ID: 791287
Sample Name: file.exe
Cookbook: default.jbs
Time: 09:26:11
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

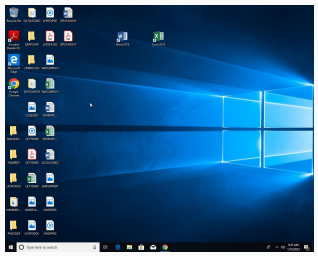
Windows Analysis Report

file.exe

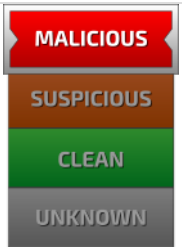
Overview

General Information

Sample Name:	file.exe
Analysis ID:	791287
MD5:	6def34b7d9603c..
SHA1:	82d464aedae69e.
SHA256:	277e1518b90973.
Tags:	exe
Infos:	



Detection



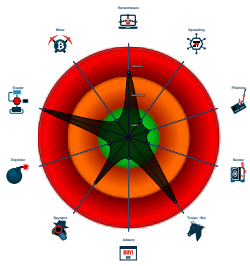
Djvu, RHADAMANTHYS, RedLine, SmokeLoader

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

Signatures

- Yara detected RedLine Stealer
- Detected unpacking (overwrites its o…
- Yara detected AntiVM3
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Yara detected RHADAMANTHYS S…
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware
- Multi AV Scanner detection for dom…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 1032 cmdline: C:\Users\user\Desktop\file.exe MD5: 6DEF34B7D9603C4FC7953F177F73C21A)
  - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - C676.exe (PID: 4620 cmdline: C:\Users\user\AppData\Local\Temp\C676.exe MD5: 261B1DB94CCF4266128E2EB71A80FDA4)
    - 43D0.exe (PID: 1332 cmdline: C:\Users\user\AppData\Local\Temp\43D0.exe MD5: 0A006808F7AA017CAF2DF9CE9E2B55A2)
      - 43D0.exe (PID: 3900 cmdline: C:\Users\user\AppData\Local\Temp\43D0.exe MD5: 0A006808F7AA017CAF2DF9CE9E2B55A2)
    - C4AA.exe (PID: 4116 cmdline: C:\Users\user\AppData\Local\Temp\C4AA.exe MD5: EA25CE2F3580AF1DD771BAC5B0D2BF83)
      - ngentask.exe (PID: 400 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe MD5: ED7F195F7121781CC3D380942765B57D)
      - ngentask.exe (PID: 4292 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe MD5: ED7F195F7121781CC3D380942765B57D)
      - fontview.exe (PID: 4772 cmdline: C:\Windows\SYSWOW64\fontview.exe MD5: 218D53564FB0DD0CAFBBF871641E70F7)
- beirutt (PID: 2236 cmdline: C:\Users\user\AppData\Roaming\beirutt MD5: 6DEF34B7D9603C4FC7953F177F73C21A)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://uaery.top/dl/build2.exe",
    "http://drampik.com/files/1/build3.exe"
  ],
  "C2 url": "http://drampik.com/lancer/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-cud8EGMtyB\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@freshmail.top\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0637JOsie",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
```

```
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu01T||/gszGuz7iKnpiRXv||||nGwWvl||/ZhD6D24AJOT+SbHfvz6LGasPMGyfXmLe6Fo7e0cUtl3OwZeuwDkg4lB4eE||||nFp6tv8RPx3NAGJjylTPy7ZhLTxEuSD
0YIP62Rs6Cek+fvfFS3PxiGJhQuIxfvAVe||||nsFSNJ1+fNU92+JI5SRY0ZJdMezrQYJC7YY0onlwpLsiPbN5Osc6Jw2oabAVAS6rn||||nwQkW0GgIFh9e9trQc9Rdc5bf9X3s95J0jKg0TaTVFdw6RECS2cvRD1tZwc196EJ1||||n
c5nBmBlLFWZqwkzVp4AORRnGGqz||/OUTXiUmgNX+umpwUvdthK+7o1zc87nS20aU+||||nowIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Threatname: RedLine

```
{
  "C2 url": [
    "89.208.103.88:37538"
  ],
  "Bot Id": "birj proliv",
  "Authorization Header": "9941068ef2768ed5ba54fc3eed22d795"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://bulimu55t.net/",
    "http://soryytlic4.net/",
    "http://bukubuka1.net/",
    "http://novanosa5org.org/",
    "http://hujukui3.net/",
    "http://newzelannd66.org/",
    "http://golilopaster.org/"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.397037744.00000000005F1000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000000.00000002.397037744.00000000005F1000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x3d4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000000.00000002.397025095.00000000005D0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000000.00000002.397025095.00000000005D0000.00000004.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x7d4:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
00000008.00000002.478433039.00000000048E8000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B

Click to see the 27 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.3.C4AA.exe.df30000.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
9.3.C4AA.exe.df30000.1.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a468:$pat14: , CommandLine: • 0x134a1:$v2_1: ListOfProcesses • 0x13280:$v4_3: base64str • 0x13e03:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12813:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
9.3.C4AA.exe.df30000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
9.3.C4AA.exe.df30000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a468:$pat14: , CommandLine: • 0x134a1:$v2_1: ListOfProcesses • 0x13280:$v4_3: base64str • 0x13e03:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12813:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
9.2.C4AA.exe.12a0ed0.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 23 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands

Yara detected Djvu Ransomware

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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

Yara detected AntiVM3

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

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

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging

Hides threads from debuggers

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

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected RHADAMANTHYS Stealer

Remote Access Functionality

Yara detected RedLine Stealer

Yara detected SmokeLoader

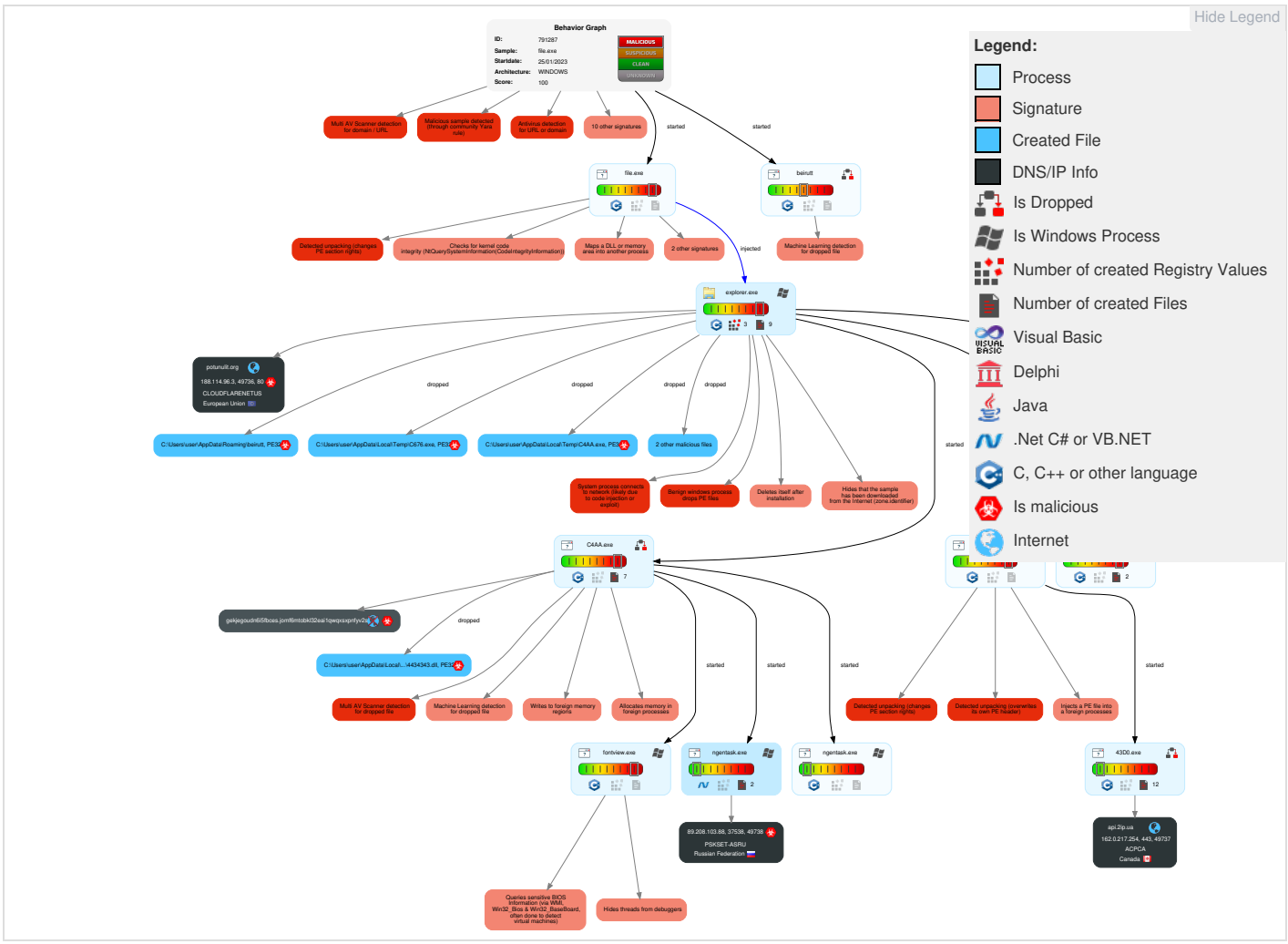
Yara detected RHADAMANTHYS Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Native API	Boot or Logon Initialization Scripts	6 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	3 1 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	2 2 Software Packing	NTDS	1 4 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	5 5 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	2 5 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Masquerading	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 5 Virtualization/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	6 1 2 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

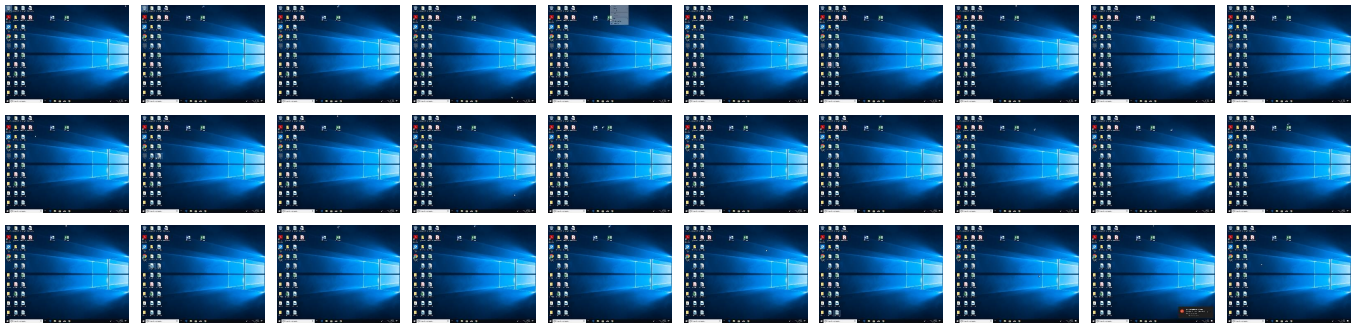
Behavior Graph



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
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\beirutt	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4434343.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C676.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C4AA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\43D0.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\43D0.exe	67%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Local\Temp\4434343.dll	18%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\C4AA.exe	43%	ReversingLabs	Win32.Spyware.RedLine	
C:\Users\user\AppData\Local\Temp\C676.exe	81%	ReversingLabs	Win32.Trojan.RedLine	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.3.C4AA.exe.df30000.1.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
6.2.C676.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1213203		Download File
9.3.C4AA.exe.df30000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
9.2.C4AA.exe.2d80000.2.unpack	100%	Avira	HEUR/AGEN.1228718		Download File
0.2.file.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.file.exe.5c0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.ngentask.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
10.2.43D0.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
0.3.file.exe.5d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
potunulit.org	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://potunulit.org/	0%	URL Reputation	safe	
http://potunulit.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Responsel	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Responsel	0%	URL Reputation	safe	
http://novanosa5org.org/	0%	URL Reputation	safe	
http://novanosa5org.org/	0%	URL Reputation	safe	
http://golilopaster.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14Responsel	0%	URL Reputation	safe	
http://bulimu55t.net/	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id3Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://ryjphgb.com/pace	0%	Avira URL Cloud	safe	
http://fedface.com/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id18Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Responsel	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Responsel	0%	URL Reputation	safe	
http://ryjphgb.com/	0%	Avira URL Cloud	safe	
http://potunulit.org:80/N	100%	Avira URL Cloud	malware	
http://potunulit.org/J2v-m	100%	Avira URL Cloud	malware	
http://109.206.243.168/upload/libcurl.dllw	0%	Avira URL Cloud	safe	
http://fedface.com/	0%	Virustotal		Browse
http://aygtqn.org/tem/W	0%	Avira URL Cloud	safe	
http://drampik.com/lancer/get.php	100%	Avira URL Cloud	malware	
http://egqgnqk.org/	0%	Avira URL Cloud	safe	
http://egqgnqk.org/s	0%	Avira URL Cloud	safe	
89.208.103.88:37538	0%	Avira URL Cloud	safe	
http://109.206.243.168/upload/libcurl.dll	0%	Avira URL Cloud	safe	
http://potunulit.org/s	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
potunulit.org	188.114.96.3	true	true	• 11%, Virustotal, Browse	unknown
api.2ip.ua	162.0.217.254	true	false		high
gekjegoudn6i5fbces.jomf6mtobkl32eai1qwqxsxpnfyv2s	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://potunulit.org/	true	• URL Reputation: safe • URL Reputation: safe	unknown
http://novanosa5org.org/	true	• URL Reputation: safe • URL Reputation: safe	unknown
http://golilopaster.org/	true	• URL Reputation: safe	unknown
http://bulimu55t.net/	true	• URL Reputation: safe	unknown
http://drampik.com/lancer/get.php	true	• Avira URL Cloud: malware	unknown
89.208.103.88:37538	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://ryjphgb.com/pace	explorer.exe, 00000003.00000003.45062747 8.00000000085C0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultP	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Responsel	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 0000000C.00000002.581410374.00000000033E6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedface.com/	explorer.exe, 00000003.00000003.450627478.00000000085C0000.00000004.00000001.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://potunulit.org/J2v-m	explorer.exe, 00000003.00000003.453675949.0000000008575000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id5	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Responsel	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id7Responsel	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

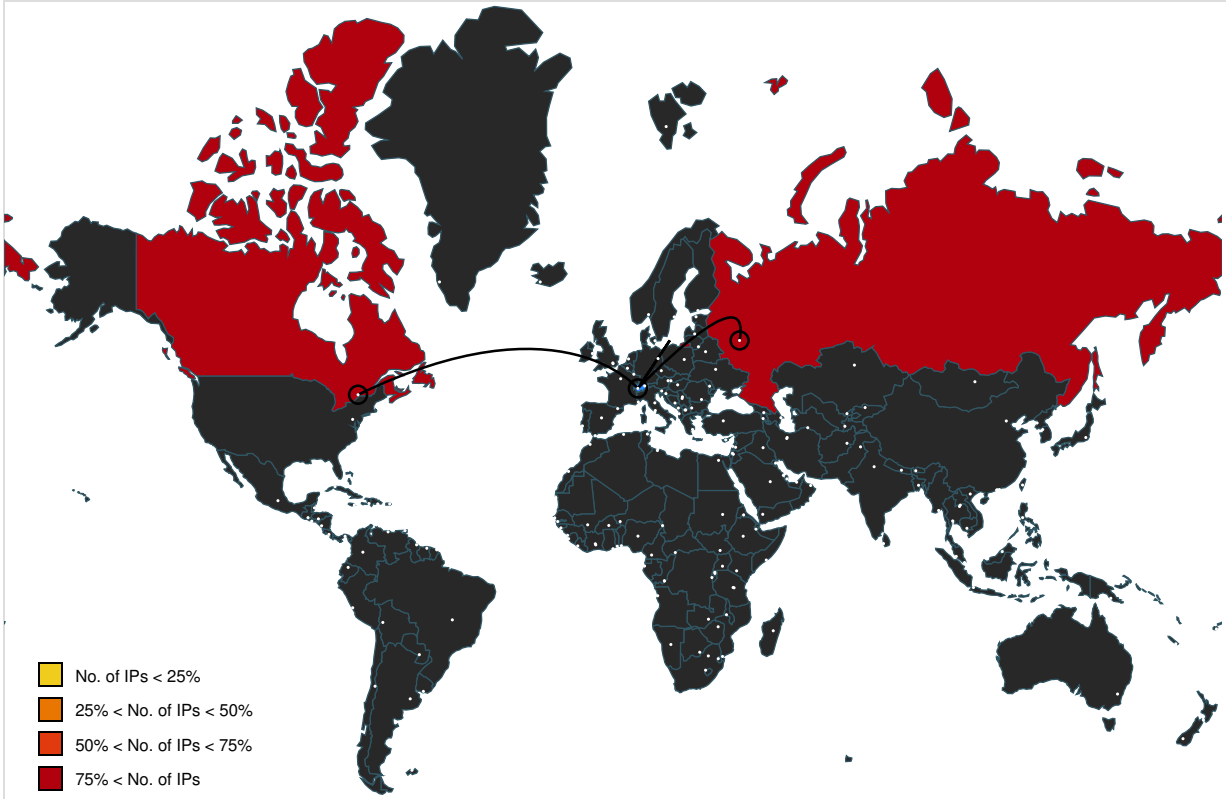
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response1	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id14Response1	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ip.sb/ip	C4AA.exe, 00000009.00000003.485078968.00 0000000DF30000.00000004.00001000.0002000 0.00000000.sdmp, C4AA.exe, 00000009.0000 0003.490022034.000000000DF32000.00000040 .00001000.00020000.00000000.sdmp, C4AA.exe, 00000009.00000002.573780441.00000000 0128B000.00000004.00000020.00020000.0000 0000.sdmp, ngentask.exe, 0000000C.000000 02.572420134.0000000000402000.00000040.0 0000400.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://109.206.243.168/upload/libcurl.dllw	fontview.exe, 0000000D.00000002.57304207 9.0000000000D8C000.00000004.00000010.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/Entity/Id8Response1	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://ryjphgb.com/	explorer.exe, 00000003.00000003.45062747 8.00000000085C0000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 00C.00000002.581410374.00000000033E6000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://potunulit.org:80/N	explorer.exe, 00000003.00000003.45066972 7.000000000CDE5000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id5Responsel	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Responsel	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://aygtqn.org/tem/W	explorer.exe, 00000003.00000003.45317666 0.000000000D15B000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.451453934.000000000D15B000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.450122194.000000 000D15B000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.449095692.000000000D15B000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.454953179.000000000D16F0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://egqgnqk.org/	explorer.exe, 00000003.00000003.45317666 0.000000000D15B000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.451453934.000000000D15B000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.450122194.000000 000D15B000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.449095692.000000000D15B000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.454953179.000000000D16F0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id3Responsel	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id12	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://egqgnqk.org/s	explorer.exe, 00000003.00000003.45317666 0.000000000D15B000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000003.451453934.000000000D15B000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.450122194.000000 000D15B000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000003.0000 0003.449095692.000000000D15B000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000003.454953179.000000000D16F0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoor dinationContextResponse	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Can cel	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id17Responsel	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id18Responsel	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://109.206.243.168/upload/libcurl.dll	fontview.exe, 0000000D.00000002.57304207 9.0000000000D8C000.00000004.00000010.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token- profile-1.1#SAMLV2.0	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token- profile-1.0#SAMLAssertionID	ngentask.exe, 0000000C.00000002.58141037 4.00000000033EA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://potunulit.org/s	explorer.exe, 00000003.00000003.45367594 9.0000000008575000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id21Responsel	ngentask.exe, 0000000C.00000002.58141037 4.00000000032F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	ngentask.exe, 0000000C.00000002.581410374.00000000033EA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	ngentask.exe, 0000000C.00000002.581410374.00000000033E6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response1	ngentask.exe, 0000000C.00000002.581410374.00000000032F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.114.96.3	potunulit.org	European Union	?	13335	CLOUDFLARENETUS	true
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
89.208.103.88	unknown	Russian Federation		42569	PSKSET-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791287
Start date and time:	2023-01-25 09:26:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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.rans.troj.evad.winEXE@17/6@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 83% (good quality ratio 75.2%) • Quality average: 69.9% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): login.live.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:28:00	API Interceptor	526x Sleep call for process: explorer.exe modified
09:28:11	Task Scheduler	Run new task: Firefox Default Browser Agent FC7EB6D179CBBFEC path: C:\Users\user\AppData\Roaming\beirutt
09:29:16	Task Scheduler	Run new task: svcupdater path: C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\43D0.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	718848
Entropy (8bit):	7.8663391957867645
Encrypted:	false
SSDEEP:	12288:XQc1wGGrXn8rDAG7ps+O6TuFlgfIEKK9LcFXTASviKWBNbaPSFS:XTwGGrsASprtEKK9wF0SrWBQKFS
MD5:	0A006808F7AA017CAF2DF9CE9E2B55A2
SHA1:	63F5B0E9FE5E3DAEBDBFC8AA168AB163E436AC32
SHA-256:	F55976607594D241004245F084ADD64F399F7D4683C603F56EF92C0CBCD41E05
SHA-512:	8AD4C111BF0904EB739A462E274C7A2FD9EC1AFB2DB7D77F176B26438520C4859B2CCB46A4C76F206E20B4584E434E1D78B26DCD042F08B3D573BB99036E8C3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..Y.pl..pl..pl.."...pl.."..rpl.(....pl..pm..pl.."...pl.."...pl.."...pl.Rich.pl... .....PE..L.....a.....Z.....6x.....@.....,...d....p..P,.....P.....Z..@..... .....text..... ..`.data.....4.....@....rsrc...P,...p.....@..@..... ....

C:\Users\user\AppData\Local\Temp\4434343.dll

Process:	C:\Users\user\AppData\Local\Temp\C4AA.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	343040
Entropy (8bit):	7.533406928573143
Encrypted:	false
SSDEEP:	6144:324+ZV6NuvwV+hq3kd2UaXYnKUFWBMljuhLaWdTPk8SarppXad:YuNuvwUhq3kd2USYKUQ6ljkLaWdTPk8q
MD5:	F56B1B3FE0C50C6ED0FAD54627DF7A9A
SHA1:	05742C9AD28475C7AFDD3D6A63DD9200FC0B9F72
SHA-256:	E8F71DA41BBC272EF84589A7575B13B8B5D6D5D01796B3AF033682657263C53B
SHA-512:	FDE2089BCDF19CDB9D27763E4D3294A0E42CD0A3132463636610D85C3903B885BE6142D3B42204E89B76B5595E8B132580C8A5C60CED96D042AD96BCFE29B19
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...r..c.....!.....\|.....@..... .....s.....<.....`.....d...$.....text..... ..`.rdata...[.....\.....@..@.data...x....0..... .....@....00cfg.....P.....&.....@..@.reloc.....`.....(.....@..B..... ....

C:\Users\user\AppData\Local\Temp\C4AA.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	1642648
Entropy (8bit):	7.847643854402106
Encrypted:	false
SSDEEP:	49152:murDawItlpDZLPU/kHWGPaYE3Ku7ZKZ6nxvax85fCSuw:muPawItlpDZDU/kZPaYm/JvaxQCK
MD5:	EA25CE2F3580AF1DD771BAC5B0D2BF83
SHA1:	8A425695AE3154F222BA4A7A8AF03287D20F8BC4
SHA-256:	768E12A9AF62F5F83F6D6FF64C6C10E37834FC202E0E4D609C80CE7FACC8C534
SHA-512:	70776BD050666D7ABCDB0668832A652FC4A67E45243DFD229520DA3712B85B506FFE9C3ED3C3C1E89F388C2D56B6E3FC8CDC31B35485FF1BA456F8A47277F04

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.b...b...b...0>..b...0/..b...09..b.....b...b...b...00..b...0...b...b-..b...0 +..b..Rich.b.....PE..L....~.c.....#.....k.....@.....9....2[....@.....P.....6.0.....9..... ..@.....`.....text...6..... ..`.rdata...0.....2.....@..@.data...<. .....@....rsrc...0.....6.....@..@.reloc...I....9..J..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\C676.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	417792
Entropy (8bit):	7.008431460440525
Encrypted:	false
SSDEEP:	6144:GILot0e73kNAn1SNCe64axZb30GvtQK/fu1d04DI12mTb:GIct0eLkPNL64Y91tQKXu1PDI12
MD5:	261B1DB94CCF4266128E2EB71A80FDA4
SHA1:	9D4CD03297F31EABE957F261DC7C3C6C268BD39F
SHA-256:	B0072463E78182E8D9721F91F889A62D9CE59A348FDDC5196B6201A5FA68B259
SHA-512:	2DD25970561CF9E3D946ACD891B601E6AA7E6563DDE6C10ED5AC1A6486BBC1851CF3908B5BDEE6C9B29633E51C90339209C50D97C0EA28B897BD6E7117B1A 7B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M_.`.>.3.>.3.>.3.IQ3->.3.I@3.>.3.IV3o>.3...3.>.3.>.3~>.3.I_3.> .3.IA3.>.3.ID3.>.3Rich.>.3.....PE..L.....b.....F.....@.....T...d.... ..(.....- ..@.....text...8..... ..`.data.....@....huxuho.p.....@..@.gini.....@..@.vab..... .....@....rsrc...(.... .....@..@.reloc.....F.....@..B..... .....

C:\Users\user\AppData\Roaming\beirutt

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	344064
Entropy (8bit):	6.5486278322749145
Encrypted:	false
SSDEEP:	6144:OnCLd9hqCWtvCuWxtt7Tfq3w2YJ5jq7VWRFBMolz90:OC/hqCJuWxttHn+7VWR5lz
MD5:	6DEF34B7D9603C4FC7953F177F73C21A
SHA1:	82D464AEDAE69E9FA5AD521CEED3840595F3AD2F
SHA-256:	277E1518B909735B16F393B7077E453735EB4D2DD651891F9F73DA605941493B
SHA-512:	751477B7F904ED0435E18A4435B54B049FFA65135B280549B0CB3CB378CEE462DC470C690927ED629F6F4B798E9EC5193AE1360ACBA34153AF5749015C546A9D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.`.>.3.>.3.>.3.IQ3.>.3.I@3.>.3.IV3.>.3...3.>.3.>.3.>.3.I_3.> .3.IA3.>.3.ID3.>.3Rich.>.3.....PE..L.....b.....n.....D.....@.....d..... .....-..@.....text..... ..`.data... .....p.....@....juv....p.....f.....@..@.rur.....j.....@..@.cenepem..... .....n.....@....rsrc.....r.....@..@.reloc.....&.....@..B..... .....

C:\Users\user\AppData\Roaming\beirutt: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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E

Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.5486278322749145
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	344064
MD5:	6def34b7d9603c4fc7953f177f73c21a
SHA1:	82d464aedae69e9fa5ad521ceed3840595f3ad2f
SHA256:	277e1518b909735b16f393b7077e453735eb4d2dd651891f9f73da605941493b
SHA512:	751477b7f904ed0435e18a4435b54b049ffa65135b280549b0cb3cb378cee462dc470c690927ed629f6f4b798e9ec5193ae1360acba34153af5749015c546a9d
SSDEEP:	6144:OnCLd9hqCWtvCuWxtt7Tfq3w2YJ5jq7VWRFBMolz90:OC/hqCJuWxttHn+7VWR5lz
TLSH:	B1749E01E2E87ED0F599CA318D2EA7EC363EFD514E156666322C7A3F29701E1C52A31D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.`.>.3.>.3.>.3.lQ3.>.3.l@3.>.3.IV3.>.3...3.>.3.>.3.>.3.l_3.>.3.IA3.>.3.ID3.>.3Rich.>.3.....PE..L.....b...

File Icon

Icon Hash:	8494a69696b484e2

Static PE Info

General

Entrypoint:	0x40449f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62BBE3DF [Wed Jun 29 05:32:15 2022 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:	861af707b319724b1132a7a971c54bc2

Entrypoint Preview

Instruction
call 00007F8B6CD1FFFEh
jmp 00007F8B6CD1C30Eh
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx

Instruction
cmp eax, dword ptr [00411008h+ecx*8]
je 00007F8B6CD1C4A5h
inc ecx
cmp ecx, 2Dh
jc 00007F8B6CD1C483h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007F8B6CD1C4A0h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [0041100Ch+ecx*8]
pop ebp
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007F8B6CD1D69Dh
test eax, eax
jne 00007F8B6CD1C498h
mov eax, 00411170h
ret
add eax, 08h
ret
mov edi, edi
push ebp
mov ebp, esp
xor eax, eax
cmp dword ptr [ebp+08h], eax
push 00000000h
sete al
push 00001000h
push eax
call dword ptr [004010CCh]
mov dword ptr [00427F60h], eax
test eax, eax
jne 00007F8B6CD1C494h
pop ebp
ret
xor eax, eax
inc eax
mov dword ptr [0042A204h], eax
pop ebp
ret
mov edi, edi
push esi
push edi
xor esi, esi
mov edi, 00427F68h
cmp dword ptr [00411184h+esi*8], 01h
jne 00007F8B6CD1C4B0h
lea eax, dword ptr [00411180h+esi*8]

Instruction
mov dword ptr [eax], edi
push 00000FA0h
push dword ptr [eax]
add edi, 18h
call 00007F8B6CD1F88Ch
pop ecx
pop ecx
test eax, eax
je 00007F8B6CD1C49Eh
inc esi
cmp esi, 24h
jl 00007F8B6CD1C464h

Rich Headers

Programming Language:	• [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf7b4	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2e000	0x2b298	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5a000	0xaa0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11d0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2da8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x190	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xf0f0	0xf200	False	0.5824832128099173	data	6.681630211805764	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x11000	0x19220	0x17000	False	0.9074388586956522	data	7.675700241362958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.juv	0x2b000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rur	0x2c000	0x2d3	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cenepem	0x2d000	0x3c3	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2e000	0x2b298	0x2b400	False	0.5356642882947977	data	5.343845697441332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x5a000	0x181a	0x1a00	False	0.3527644230769231	data	3.5621171270928884	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x563f0	0x2	data		
AFX_DIALOG_LAYOUT	0x563d8	0x2	data		
AFX_DIALOG_LAYOUT	0x563e0	0xc	data		
RT_CURSOR	0x563f8	0x330	Device independent bitmap graphic, 48 x 96 x 1, image size 0		
RT_CURSOR	0x56728	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x56880	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_CURSOR	0x57728	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_CURSOR	0x57ff8	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x58128	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0		
RT_ICON	0x2ee20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2fcc8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x30570	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x32b18	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x33bc0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x34078	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x34740	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x36ce8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x37180	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x38028	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x388d0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x38e38	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x3b3e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x3c488	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x3ce10	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x3d2e0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x3e188	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x3ea30	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x3f0f8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x3f660	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x41c08	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x42cb0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x43180	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x44028	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors		
RT_ICON	0x448d0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors		
RT_ICON	0x44f98	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors		
RT_ICON	0x45500	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x47aa8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0x48b50	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304		
RT_ICON	0x494d8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024		
RT_ICON	0x499b8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x4a860	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x4b108	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x4b670	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x4dc18	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x4ecc0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x4f648	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x4fb18	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x509c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x51268	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x51930	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x51e98	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x54440	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x554e8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x55e70	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x58418	0x67c	data		
RT_STRING	0x58a98	0x450	data		
RT_STRING	0x58ee8	0x3ac	data		
RT_ACCELERATOR	0x56350	0x58	data		
RT_ACCELERATOR	0x563a8	0x30	data		
RT_GROUP_CURSOR	0x56858	0x22	data		
RT_GROUP_CURSOR	0x57fd0	0x22	data		
RT_GROUP_CURSOR	0x581d8	0x22	data		
RT_GROUP_ICON	0x4fab0	0x68	data		
RT_GROUP_ICON	0x34028	0x4c	data		
RT_GROUP_ICON	0x43118	0x68	data		
RT_GROUP_ICON	0x37150	0x30	data		
RT_GROUP_ICON	0x3d278	0x68	data		
RT_GROUP_ICON	0x49940	0x76	data		
RT_GROUP_ICON	0x562d8	0x76	data		
RT_VERSION	0x58200	0x214	data		

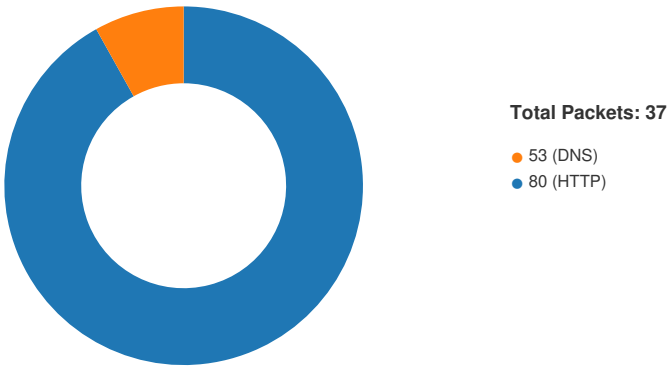
Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetCPInfo, FindResourceExW, EndUpdateResourceW, InterlockedIncrement, GetConsoleAliasA, SetConsoleActiveScreenBuffer, GetModuleHandleW, GetGeoInfoW, GetPriorityClass, GlobalAlloc, LoadLibraryW, CreateEventA, GetSystemWindowsDirectoryA, EnumSystemCodePagesA, GetNamedPipeInfo, GetDevicePowerState, IsBadStringPtrA, LCMapStringA, SetLastError, GetConsoleAliasExesA, GetProcAddress, VirtualAlloc, HeapSize, LoadLibraryA, OpenWaitableTimerW, DnsHostnameToComputerNameA, AddAtomW, GetCommMask, FoldStringW, lstrcmpiW, BuildCommDCBA, VirtualProtect, GetConsoleCursorInfo, GetVolumeNameForVolumeMountPointW, CreateWaitableTimerA, GetConsoleProcessList, EnumCalendarInfoExA, LCMapStringW, CreateFiber, lstrlenA, ReadConsoleOutputCharacterA, GetComputerNameA, GetLastError, HeapFree, Sleep, ExitProcess, GetStartupInfoW, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, HeapAlloc, HeapReAlloc, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, GetCurrentThreadId, InterlockedDecrement, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RaiseException, WriteFile, GetStdHandle, GetModuleFileNameA, InitializeCriticalSectionAndSpinCount, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, SetHandleCount, GetFileType, GetStartupInfoA, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, RtlUnwind, GetACP, GetOEMCP, IsValidCodePage, GetModuleHandleA, GetLocaleInfoA, WideCharToMultiByte, GetStringTypeA, MultiByteToWideChar, GetStringTypeW
USER32.dll	LoadMenuA, SetCaretPos, GetMenuItemID
GDI32.dll	GetCharWidthA
ADVAPI32.dll	BackupEventLogW

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:28:11.568511009 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.586102009 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.586241961 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.586745024 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.586745977 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.603856087 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.603900909 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.725743055 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.725814104 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.725912094 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.739520073 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.739564896 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.760066986 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.760123014 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821665049 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821738005 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821789980 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821837902 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821856976 CET	49736	80	192.168.2.4	188.114.96.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:28:11.821885109 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821911097 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.821933985 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.821981907 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.822033882 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.822046995 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.822108030 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.822256088 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.822305918 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.822354078 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.822366953 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.822397947 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.822457075 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.864998102 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865067959 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865115881 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865165949 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865199089 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.865211010 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865257025 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.865258932 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865307093 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865343094 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.865355968 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.865415096 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.866022110 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866070986 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866117954 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866147041 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.866164923 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866239071 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.866822004 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866868019 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866913080 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.866947889 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.866961002 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.867021084 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.867681980 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.867774010 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.867818117 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.867851019 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.867865086 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.867933035 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.870872974 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.870923042 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.870965004 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.871004105 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.909089088 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909207106 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909255981 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.909269094 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909321070 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909351110 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.909368038 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909418106 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909440041 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.909465075 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909511089 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.909528017 CET	49736	80	192.168.2.4	188.114.96.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:28:11.910379887 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.910433054 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.910464048 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.910480022 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.910528898 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.910551071 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.911082029 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.911133051 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.911155939 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.911180019 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.911226988 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.911274910 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.911904097 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.911952019 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.911997080 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.912044048 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.912086010 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.912723064 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.912769079 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.912816048 CET	80	49736	188.114.96.3	192.168.2.4
Jan 25, 2023 09:28:11.912816048 CET	49736	80	192.168.2.4	188.114.96.3
Jan 25, 2023 09:28:11.912863016 CET	80	49736	188.114.96.3	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:28:11.521898031 CET	56807	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:28:11.545039892 CET	53	56807	8.8.8.8	192.168.2.4
Jan 25, 2023 09:28:27.594902039 CET	61007	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:28:27.617297888 CET	53	61007	8.8.8.8	192.168.2.4
Jan 25, 2023 09:28:29.245378017 CET	60686	53	192.168.2.4	8.8.8.8
Jan 25, 2023 09:28:29.266858101 CET	53	60686	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 09:28:11.521898031 CET	192.168.2.4	8.8.8.8	0xe307	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:28:27.594902039 CET	192.168.2.4	8.8.8.8	0xa725	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:28:29.245378017 CET	192.168.2.4	8.8.8.8	0x149b	Standard query (0)	gekjegoudn 6i5fbces.j omf6mtobkl 32eai1qwqx sxpnfyv2s	A (IP address)	IN (0x0001)	false

DNS Answers

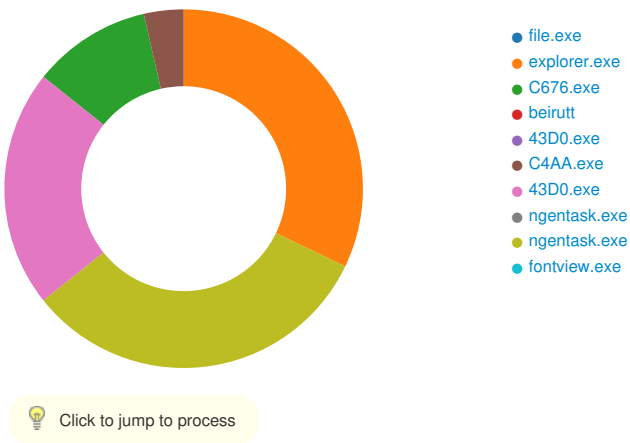
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 09:28:11.545039892 CET	8.8.8.8	192.168.2.4	0xe307	No error (0)	potunulit.org		188.114.96.3	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:28:11.545039892 CET	8.8.8.8	192.168.2.4	0xe307	No error (0)	potunulit.org		188.114.97.3	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:28:27.617297888 CET	8.8.8.8	192.168.2.4	0xa725	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:28:29.266858101 CET	8.8.8.8	192.168.2.4	0x149b	Name error (3)	gekjegoudn 6i5fbces.j omf6mtobkl 32eai1qwqx sxpnfyv2s	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.2ip.ua
- ryjphgb.com
  - potunulit.org
- egqgnqk.org
- aygtqn.org
- fedface.com
- pghirnwb.com
- hkrpyqspb.net
- jwoitvech.com
- fedbh.net
- fyugji.net
- mlleyedksk.org
- vjawtynvst.net
- fyeyf.org

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **1032**, Parent PID: **3528**

General	
Target ID:	0
Start time:	09:27:06
Start date:	25/01/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	344064 bytes
MD5 hash:	6DEF34B7D9603C4FC7953F177F73C21A
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: 00000000.00000002.397037744.00000000005F1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.397037744.00000000005F1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.397025095.00000000005D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.397025095.00000000005D0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.397101149.00000000007A9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.397013971.00000000005C0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3528**, Parent PID: **1032**

General	
Target ID:	3
Start time:	09:27:39
Start date:	25/01/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: C676.exe PID: **4620**, Parent PID: **3528**

General	
Target ID:	6
Start time:	09:28:11
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\C676.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Local\Temp\C676.exe
Imagebase:	0x400000
File size:	417792 bytes
MD5 hash:	261B1DB94CCF4266128E2EB71A80FDA4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000006.00000002.574270691.00000000006A8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000006.00000002.573778926.0000000000580000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 81%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Win32Sync	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4114C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	42E403	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4d 5f fd 60 09 3e fd 33 09 3e fd 33 09 3e fd 33 17 6c 51 33 2d 3e fd 33 17 6c 40 33 1f 3e fd 33 17 6c 56 33 6f 3e fd 33 2e fd fd 33 00 3e fd 33 09 3e fd 33 7e 3e fd 33 17 6c 5f 33 08 3e fd 33 17 6c 41 33 08 3e fd 33 17 6c 44 33 08 3e fd 33 52 69 63 68 09 3e fd 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 fd fd 1a 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$M_`>3>3>3lQ3->3l@3>3lV3o>3.3>3>3~>3l_3>3lA3>3lD3>3Rich>3PELb	success or wait	102	4218C4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe	417792	1048576	a1 fd 5a fd fd fd 25 24 fd 62 46 fd 54 29 2f 7b fd 25 2e db 6f fd 5f fd 26 73 fd fd fd 35 5d 2b 5b fd fd fd 0c 57 3c fd fd fd fd 01 55 01 30 7b fd 66 3d fd 37 65 6c 17 fd fd 3a 78 3d 5f fd 47 20 05 35 7c fd 21 5e fd fd 7b 0c fd 70 73 fd fd fd 62 08 fd 65 fd 59 fd 4e 1d fd 56 6e fd 27 fd 27 fd 13 fd 4a fd fd fd 3b fd 1a 22 50 24 fd 28 7b 31 70 3d 29 fd fd 76 69 56 fd fd 51 22 02 1a fd fd 2f fd fd fd 7e fd 43 fd 6c fd fd fd 38 98 e1 66 77 57 fd 25 70 0a 3a 5c fd 12 fd 74 fd 37 57 fd fd 3a 2e fd fd 68 4d fd fd 6e 7b fd 76 6f 23 fd 18 54 57 2a 64 15 19 fd 14 fd fd 20 14 01 fd fd fd 63 49 fd 44 fd fd 58 fd 74 5f 2e 7c 0e fd 41 2e 77 60 fd 86 fd fd fd 6a 7f fd 53 42 3e 5f 6f fd fd fd 18 fd 4f 36 4c fd 38 36 5d 72 fd 7f fd e4	Z%$bFT)/{%.o_&s5]+ [W<U0{f=7el:x=_G 5\|!^{sbeYNVn"J;"P$({1p=) viVQ"/~Cl8fwW%p:\t7W:. hMn{vo#TWd cIDXt_.|A.w`jSB>_oO6L8 6]r	success or wait	706	4218C4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C676.exe	unknown	4096	success or wait	102	4251A5	ReadFile
C:\Users\user\AppData\Local\Temp\C676.exe	unknown	4096	end of file	1	4251A5	ReadFile

Analysis Process: beirutt PID: **2236**, Parent PID: **1088**

General

Target ID:	7
Start time:	09:28:11
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Roaming\beirutt
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\beirutt
Imagebase:	0x400000
File size:	344064 bytes
MD5 hash:	6DEF34B7D9603C4FC7953F177F73C21A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 43D0.exe PID: **1332**, Parent PID: **3528**

General

Target ID:	8
Start time:	09:28:19
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\43D0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\43D0.exe
Imagebase:	0x400000
File size:	718848 bytes
MD5 hash:	0A006808F7AA017CAF2DF9CE9E2B55A2
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000008.00000002.478433039.00000000048E8000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000008.00000002.479914181.0000000004980000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000008.00000002.479914181.0000000004980000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs
Reputation:	moderate

Analysis Process: C4AA.exe PID: **4116**, Parent PID: **3528**

General

Target ID:	9
Start time:	09:28:22
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\C4AA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C4AA.exe
Imagebase:	0x860000
File size:	1642648 bytes
MD5 hash:	EA25CE2F3580AF1DD771BAC5B0D2BF83
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000009.00000003.485078968.000000000DF30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000009.00000003.485078968.000000000DF30000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000009.00000003.490022034.000000000DF32000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000009.00000002.573780441.000000000128B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 43%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4434343.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2E0FA56	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4434343.dll	0	343040	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 05 00 72 fd fd 63 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 fd 04 00 00 7c 00 00 00 00 00 00 fd 11 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 05 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 1d 05 00 73 00 00 00 03 1e 05 00 3c 00 00	MZx@x!L!This program cannot be run in DOS mode.$PELrc!|@s<	success or wait	1	2E10041	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 43D0.exe PID: **3900**, Parent PID: **1332**

General

Target ID:	10
Start time:	09:28:25
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\43D0.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\43D0.exe
Imagebase:	0x400000
File size:	718848 bytes
MD5 hash:	0A006808F7AA017CAF2DF9CE9E2B55A2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000000A.00000002.481185705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000A.00000002.481185705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000000A.00000002.481185705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000A.00000002.481185705.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ngentask.exe PID: **400**, Parent PID: **4116**

General

Target ID:	11
Start time:	09:28:31
Start date:	25/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe
Imagebase:	0x360000
File size:	85096 bytes
MD5 hash:	ED7F195F7121781CC3D380942765B57D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ngentask.exe PID: **4292**, Parent PID: **4116**

General

Target ID:	12
Start time:	09:28:32
Start date:	25/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe
Imagebase:	0xfa0000
File size:	85096 bytes
MD5 hash:	ED7F195F7121781CC3D380942765B57D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.572420134.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.581410374.00000000033E6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	72D503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: fontview.exe PID: **4772**, Parent PID: **4116**

General

Target ID:	13
Start time:	09:28:34
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\fontview.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SYSWOW64\fontview.exe
Imagebase:	0xdb0000
File size:	114176 bytes
MD5 hash:	218D53564FB0DD0CAFBBF871641E70F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000003.510365391.0000000003056000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 0000000D.00000003.510365391.0000000003056000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000D.00000003.516786735.0000000004F75000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.573423971.0000000004AD0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 0000000D.00000002.573423971.0000000004AD0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly