ID: 322215
Sample Name: kelvinx.exe
Cookbook: default.jbs
Time: 17:56:15
Date: 24/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

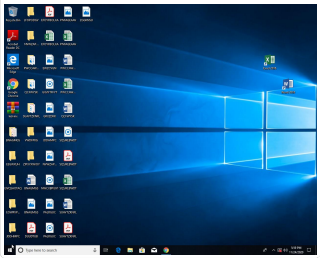
Analysis Report kelvinx.exe

Overview

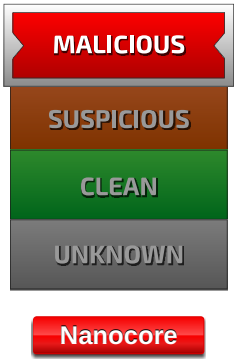
General Information

Sample Name:	kelvinx.exe
Analysis ID:	322215
MD5:	0e4ecbb7ebdd4c..
SHA1:	994026038fcbd05.
SHA256:	20eb19ebf2de899.
Tags:	exe NanoCore

Most interesting Screenshot:



Detection

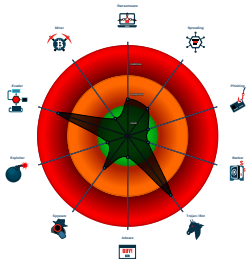


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code references suspic…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other …

Classification



Startup

- **System is w10x64**
- kelvinx.exe (PID: 5332 cmdline: 'C:\Users\user\Desktop\kelvinx.exe' MD5: 0E4ECBB7EBDD4C7341658B9E6471A0B7)
  - kelvinx.exe (PID: 1556 cmdline: C:\Users\user\Desktop\kelvinx.exe MD5: 0E4ECBB7EBDD4C7341658B9E6471A0B7)
- noteped.exe (PID: 5368 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe' MD5: 0E4ECBB7EBDD4C7341658B9E6471A0B7)
  - noteped.exe (PID: 6312 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe MD5: 0E4ECBB7EBDD4C7341658B9E6471A0B7)
- noteped.exe (PID: 6360 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe' MD5: 0E4ECBB7EBDD4C7341658B9E6471A0B7)
  - noteped.exe (PID: 6648 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe MD5: 0E4ECBB7EBDD4C7341658B9E6471A0B7)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.140.53.132"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.306118461.0000000003AE9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.306118461.0000000003AE9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x42f15:$a: NanoCore • 0x42f6e:$a: NanoCore • 0x42fab:$a: NanoCore • 0x43024:$a: NanoCore • 0x566cf:$a: NanoCore • 0x566e4:$a: NanoCore • 0x56719:$a: NanoCore • 0x6f19b:$a: NanoCore • 0x6f1b0:$a: NanoCore • 0x6f1e5:$a: NanoCore • 0x42f77:$b: ClientPlugin • 0x42fb4:$b: ClientPlugin • 0x438b2:$b: ClientPlugin • 0x438bf:$b: ClientPlugin • 0x5648b:$b: ClientPlugin • 0x564a6:$b: ClientPlugin • 0x564d6:$b: ClientPlugin • 0x566ed:$b: ClientPlugin • 0x56722:$b: ClientPlugin • 0x6ef57:$b: ClientPlugin • 0x6ef72:$b: ClientPlugin
00000001.00000002.492062764.00000000041A9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.492062764.00000000041A9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f15:$a: NanoCore • 0x2f6e:$a: NanoCore • 0x2fab:$a: NanoCore • 0x3024:$a: NanoCore • 0x166cf:$a: NanoCore • 0x166e4:$a: NanoCore • 0x16719:$a: NanoCore • 0x2f19b:$a: NanoCore • 0x2f1b0:$a: NanoCore • 0x2f1e5:$a: NanoCore • 0x2f77:$b: ClientPlugin • 0x2fb4:$b: ClientPlugin • 0x38b2:$b: ClientPlugin • 0x38bf:$b: ClientPlugin • 0x1648b:$b: ClientPlugin • 0x164a6:$b: ClientPlugin • 0x164d6:$b: ClientPlugin • 0x166ed:$b: ClientPlugin • 0x16722:$b: ClientPlugin • 0x2ef57:$b: ClientPlugin • 0x2ef72:$b: ClientPlugin
00000001.00000002.493316264.0000000005A30000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.noteped.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
12.2.noteped.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
12.2.noteped.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

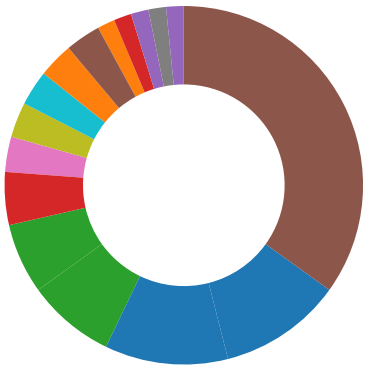
Source	Rule	Description	Author	Strings
12.2.noteped.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
6.2.noteped.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Spreading
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

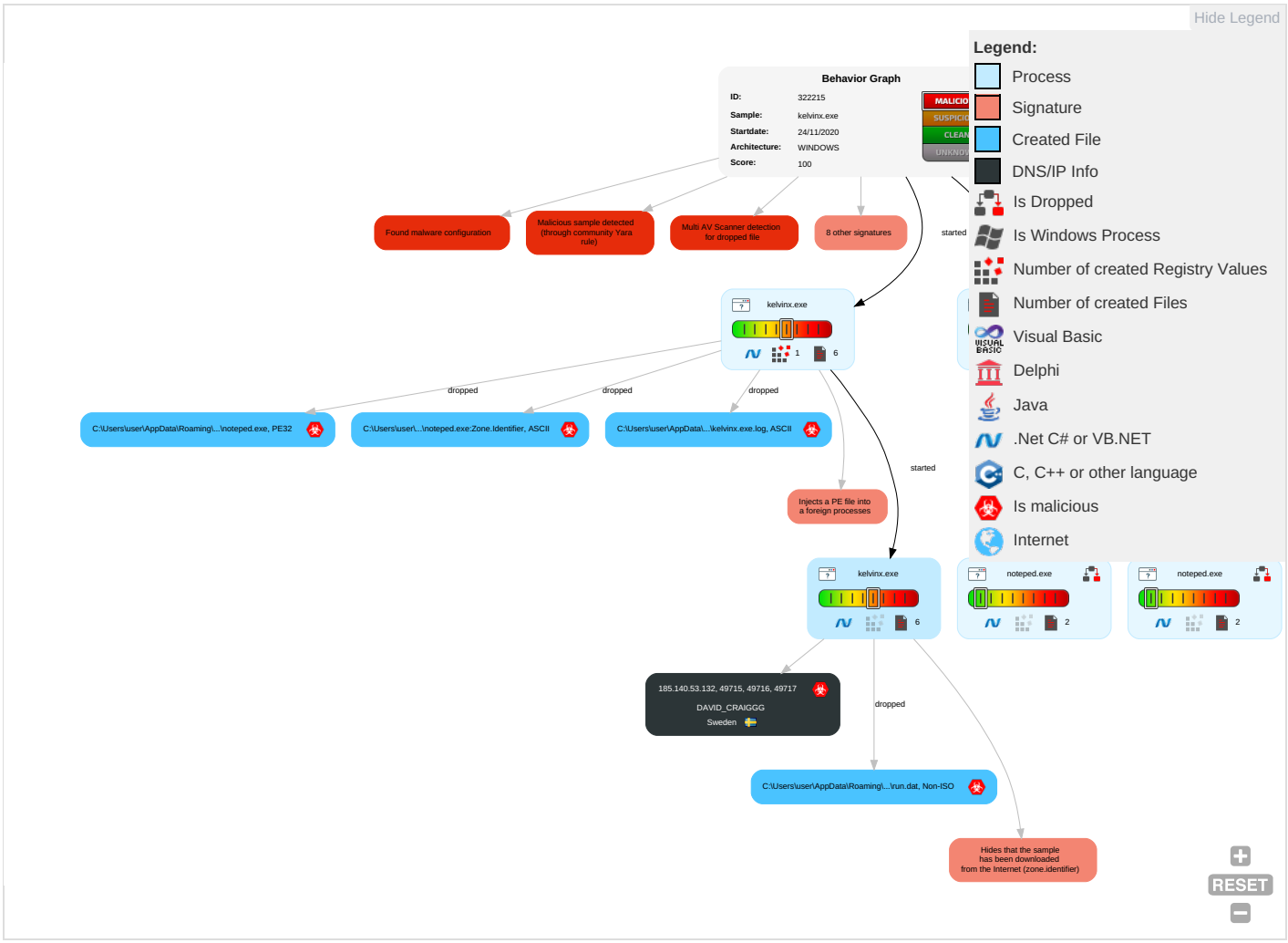
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

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
kelvinx.exe	35%	Virustotal		Browse
kelvinx.exe	52%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
kelvinx.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe	52%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.noteped.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.noteped.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.kelvinx.exe.5a30000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
1.2.kelvinx.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/0w	0%	Avira URL Cloud	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://www.jiyu-kobo.co.jp/jp/.w	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna-d	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn~	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/J	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmNormalr	0%	Avira URL Cloud	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.fontbureau.comcomo	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnude	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/qwCz	0%	Avira URL Cloud	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	
http://www.jiyu-kobo.co.jp/Vwfz	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
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://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.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.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.jiyu-kobo.co.jp/z	0%	Avira URL Cloud	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://www.carterandcone.comimS	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/Y01	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	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.founder.com.cn/cnd:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/xwtz	0%	Avira URL Cloud	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://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://en.wikipF	0%	Avira URL Cloud	safe	
http://en.wC	0%	Avira URL Cloud	safe	
http://www.carterandcone.comper	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/0w	kelvinx.exe, 00000000.00000003.221803128.00000000057C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, kelvinx.exe, 00000000.00000003.221048841.00000000057D7000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high

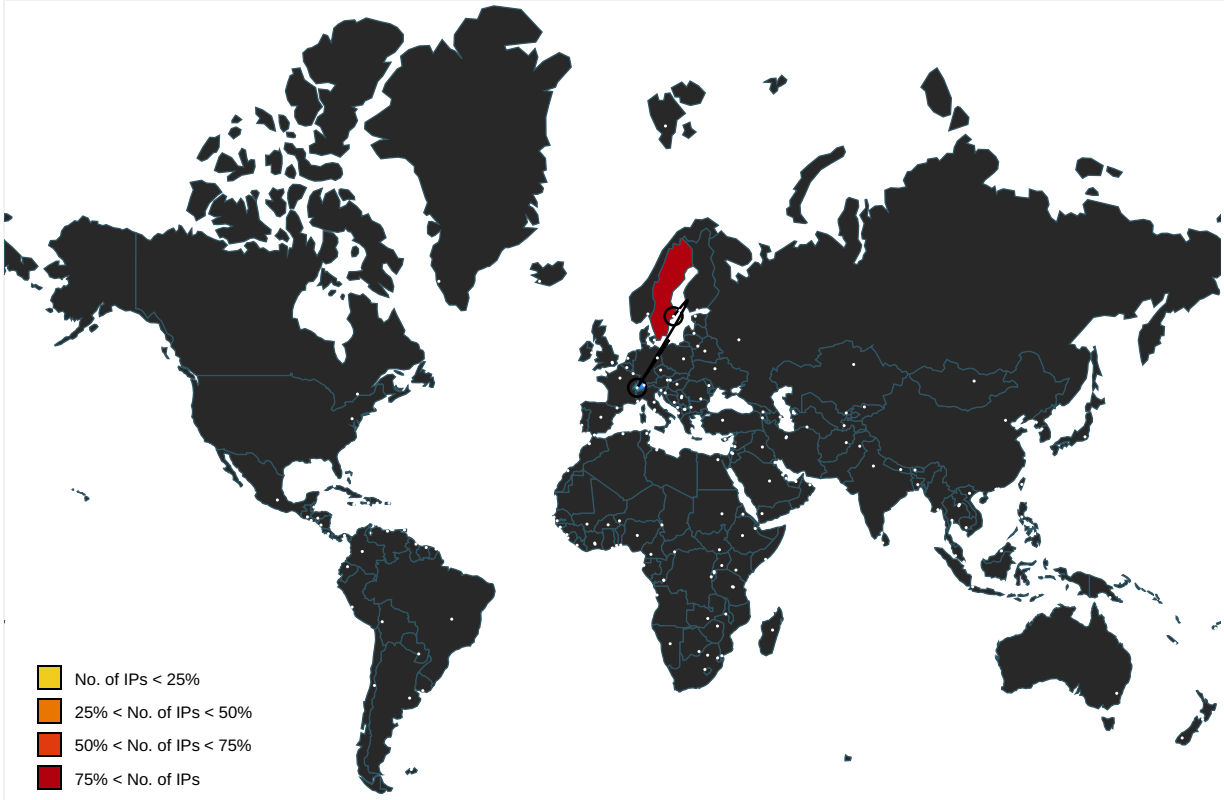
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000005BD0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/.w	kelvinx.exe, 00000000.00000003.221900652.00000000057D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna-d	kelvinx.exe, 00000000.00000003.220725135.00000000057EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn~	kelvinx.exe, 00000000.00000003.220911534.00000000057EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/J	kelvinx.exe, 00000000.00000003.221900652.00000000057D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmNormalr	kelvinx.exe, 00000000.00000003.225402812.00000000057C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comcomo	kelvinx.exe, 00000000.00000003.237362642.00000000057C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnude	kelvinx.exe, 00000000.00000003.220911534.00000000057EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/qwCz	kelvinx.exe, 00000000.00000003.221803128.00000000057C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Vwfz	kelvinx.exe, 00000000.00000003.221900652.00000000057D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	kelvinx.exe, 00000000.00000003.221502115.00000000057D2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	kelvinx.exe, 00000000.00000003.222579187.00000000057CE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	kelvinx.exe, 00000000.00000003.220047831.00000000057E7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	kelvinx.exe, 00000000.00000003.220824103.00000000057EC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/z	kelvinx.exe, 00000000.00000003.221803128.00000000057C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comimS	kelvinx.exe, 00000000.00000003.221173652.00000000057CE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	kelvinx.exe, 00000000.00000003.220783733.00000000057F2000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.00000000005BD0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y01	kelvinx.exe, 00000000.00000003.221985463.00000000057D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	kelvinx.exe, 00000000.00000003.222115295.00000000057CE000.00000004.00000001.sdmp, kelvinx.exe, 00000000.00000003.221900652.00000000057D5000.00000004.00000001.sdmp, kelvinx.exe, 00000000.00000003.221985463.00000000057D5000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnd:	kelvinx.exe, 00000000.00000003.220725135.00000000057EC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/xwtz	kelvinx.exe, 00000000.00000003.221985463.00000000057D5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	kelvinx.exe, 00000000.00000002.244011097.0000000006A52000.00000004.00000001.sdmp, noteped.exe, 00000002.00000002.274192762.00000000055C0000.00000002.00000001.sdmp, noteped.exe, 00000007.00000002.296939599.0000000005BD0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.wikipF	kelvinx.exe, 00000000.00000003.219971249.00000000057E7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wC	kelvinx.exe, 00000000.00000003.219897482.00000000057E6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comper	kelvinx.exe, 00000000.00000003.221173652.00000000057CE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.132	unknown	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322215
Start date:	24.11.2020
Start time:	17:56:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kelvinx.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:	23
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.evad.winEXE@9/5@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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 • 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.

Simulations

Behavior and APIs

Time	Type	Description
17:57:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run noteped "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe"
17:57:11	API Interceptor	951x Sleep call for process: kelvinx.exe modified
17:57:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run noteped "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.132	1kn1ejwPxi.exe	Get hash	malicious	Browse	
	7iatifHQEp.exe	Get hash	malicious	Browse	
	Do43p0ghpz.exe	Get hash	malicious	Browse	
	zWKtabs92B.exe	Get hash	malicious	Browse	
	0076364_00533MXS2.jar	Get hash	malicious	Browse	
	Atlas Home Products Inc RFQ_pdf.jar	Get hash	malicious	Browse	
	Payment Advice Hsbc_pdf.jar	Get hash	malicious	Browse	
	NOTIFICA DI ARRIVO DHL_PDF.jar	Get hash	malicious	Browse	
	NOTIFICA DI ARRIVO DHL_PDF.jar	Get hash	malicious	Browse	
	BOLDROCCHI SRL ITALY QUOTATION REQUEST_PDF.jar	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION.jar	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION_pdf.jar	Get hash	malicious	Browse	
	REQUEST FOR QUOTATION_pdf.jar	Get hash	malicious	Browse	
	Yasuda Kogyo Thailand Co Ltd Request For Quotation_pdf.jar	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Yasuda Kogyo Thailand Co Ltd Request For Quotation_pdf.jar	Get hash	malicious	Browse	
	Ziraat Bankasi Swift_pdf.jar	Get hash	malicious	Browse	
	YI SHNUFA REQUEST FOR QUOTATION.jar	Get hash	malicious	Browse	
	YI SHNUFA REQUEST FOR QUOTATION.jar	Get hash	malicious	Browse	
	TyRSrOojgV.exe	Get hash	malicious	Browse	
	2KGU6Ue1fD.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Order-2311.exe	Get hash	malicious	Browse	• 91.193.75.147
	YZD221120.exe	Get hash	malicious	Browse	• 91.193.75.147
	ORDER #201120A.exe	Get hash	malicious	Browse	• 185.244.30.92
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 185.140.53.149
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Ups file de.exe	Get hash	malicious	Browse	• 185.140.53.221
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 185.140.53.149
	purchase order.exe	Get hash	malicious	Browse	• 185.140.53.233
	Remittance Details.xls	Get hash	malicious	Browse	• 185.140.53.184
	PaymentConfirmation.exe	Get hash	malicious	Browse	• 185.140.53.183
	ORDER #02676.doc.exe	Get hash	malicious	Browse	• 185.244.30.92
	b11305c6ab207f830062f80eeec728c4.exe	Get hash	malicious	Browse	• 185.140.53.233
	ShippingDoc.jar	Get hash	malicious	Browse	• 185.244.30.139
	1kn1ejwPxi.exe	Get hash	malicious	Browse	• 185.140.53.132
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 185.140.53.149
	7iatifHQEp.exe	Get hash	malicious	Browse	• 185.140.53.132
	Sbext4ZNBq.exe	Get hash	malicious	Browse	• 185.140.53.197
	xEdiPz1bC3.exe	Get hash	malicious	Browse	• 185.140.53.234
	7D1wvBrRib.exe	Get hash	malicious	Browse	• 185.140.53.234

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kelvinx.exe.log

Process:	C:\Users\user\Desktop\kelvinx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kelvinx.exe.log	
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\noteped.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	false
Reputation:	moderate, very likely benign file
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\kelvinx.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:j/tn:B
MD5:	7BA5C76EEEAAFAC03FA652DB1B992259
SHA1:	A003E71FB8D389EA8D30D464095DD3CA0AFE8302
SHA-256:	A3B6AD29006658E0A88D38C34AD7541C0C6BEB75E76C7AEF80195110DFCE5406
SHA-512:	B22927302B1614585CDD5F6BFD9935EA64F240800D2801398D25543D9E0E85D2123F73785954523A8DF2D88E0B772B4DB2E076E8381592EFBB44BC0EDA0763F5
Malicious:	**true**
Reputation:	low
Preview:	..#l..H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe	
Process:	C:\Users\user\Desktop\kelvinx.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	783872
Entropy (8bit):	4.202608930384064
Encrypted:	false
SSDEEP:	12288:uAeJdbNJHrO2MZQZhCHy3yYoNp8sGayaRHWXVM4tGG:ybNJLnMZQZMNp7z0GG
MD5:	0E4ECBB7EBDD4C7341658B9E6471A0B7
SHA1:	994026038FCBD0514D029C511F20BDA6B0B17080
SHA-256:	20EB19EBF2DE8995ADBC740F2A797CC3119FACE8760885E7CB9E3A6F3D376D5D
SHA-512:	71493FA50A84576DD8DE39B6A4A111DAB5626073589AFDD9F172C4E292F2E1C220F4DE5257DDAB932A73BC5DD0CCDDEA89336D36536AB4EC2C264DFFFE2EFEA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 52%
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....L..... .....@.. .....`..... ..@.....W.....H.....@..... ..... ..H.....text..... ..... ..`.rsrc....H.....J.....@..@.rel oc.....@.....@..B.....H.....I...0).....IJ...S.....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0.....-.&(....+.&+.*....0 .....-.&(....+.&+.*....0.....,.&(....+.&+.*....0.....-.&(....+.&+.*....0..).....-...-.&sf....-.&+.(....+.(....+.(....+.*....0.....-.&(....+.&+.*....0..F.....~....(....,3 .4..(..... (....o....s.....-.&..-.&+..+.....+.~....*...~....*..0.....-.&+.....+.*.j(.... .

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.202608930384064
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:	kelvinx.exe
File size:	783872
MD5:	0e4ecbb7ebdd4c7341658b9e6471a0b7
SHA1:	994026038fcbd0514d029c511f20bda6b0b17080
SHA256:	20eb19ebf2de8995adbc740f2a797cc3119face8760885e7cb9e3a6f3d376d5d
SHA512:	71493fa50a84576dd8de39b6a4a111dab5626073589afd9f172c4e292f2e1c220f4de5257ddab932a73bc5dd0ccddea89336d36536ab4ec2c264dfffe2ef5ea
SSDEEP:	12288:uAeJdbNJHrO2MZQZhCHy3yYoNp8sGayaRHWXVM4tGG:ybNJLnMZQZMNp7z0GG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....L..... .....@.. .....`.....@.....

File Icon

Icon Hash:	31b1393969391b39

Static PE Info

General

Entrypoint:	0x4bc6f6
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBBAB02 [Mon Nov 23 12:28:50 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc69c	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x48b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xba6fc	0xba800	False	0.415618978301	data	4.02562612318	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x48b4	0x4a00	False	0.664643158784	data	6.51515856258	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	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	0xbe130	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294268550, next used block 4294202757		
RT_GROUP_ICON	0xc2358	0x14	data		
RT_VERSION	0xc236c	0x394	data		
RT_MANIFEST	0xc2700	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Valts Silaputnins (c) 2002-2017 All Rights Reserved
Assembly Version	6.4.0.7666
InternalName	Khmprj5.exe
FileVersion	6.4.0.7666
CompanyName	Proxy Switcher
Comments	Proxy Switcher
ProductName	Proxy Switcher
ProductVersion	6.4.0.7666
FileDescription	Proxy Switcher
OriginalFilename	Khmprj5.exe

Network Behavior

TCP Packets

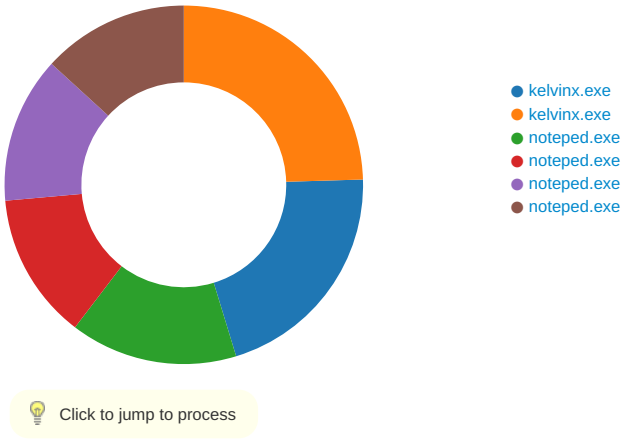
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 17:57:25.073673964 CET	49715	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:25.101609945 CET	7600	49715	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:25.602993965 CET	49715	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:25.629240036 CET	7600	49715	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:26.134700060 CET	49715	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:26.161360025 CET	7600	49715	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:30.198173046 CET	49716	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:30.225003958 CET	7600	49716	185.140.53.132	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 17:57:30.728708982 CET	49716	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:30.755484104 CET	7600	49716	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:31.260085106 CET	49716	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:31.286396980 CET	7600	49716	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:35.405589104 CET	49717	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:35.432176113 CET	7600	49717	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:35.947624922 CET	49717	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:35.974446058 CET	7600	49717	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:36.494554996 CET	49717	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:36.521564960 CET	7600	49717	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:53.293711901 CET	49735	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:53.320538998 CET	7600	49735	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:53.824115992 CET	49735	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:53.850712061 CET	7600	49735	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:54.355438948 CET	49735	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:54.382368088 CET	7600	49735	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:58.482429981 CET	49737	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:58.509083033 CET	7600	49737	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:59.012036085 CET	49737	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:59.038661957 CET	7600	49737	185.140.53.132	192.168.2.5
Nov 24, 2020 17:57:59.543447971 CET	49737	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:57:59.570210934 CET	7600	49737	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:03.577419996 CET	49739	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:03.603759050 CET	7600	49739	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:04.106302023 CET	49739	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:04.132730961 CET	7600	49739	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:04.637505054 CET	49739	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:04.664300919 CET	7600	49739	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:20.812513113 CET	49740	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:20.839032888 CET	7600	49740	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:21.342053890 CET	49740	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:21.368587017 CET	7600	49740	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:21.873284101 CET	49740	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:21.899713993 CET	7600	49740	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:25.922238111 CET	49743	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:25.948868036 CET	7600	49743	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:26.451749086 CET	49743	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:26.478372097 CET	7600	49743	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:26.983045101 CET	49743	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:27.009251118 CET	7600	49743	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:31.330995083 CET	49744	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:31.357367039 CET	7600	49744	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:31.874105930 CET	49744	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:31.900265932 CET	7600	49744	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:32.421050072 CET	49744	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:32.447215080 CET	7600	49744	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:49.379565954 CET	49745	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:49.406280994 CET	7600	49745	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:49.906951904 CET	49745	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:49.933033943 CET	7600	49745	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:50.438106060 CET	49745	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:50.464126110 CET	7600	49745	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:54.503382921 CET	49746	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:54.529875994 CET	7600	49746	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:55.032444000 CET	49746	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:55.058907032 CET	7600	49746	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:55.565989017 CET	49746	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:55.592271090 CET	7600	49746	185.140.53.132	192.168.2.5
Nov 24, 2020 17:58:59.597549915 CET	49747	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:58:59.624389887 CET	7600	49747	185.140.53.132	192.168.2.5
Nov 24, 2020 17:59:00.126689911 CET	49747	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:59:00.153503895 CET	7600	49747	185.140.53.132	192.168.2.5
Nov 24, 2020 17:59:00.657816887 CET	49747	7600	192.168.2.5	185.140.53.132
Nov 24, 2020 17:59:00.684556961 CET	7600	49747	185.140.53.132	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: kelvinx.exe PID: 5332 Parent PID: 5744

General

Start time:	17:57:00
Start date:	24/11/2020
Path:	C:\Users\user\Desktop\kelvinx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\kelvinx.exe'
Imagebase:	0x4b0000
File size:	783872 bytes
MD5 hash:	0E4ECBB7EBDD4C7341658B9E6471A0B7
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: 00000000.00000002.240965816.0000000003B26000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.240965816.0000000003B26000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.240965816.0000000003B26000.00000004.00000001.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	6DD1CF06	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	6DD1CF06	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.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	873E4EB	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	873E4EB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kelvinx.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe	0	262144	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 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 02 ab bb 5f 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 a8 0b 00 00 4c 00 00 00 00 00 00 f6 c6 0b 00 00 20 00 00 00 e0 0b 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 0c 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......_.......... ....L........... ....@.. ....` ....@................	success or wait	3	873E4EB	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	873E4EB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kelvinx.exe.log	unknown	1119	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	6E02C907	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	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	noteped	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe"	success or wait	1	6CB6646A	RegSetValueExW

Analysis Process: kelvinx.exe PID: 1556 Parent PID: 5332

General

Start time:	17:57:09
Start date:	24/11/2020
Path:	C:\Users\user\Desktop\kelvinx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kelvinx.exe
Imagebase:	0xe20000
File size:	783872 bytes
MD5 hash:	0E4ECBB7EBDD4C7341658B9E6471A0B7
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: 00000001.00000002.492062764.00000000041A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.492062764.00000000041A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.493316264.0000000005A30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.493316264.0000000005A30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.493316264.0000000005A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.493282549.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.493282549.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.488239312.0000000003161000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.485264467.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.485264467.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.485264467.0000000000402000.00000040.00000001.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	6DD1CF06	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	6DD1CF06	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	6CB6BEFF	CreateDirectoryW
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	6CB61E60	CreateFileW
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	6CB6BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CB6BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\kelvinx.exe:Zone.Identifier	success or wait	1	6CAE2935	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	a4 f0 23 6c e5 90 d8 48	..#l...H	success or wait	1	6CB61B4F	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	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile
C:\Users\user\Desktop\kelvinx.exe	unknown	4096	success or wait	1	6DCDD72F	unknown
C:\Users\user\Desktop\kelvinx.exe	unknown	512	success or wait	1	6DCDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DCDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DCDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DCDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DCDD72F	unknown

Analysis Process: noteped.exe PID: 5368 Parent PID: 3472

General

Start time:	17:57:16
Start date:	24/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe'
Imagebase:	0x130000
File size:	783872 bytes
MD5 hash:	0E4ECBB7EBDD4C7341658B9E6471A0B7
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: 00000002.00000002.269811701.00000000035FB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.269811701.00000000035FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.269811701.00000000035FB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 52%, 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	6DD1CF06	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	6DD1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\noteped.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E02C78D	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\noteped.exe.log	unknown	1119	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	6E02C907	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	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile

Analysis Process: noteped.exe PID: 6312 Parent PID: 5368

General

Start time:	17:57:23
Start date:	24/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
Imagebase:	0xa60000
File size:	783872 bytes
MD5 hash:	0E4ECBB7EBDD4C7341658B9E6471A0B7
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: 00000006.00000002.284681945.0000000002FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.284681945.0000000002FB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.284823064.0000000003FB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.284823064.0000000003FB9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.283332088.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.283332088.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.283332088.0000000000402000.00000040.00000001.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	6DD1CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DD1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile

Analysis Process: noteped.exe PID: 6360 Parent PID: 3472

General

Start time:	17:57:24
Start date:	24/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe'
Imagebase:	0x7d0000
File size:	783872 bytes
MD5 hash:	0E4ECBB7EBDD4C7341658B9E6471A0B7
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: 00000007.00000002.289900545.0000000003C9C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.289900545.0000000003C9C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.289900545.0000000003C9C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DD1CF06	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	6DD1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile

Analysis Process: noteped.exe PID: 6648 Parent PID: 6360

General

Start time:	17:57:31
Start date:	24/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepod\noteped.exe
Imagebase:	0x6e0000
File size:	783872 bytes
MD5 hash:	0E4ECBB7EBDD4C7341658B9E6471A0B7
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: 0000000C.00000002.306118461.0000000003AE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.306118461.0000000003AE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.305164959.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.305164959.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.305164959.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.306051125.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.306051125.0000000002AE1000.00000004.00000001.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	6DD1CF06	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	6DD1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB61B4F	ReadFile

Disassembly

Code Analysis