... ....\.HvLE.N.....U.....J..*...U.M..J.G.....`... ..hbin.....p.\..,.....nk,..Y.w..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ..Y.w..... ....Z.....Root.....lf.....Root....nk ..Y.w.....}..... .....*.....DeviceCensus..... .vk.....WritePermissionsCheck.....p...

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3773
Entropy (8bit):	4.7109073551842435
Encrypted:	false
SSDEEP:	48:VHILZNfrI7WFY32iIiNOmV/HToZV9It199hiALlIg39bWA1RvTBi/g2eB:VoLr0y9iIiNOoHTou7bhBllydWALLt2w
MD5:	DA3247A302D70819F10BCEEBAF400503
SHA1:	2857AA198EE76C86FC929CC3388A56D5FD051844

\Device\ConDrv	
SHA-256:	5262E1EE394F329CD1F87EA31BA4A396C4A76EDC3A87612A179F81F21606ABC8
SHA-512:	48FFEC059B4E88F21C2AA4049B7D9E303C0C93D1AD771E405827149EDDF986A72EF49C0F6D8B70F5839DCDBD6B1EA8125C8B300134B7F71C47702B577AD090F
Malicious:	false
Reputation:	unknown
Preview:	..A specified value is not valid.....Usage: add rule name=<string>.. dir=in|out.. action=allow|block|bypass.. [program=<program path>].. [service=<service short name>|any].. [description=<string>].. [enable=yes|no (default=yes)].. [profile=public|private|domain|any[,...]].. [localip=any|<IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [remoteip=any|localsubnet|dns|dhcp|wins|defaultgateway|.. <IPv4 address>|<IPv6 address>|<subnet>|<range>|<list>].. [localport=0-65535|<port range>[,...]|RPC|RPC-EPMap|IPHTTPS|any (default=any)].. [remoteport=0-65535|<port range>[,...]|any (default=any)].. [protocol=0-255|icmpv4|icmpv6|icmpv4:type,code|icmpv6:type,code|.. tcp|udp|any (default=any)].. [interfacetype=wireless|lan|ras|any].. [rmtcomputergrp=<SDDL string>].. [rmtusrgrp=<SDDL string>].. [edge=yes|deferapp|deferuser|no (default=no)].. [security=authenticate|authenc|authdynenc|authnoencap|

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.693501670017806
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	urMpgNNXPM.exe
File size:	319488
MD5:	c94a5671588abb64eab63db753ff3dde
SHA1:	a04fe7f0944c051d9eb60a53e321bae5ad139912
SHA256:	50bee5c11d3905157aa3aa461b9da69cc05c90d748330e98324cc36815610bc0
SHA512:	9bc30bbd2e6c0c28223050ba939e2c89b77f4c89991fb59d101c026058563a5f3adee5b851173541735badc83e419e5f3af81cad2f53c36bb417bbd93e36502
SSDEEP:	6144:RnueuQuWjRKidSSUeE+XaiDiGvDvi00bbVzTN119N7ZM69A:R1uejdSSUcX3HrvEbRN11z6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R...R...R.....R.....g.R..])...R...S...R.....R.....R.....R.Rich..R.....PE..L....._.....

File Icon

Icon Hash:	c8d0d8e0f8f0f4e8

Static PE Info

General

Entrypoint:	0x41b510
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5FDECDE5 [Sun Dec 20 04:07:01 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	80fec6fca6f81033220e34b44810dbfd

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e5a4	0x3e600	False	0.582395259269	data	6.96770613862	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x10c988	0x1800	False	0.340006510417	data	3.47096777367	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.duduti	0x14d000	0x5	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.xibasej	0x14e000	0xea	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.kak	0x14f000	0xd93	0xe00	False	0.00697544642857	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x150000	0x83b8	0x8400	False	0.597271543561	data	5.82804585423	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x159000	0x465a	0x4800	False	0.346299913194	data	3.68706207447	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Dutch	Netherlands	
Spanish	Colombia	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:52:24.654551029 CET	192.168.2.6	8.8.8.8	0x3807	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:52:25.660358906 CET	192.168.2.6	8.8.8.8	0x3807	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:25.846137047 CET	192.168.2.6	8.8.8.8	0x4167	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.285420895 CET	192.168.2.6	8.8.8.8	0xcd33	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.452163935 CET	192.168.2.6	8.8.8.8	0xb08c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.926434994 CET	192.168.2.6	8.8.8.8	0x2d87	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:27.096297026 CET	192.168.2.6	8.8.8.8	0xa41f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:28.484508991 CET	192.168.2.6	8.8.8.8	0x8c3e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:28.666481018 CET	192.168.2.6	8.8.8.8	0x3e44	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:29.101421118 CET	192.168.2.6	8.8.8.8	0x3220	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.000447989 CET	192.168.2.6	8.8.8.8	0xfc3a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.169842958 CET	192.168.2.6	8.8.8.8	0xa955	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.337724924 CET	192.168.2.6	8.8.8.8	0xedfa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.629730940 CET	192.168.2.6	8.8.8.8	0x2c5d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.796508074 CET	192.168.2.6	8.8.8.8	0xb425	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.232522964 CET	192.168.2.6	8.8.8.8	0x9eee	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.310174942 CET	192.168.2.6	8.8.8.8	0xa872	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.789386988 CET	192.168.2.6	8.8.8.8	0x4385	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.961766005 CET	192.168.2.6	8.8.8.8	0x1fa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:33.156282902 CET	192.168.2.6	8.8.8.8	0xbf1d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:33.325922012 CET	192.168.2.6	8.8.8.8	0xab3b	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:37.588368893 CET	192.168.2.6	8.8.8.8	0x80d8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:37.760811090 CET	192.168.2.6	8.8.8.8	0x2d84	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:37.954890966 CET	192.168.2.6	8.8.8.8	0x2762	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:38.989835024 CET	192.168.2.6	8.8.8.8	0x2762	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:39.154247046 CET	192.168.2.6	8.8.8.8	0xecd2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.471626997 CET	192.168.2.6	8.8.8.8	0xe51a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.658560991 CET	192.168.2.6	8.8.8.8	0x5295	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.828239918 CET	192.168.2.6	8.8.8.8	0xb76	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.999852896 CET	192.168.2.6	8.8.8.8	0x8181	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:44.193207026 CET	192.168.2.6	8.8.8.8	0x37e1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:44.364022970 CET	192.168.2.6	8.8.8.8	0xf5df	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:44.551337957 CET	192.168.2.6	8.8.8.8	0x73d3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:56.052637100 CET	192.168.2.6	8.8.8.8	0xa281	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:58.740139961 CET	192.168.2.6	8.8.8.8	0x533c	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:05.863529921 CET	192.168.2.6	8.8.8.8	0x52a1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.038395882 CET	192.168.2.6	8.8.8.8	0x2e77	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:53:06.217262983 CET	192.168.2.6	8.8.8.8	0x8150	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.380723953 CET	192.168.2.6	8.8.8.8	0xbad	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.546901941 CET	192.168.2.6	8.8.8.8	0x6b54	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.741323948 CET	192.168.2.6	8.8.8.8	0xc108	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.910912037 CET	192.168.2.6	8.8.8.8	0xfe73	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.079888105 CET	192.168.2.6	8.8.8.8	0x3553	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.250935078 CET	192.168.2.6	8.8.8.8	0xdd4b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.421092987 CET	192.168.2.6	8.8.8.8	0x958d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.615502119 CET	192.168.2.6	8.8.8.8	0xd807	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.795175076 CET	192.168.2.6	8.8.8.8	0x1922	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:08.757597923 CET	192.168.2.6	8.8.8.8	0x1922	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:08.927258968 CET	192.168.2.6	8.8.8.8	0x8b0d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:09.099863052 CET	192.168.2.6	8.8.8.8	0xed51	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:13.541783094 CET	192.168.2.6	8.8.8.8	0x8e65	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:14.120116949 CET	192.168.2.6	8.8.8.8	0x137d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:14.347100973 CET	192.168.2.6	8.8.8.8	0x9750	Standard query (0)	goo.su	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:15.028245926 CET	192.168.2.6	8.8.8.8	0xceed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:15.591371059 CET	192.168.2.6	8.8.8.8	0x89ee	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:15.925843954 CET	192.168.2.6	8.8.8.8	0xcd43	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.096606016 CET	192.168.2.6	8.8.8.8	0x492b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.263859987 CET	192.168.2.6	8.8.8.8	0xd47f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.439399004 CET	192.168.2.6	8.8.8.8	0x59f4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.645344973 CET	192.168.2.6	8.8.8.8	0xefd5	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.135286093 CET	192.168.2.6	8.8.8.8	0x72d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.304049015 CET	192.168.2.6	8.8.8.8	0x1397	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.478251934 CET	192.168.2.6	8.8.8.8	0xca63	Standard query (0)	a0621298.xsph.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.824640989 CET	192.168.2.6	8.8.8.8	0xa0bc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.988061905 CET	192.168.2.6	8.8.8.8	0x6587	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:25.199408054 CET	192.168.2.6	8.8.8.8	0x8a89	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:32.048135996 CET	192.168.2.6	8.8.8.8	0xbe2a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:32.892185926 CET	192.168.2.6	8.8.8.8	0xd078	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:33.118439913 CET	192.168.2.6	8.8.8.8	0x2ff3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:33.325548887 CET	192.168.2.6	8.8.8.8	0x500e	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:39.001521111 CET	192.168.2.6	8.8.8.8	0xc9b8	Standard query (0)	patmushta.info	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:40.591614008 CET	192.168.2.6	8.8.8.8	0x5df	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:40.757642031 CET	192.168.2.6	8.8.8.8	0x2c6d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:41.241261959 CET	192.168.2.6	8.8.8.8	0x6d42	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:53:42.873996019 CET	192.168.2.6	8.8.8.8	0x5d38	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:43.043747902 CET	192.168.2.6	8.8.8.8	0x5443	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:43.207545042 CET	192.168.2.6	8.8.8.8	0x1679	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:45.097480059 CET	192.168.2.6	8.8.8.8	0x1fb6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:45.394380093 CET	192.168.2.6	8.8.8.8	0xa06d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:45.922348976 CET	192.168.2.6	8.8.8.8	0x312f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:46.105789900 CET	192.168.2.6	8.8.8.8	0x6eb7	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:46.280946016 CET	192.168.2.6	8.8.8.8	0x358b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:46.456178904 CET	192.168.2.6	8.8.8.8	0xbe6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.358208895 CET	192.168.2.6	8.8.8.8	0x5ad3	Standard query (0)	microsoft-com.mail.protection.outlook.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:52:25.677303076 CET	8.8.8.8	192.168.2.6	0x3807	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:25.976010084 CET	8.8.8.8	192.168.2.6	0x3807	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.134783030 CET	8.8.8.8	192.168.2.6	0x4167	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.302778959 CET	8.8.8.8	192.168.2.6	0xcd33	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.764352083 CET	8.8.8.8	192.168.2.6	0xb08c	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:26.943152905 CET	8.8.8.8	192.168.2.6	0x2d87	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:27.115442038 CET	8.8.8.8	192.168.2.6	0xa41f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:28.502018929 CET	8.8.8.8	192.168.2.6	0x8c3e	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:28.952187061 CET	8.8.8.8	192.168.2.6	0x3e44	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:29.417875051 CET	8.8.8.8	192.168.2.6	0x3220	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.018002033 CET	8.8.8.8	192.168.2.6	0xfc3a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.186986923 CET	8.8.8.8	192.168.2.6	0xa955	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.356897116 CET	8.8.8.8	192.168.2.6	0xedfa	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:31.648720980 CET	8.8.8.8	192.168.2.6	0x2c5d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.083039999 CET	8.8.8.8	192.168.2.6	0xb425	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.253036022 CET	8.8.8.8	192.168.2.6	0x9eee	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.634856939 CET	8.8.8.8	192.168.2.6	0xa872	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:52:32.808607101 CET	8.8.8.8	192.168.2.6	0x4385	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:32.979103088 CET	8.8.8.8	192.168.2.6	0x1fa	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:33.175611019 CET	8.8.8.8	192.168.2.6	0xbf1d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:33.613033056 CET	8.8.8.8	192.168.2.6	0xab3b	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:37.606149912 CET	8.8.8.8	192.168.2.6	0x80d8	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:37.780322075 CET	8.8.8.8	192.168.2.6	0x2d84	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:39.009100914 CET	8.8.8.8	192.168.2.6	0x2762	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:39.173664093 CET	8.8.8.8	192.168.2.6	0xecd2	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:39.289155960 CET	8.8.8.8	192.168.2.6	0x2762	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.490735054 CET	8.8.8.8	192.168.2.6	0xe51a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.677912951 CET	8.8.8.8	192.168.2.6	0x5295	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:41.847886086 CET	8.8.8.8	192.168.2.6	0xb76	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:42.022020102 CET	8.8.8.8	192.168.2.6	0x8181	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:42.022020102 CET	8.8.8.8	192.168.2.6	0x8181	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:42.022020102 CET	8.8.8.8	192.168.2.6	0x8181	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:42.022020102 CET	8.8.8.8	192.168.2.6	0x8181	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:42.022020102 CET	8.8.8.8	192.168.2.6	0x8181	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:44.210670948 CET	8.8.8.8	192.168.2.6	0x37e1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:44.383157969 CET	8.8.8.8	192.168.2.6	0xf5df	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:44.570828915 CET	8.8.8.8	192.168.2.6	0x73d3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:56.081125021 CET	8.8.8.8	192.168.2.6	0xa281	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:56.081125021 CET	8.8.8.8	192.168.2.6	0xa281	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:56.081125021 CET	8.8.8.8	192.168.2.6	0xa281	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:56.081125021 CET	8.8.8.8	192.168.2.6	0xa281	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:52:56.081125021 CET	8.8.8.8	192.168.2.6	0xa281	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:56.081125021 CET	8.8.8.8	192.168.2.6	0xa281	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:52:58.759690046 CET	8.8.8.8	192.168.2.6	0x533c	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:05.883285046 CET	8.8.8.8	192.168.2.6	0x52a1	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.057931900 CET	8.8.8.8	192.168.2.6	0x2e77	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.234260082 CET	8.8.8.8	192.168.2.6	0x8150	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.398336887 CET	8.8.8.8	192.168.2.6	0xbad	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.566031933 CET	8.8.8.8	192.168.2.6	0x6b54	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.760056019 CET	8.8.8.8	192.168.2.6	0xc108	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:06.927711010 CET	8.8.8.8	192.168.2.6	0xfe73	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.099093914 CET	8.8.8.8	192.168.2.6	0x3553	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.267967939 CET	8.8.8.8	192.168.2.6	0xdd4b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.439812899 CET	8.8.8.8	192.168.2.6	0x958d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:07.634640932 CET	8.8.8.8	192.168.2.6	0xd807	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:08.774995089 CET	8.8.8.8	192.168.2.6	0x1922	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:08.944542885 CET	8.8.8.8	192.168.2.6	0x8b0d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:09.108695030 CET	8.8.8.8	192.168.2.6	0x1922	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:09.119329929 CET	8.8.8.8	192.168.2.6	0xed51	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:13.561172962 CET	8.8.8.8	192.168.2.6	0x8e65	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:14.137269020 CET	8.8.8.8	192.168.2.6	0x137d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:14.374198914 CET	8.8.8.8	192.168.2.6	0x9750	No error (0)	goo.su		104.21.38.221	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:14.374198914 CET	8.8.8.8	192.168.2.6	0x9750	No error (0)	goo.su		172.67.139.105	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:15.350929022 CET	8.8.8.8	192.168.2.6	0xceed	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:15.610816956 CET	8.8.8.8	192.168.2.6	0x89ee	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:15.944710016 CET	8.8.8.8	192.168.2.6	0xcd43	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:53:16.116038084 CET	8.8.8.8	192.168.2.6	0x492b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.282999992 CET	8.8.8.8	192.168.2.6	0xd47f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.457016945 CET	8.8.8.8	192.168.2.6	0x59f4	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:16.985060930 CET	8.8.8.8	192.168.2.6	0xefd5	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.152723074 CET	8.8.8.8	192.168.2.6	0x72d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.323434114 CET	8.8.8.8	192.168.2.6	0x1397	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.497729063 CET	8.8.8.8	192.168.2.6	0xca63	No error (0)	a0621298.xsph.ru		141.8.194.74	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:24.842113018 CET	8.8.8.8	192.168.2.6	0xa0bc	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:25.007565022 CET	8.8.8.8	192.168.2.6	0x6587	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:25.218637943 CET	8.8.8.8	192.168.2.6	0x8a89	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:32.065937996 CET	8.8.8.8	192.168.2.6	0xbe2a	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:32.912306070 CET	8.8.8.8	192.168.2.6	0xd078	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:33.138006926 CET	8.8.8.8	192.168.2.6	0x2ff3	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:33.344937086 CET	8.8.8.8	192.168.2.6	0x500e	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:39.020761013 CET	8.8.8.8	192.168.2.6	0xc9b8	No error (0)	patmushta.info		94.142.143.116	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:40.610492945 CET	8.8.8.8	192.168.2.6	0x5df	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:41.090313911 CET	8.8.8.8	192.168.2.6	0x2c6d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:41.258994102 CET	8.8.8.8	192.168.2.6	0x6d42	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:42.893403053 CET	8.8.8.8	192.168.2.6	0x5d38	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:43.061167955 CET	8.8.8.8	192.168.2.6	0x5443	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:43.546730042 CET	8.8.8.8	192.168.2.6	0x1679	No error (0)	data-host-coin-8.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:45.114891052 CET	8.8.8.8	192.168.2.6	0x1fb6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:45.413424969 CET	8.8.8.8	192.168.2.6	0xa06d	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:45.941740990 CET	8.8.8.8	192.168.2.6	0x312f	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:46.122853994 CET	8.8.8.8	192.168.2.6	0x6eb7	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:46.298351049 CET	8.8.8.8	192.168.2.6	0x358b	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:53:46.473037004 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	host-data-coin-11.com		8.209.70.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.387037992 CET	8.8.8.8	192.168.2.6	0x5ad3	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.387037992 CET	8.8.8.8	192.168.2.6	0x5ad3	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.212.0	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.387037992 CET	8.8.8.8	192.168.2.6	0x5ad3	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.54.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.387037992 CET	8.8.8.8	192.168.2.6	0x5ad3	No error (0)	microsoft-com.mail.protection.outlook.com		104.47.53.36	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.387037992 CET	8.8.8.8	192.168.2.6	0x5ad3	No error (0)	microsoft-com.mail.protection.outlook.com		40.93.207.1	A (IP address)	IN (0x0001)
Jan 14, 2022 10:53:53.387037992 CET	8.8.8.8	192.168.2.6	0x5ad3	No error (0)	microsoft-com.mail.protection.outlook.com		52.101.24.0	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- weljlc.org
  - host-data-coin-11.com
- hayrfyccj.com
- tuycuvbg.net
- ekawsccbq.com
- kcwcrh.net
- bpvodqrew.org
- asarkm.com
- mnllv.com
- data-host-coin-8.com
- ogofho.net
- dbjbh.com
- ppffsgvja.org
- hrsrlyx.org
- kshsgpunb.net
- unicupload.top
- xsprn.net
- uurfua.org
- rlqbx.com

- dgjupwntau.net
- mysywrslju.net
- xwiyqrp.org
- jinpxtqfj.com
- uamdn.com
- 185.7.214.171:8080
- vxqucx.net
- yfxxxhhksn.net
- jamcbie.org
- htnsmvsyss.net
- ohcatqdd.com
- xowgyo.net
- lpclestri.org
- jsgvixvqr.org
- lxxgnl.org
- llxelhpa.net
- qqrjksik.net
- enomb.org
- snmxoegc.org
- nprtbw.net
- tqxibbs.net
- ipsxcompsh.com
- sfylh.com
- toutoxfm.org
- wdjgwmxxgn.com
- erbieb.net
- crbui.com
- aygvaoanp.org
- sfqstuigh.org
- fohwktm.net

- gdqyg.com
- fultemtcsj.com
- qnkvoprwpm.net
- qyltp.com
- a0621298.xsph.ru
- fcfaulckr.net
- girilqetk.com
- 185.163.204.22
- 185.163.204.24
- ogsob.net
- swynuffv.org
- syexhpbb.com
- 185.215.113.35
- lhqpichr.net
- fdehu.net
- hugscb.org
- mhokygbj.com
- vvtjauw.net
- xyvsvse.org
- bslbgffclk.org
- cpibq.com
- hbtes.com
- jwqhpinwbm.com

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: urMpgNNXPM.exe PID: 7052 Parent PID: 5340

General

Start time:	10:51:41
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\urMpgNNXPM.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\urMpgNNXPM.exe"
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	C94A5671588ABB64EAB63DB753FF3DDE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: urMpgNNXPM.exe PID: 7120 Parent PID: 7052

General

Start time:	10:51:43
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\urMpgNNXPM.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\urMpgNNXPM.exe"
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	C94A5671588ABB64EAB63DB753FF3DDE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.407856003.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.407888776.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3440 Parent PID: 7120

General

Start time:	10:51:50
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000005.00000000.392146415.0000000002E31000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 4708 Parent PID: 560

General

Start time:	10:51:50
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3640 Parent PID: 560

General

Start time:	10:52:08
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 5620 Parent PID: 560

General

Start time:	10:52:24
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: brgebic PID: 5636 Parent PID: 936

General

Start time:	10:52:25
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\brgebic
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\brgebic
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	C94A5671588ABB64EAB63DB753FF3DDE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: brgebic PID: 6596 Parent PID: 5636

General

Start time:	10:52:27
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\brgebic
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\brgebic
Imagebase:	0x400000
File size:	319488 bytes
MD5 hash:	C94A5671588ABB64EAB63DB753FF3DDE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.459976464.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.459947812.0000000000680000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: 7CF6.exe PID: 6592 Parent PID: 3440

General

Start time:	10:52:29
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\7CF6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\7CF6.exe
Imagebase:	0x7ff6b7590000
File size:	301056 bytes
MD5 hash:	277680BD3182EB0940BC356FF4712BEF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	moderate

Analysis Process: svchost.exe PID: 6848 Parent PID: 560

General

Start time:	10:52:32
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 6908 Parent PID: 6848

General

Start time:	10:52:33
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 488 -p 6592 -ip 6592
Imagebase:	0xb80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 8D62.exe PID: 6784 Parent PID: 3440

General

Start time:	10:52:34

Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8D62.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8D62.exe
Imagebase:	0x400000
File size:	323072 bytes
MD5 hash:	69D8C52799339ABA9407830AB8AA210B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.463738974.0000000000792000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000011.00000002.463738974.0000000000792000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: 5900 Parent PID: 6592

General

Start time:	10:52:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6592 -s 520
Imagebase:	0xb80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: F9FC.exe PID: 6248 Parent PID: 3440

General

Start time:	10:52:39
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\F9FC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F9FC.exe
Imagebase:	0x400000

File size:	320512 bytes
MD5 hash:	8B25D9317E18654C3F83EF8630D1DE16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000014.00000002.490147726.0000000000630000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000014.00000002.489718106.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000014.00000003.470461720.0000000000660000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: 4BB.exe PID: 5128 Parent PID: 3440

General

Start time:	10:52:42
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\4BB.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\4BB.exe
Imagebase:	0xcd0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000015.00000002.527776189.00000000040B1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 4624 Parent PID: 6248

General

Start time:	10:52:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\System32\cmd.exe" /C mkdir C:\Windows\SysWOW64\cnuxfiv\
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 4756 Parent PID: 4624

General

Start time:	10:52:44
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 3576 Parent PID: 6248

General

Start time:	10:52:45
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\mtkthtmd.exe" C:\Windows\SysWOW64\cnuxfiv\
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 6716 Parent PID: 3576

General

Start time:	10:52:45
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6684 Parent PID: 560

General

Start time:	10:52:46
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff65d2f0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: sc.exe PID: 6068 Parent PID: 6248

General

Start time:	10:52:46
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" create cnuxfiv binPath= "C:\Windows\SysWOW64\cnuxfiv \mtkthtmd.exe /d\"C:\Users\user\AppData\Local\Temp\F9FC.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x40000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4216 Parent PID: 6068

General

Start time:	10:52:47
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5400 Parent PID: 6248

General

Start time:	10:52:47
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\sc.exe" description cnuxfiv "wifi internet conection
Imagebase:	0x40000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4272 Parent PID: 5400

General

Start time:	10:52:48
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 660 Parent PID: 6248

General

Start time:	10:52:48
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\sc.exe" start cnuxfiv
Imagebase:	0x40000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4860 Parent PID: 660

General

Start time:	10:52:49
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 5356 Parent PID: 6248

General

Start time:	10:52:50
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\netsh.exe" advfirewall firewall add rule name="Host-process for services of Windows" dir=in action=allow program="C:\Windows\SysWOW64\svchost.exe" enable=yes>nul
Imagebase:	0x9e0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mtkthtmd.exe PID: 528 Parent PID: 560

General

Start time:	10:52:50
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cnuxfiv\mtkthtmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cnuxfiv\mtkthtmd.exe /d"C:\Users\user\AppData\Local\Temp\F9FC.exe"
Imagebase:	0x400000
File size:	14881792 bytes
MD5 hash:	6697E6F7370892D5B7251882BEDAD002
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000025.00000002.499632659.0000000000630000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000025.00000002.498726518.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000025.00000002.499963513.0000000000740000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000025.00000003.492214272.0000000000650000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 400 Parent PID: 5356

General

Start time:	10:52:50
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5920 Parent PID: 528

General

Start time:	10:52:52
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	svchost.exe
Imagebase:	0x360000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 00000027.00000002.628334605.0000000002E90000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: 4BB.exe PID: 6040 Parent PID: 5128

General

Start time:	10:52:58
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\4BB.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\4BB.exe
Imagebase:	0xea0000
File size:	537088 bytes
MD5 hash:	D7DF01D8158BFADDC8BA48390E52F355
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000002.622166424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.517460505.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.519326789.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.518322210.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000028.00000000.520547153.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6732 Parent PID: 560

General

Start time:	10:53:02
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 6DF6.exe PID: 6548 Parent PID: 3440

General

Start time:	10:53:09
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\6DF6.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6DF6.exe
Imagebase:	0x400000
File size:	905216 bytes
MD5 hash:	852D86F5BC34BF4AF7FA89C60569DF13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000002A.00000002.638483235.0000000004D10000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000002A.00000003.556642390.0000000004DC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 0000002A.00000002.625128489.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: 8DA4.exe PID: 7060 Parent PID: 3440

General

Start time:	10:53:19
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8DA4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8DA4.exe
Imagebase:	0x400000
File size:	373760 bytes
MD5 hash:	8B239554FE346656C8EEF9484CE8092F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000002D.00000002.580424216.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000002D.00000003.562920676.00000000006F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000002D.00000002.580758343.00000000006B0000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: B169.exe PID: 1684 Parent PID: 3440

General

Start time:	10:53:27
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\B169.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B169.exe
Imagebase:	0x400000
File size:	3576320 bytes
MD5 hash:	5800952B83AECEFC3AA06CCB5B29A4C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002E.00000002.589443609.00000000000C2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000002E.00000003.588752731.0000000003702000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis