ID: 319657
Sample Name:
NXKfWP9SPF0XHRu.exe
Cookbook: default.jbs
Time: 14:24:04
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

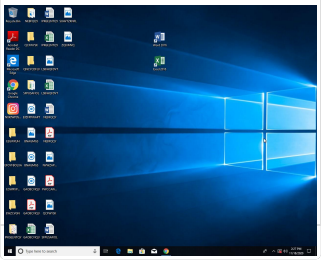
Analysis Report NXKfWP9SPF0XHRu.exe

Overview

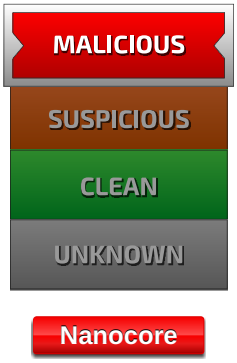
General Information

Sample Name:	NXKfWP9SPF0XHRu.exe
Analysis ID:	319657
MD5:	444332a61d888a..
SHA1:	5d518f814c09b15.
SHA256:	611c893208d8bf0.
Tags:	ESP exe geo NanoCore RAT

Most interesting Screenshot:



Detection

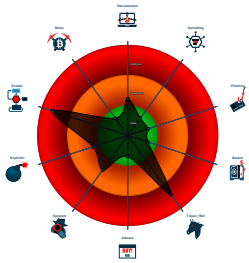


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- NXKfWP9SPF0XHRu.exe (PID: 5952 cmdline: 'C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe' MD5: 444332A61D888AC4F80DB03B3C2129E9)
  - schtasks.exe (PID: 6052 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ynSazlVxDpCRe' /XML 'C:\Users\user\AppData\Local\Temp\tmp10AA.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NXKfWP9SPF0XHRu.exe (PID: 768 cmdline: {path} MD5: 444332A61D888AC4F80DB03B3C2129E9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.512257767.000000000571 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000003.00000002.512257767.000000000571 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000003.00000002.512257767.000000000571 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.253897211.0000000003B4 2000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x24f68d:$x1: NanoCore.ClientPluginHost • 0x24f6ca:$x2: IClientNetworkHost • 0x2531fd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.253897211.0000000003B4 2000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.NXKfWP9SPF0XHRu.exe.5710000.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
3.2.NXKfWP9SPF0XHRu.exe.5710000.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
3.2.NXKfWP9SPF0XHRu.exe.5710000.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.2.NXKfWP9SPF0XHRu.exe.5710000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
3.2.NXKfWP9SPF0XHRu.exe.5710000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
Click to see the 7 entries				

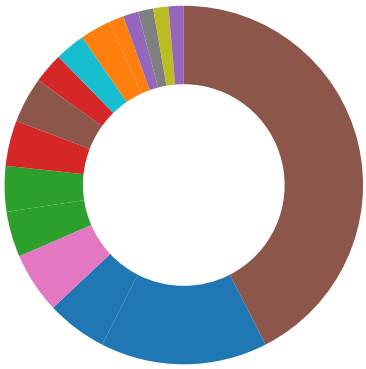
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Software Vulnerabilities
- 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:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

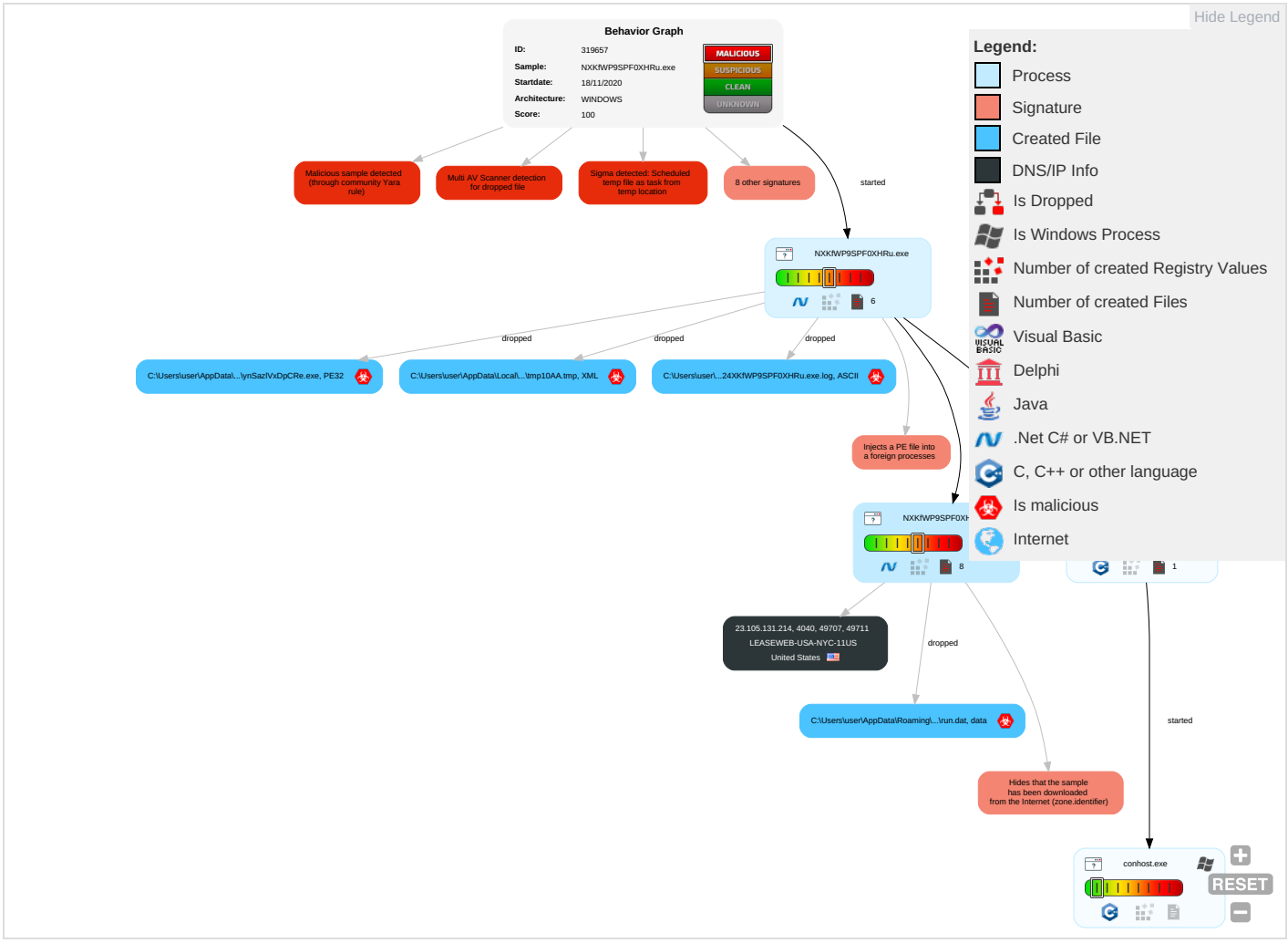
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	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	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Protc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

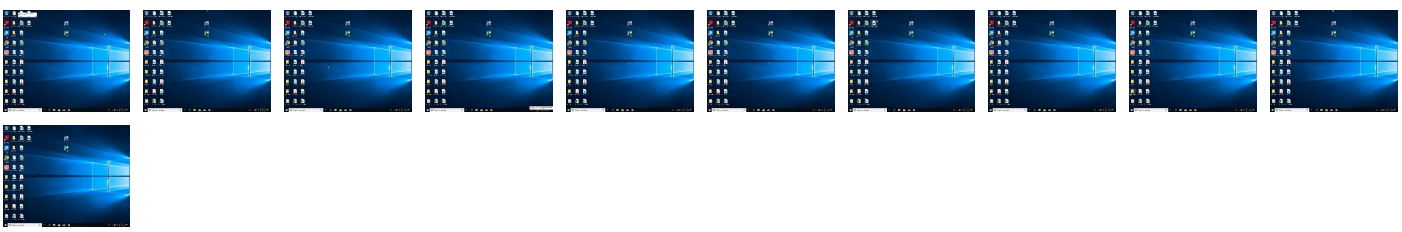
Behavior Graph



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
NXKfWP9SPF0XHRu.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ynSazlVxDpCRe.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.NXKfWP9SPF0XHRu.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comoa	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.founder.com.cn/cn/bThe	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.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	
http://www.goodfont.co.kr	0%	URL Reputation	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.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/7	0%	Virustotal		Browse
http://www.jiyu-kobo.co.jp/jp/7	0%	Avira URL Cloud	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.carterandcone.comefaD	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/roso	0%	Avira URL Cloud	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.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.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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/h	0%	Avira URL Cloud	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://www.jiyu-kobo.co.jp/)	0%	Avira URL Cloud	safe	
http://www.carterandcone.comadi	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://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comlicF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed)	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comM.TTFh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	Avira URL Cloud	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://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	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.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.fontbureau.comituF	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/v	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/vvU	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.fontbureau.comdE	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdL	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Bold	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

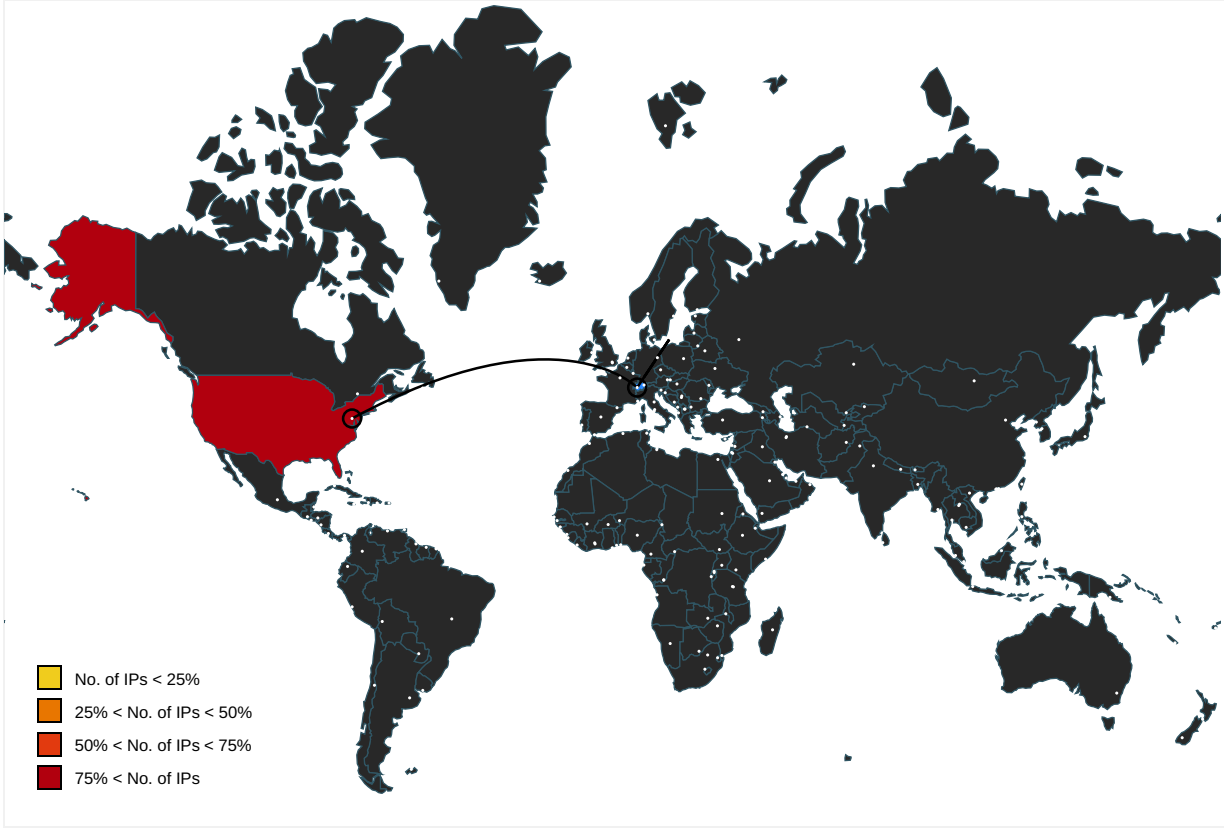
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comoa	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.tiro.com	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp, NXKfWP9SPF0XHRu.exe, 00000000.00000003.239916983.0000000004C74000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/7	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comefaD	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240460926.0000000004C6B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/roso	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/7	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240460926.0000000004C6B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/h	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240460926.0000000004C6B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240762052.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comadi	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comlicF	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comessed)	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comF	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comM.TTFh	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/E	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp, NXKfWP9SPF0XHRu.exe, 00000000.00000003.240460926.0000000004C6B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255001568.0000000004C60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	NXKfWP9SPF0XHRu.exe, 00000000.00000003.239663209.0000000004C70000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comituF	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp, NXKfWP9SPF0XHRu.exe, 00000000.00000003.239663209.0000000004C70000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/v	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/)	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240678890.0000000004C69000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/vvU	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240460926.0000000004C6B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp, NXKfWP9SPF0XHRu.exe, 00000000.00000003.240252277.0000000004C6B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comdE	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	NXKfWP9SPF0XHRu.exe, 00000000.00000002.255243254.0000000004E72000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/h	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240900347.0000000004C68000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdL	NXKfWP9SPF0XHRu.exe, 00000000.00000003.241684541.0000000004C6A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Bold	NXKfWP9SPF0XHRu.exe, 00000000.00000003.240252277.0000000004C6B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.105.131.214	unknown	United States		396362	LEASEWEB-USA-NYC-11US	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319657
Start date:	18.11.2020
Start time:	14:24:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NXKfWP9SPF0XHRu.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:	13
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@6/4@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 4.3% (good quality ratio 2.5%) • Quality average: 36.9% • Quality standard deviation: 37.2%
HCA Information:	• Successful, ratio: 95% • 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. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:25:00	API Interceptor	1032x Sleep call for process: NXKfWP9SPF0XHRu.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	DOC.exe	Get hash	malicious	Browse	• 23.105.131.162
	Shipping_Details.exe	Get hash	malicious	Browse	• 23.105.131.165
	2AyWKsCvVF.exe	Get hash	malicious	Browse	• 192.253.246.143
	tn9jVPvlMSqAUX5.exe	Get hash	malicious	Browse	• 23.105.131.229
	HLiw2LPA8i.rtf	Get hash	malicious	Browse	• 192.253.246.143
	TDToxqrclL.exe	Get hash	malicious	Browse	• 23.105.131.177
	Ziiq5tI3CT.exe	Get hash	malicious	Browse	• 23.105.131.239
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.246.143
	ORDER INQUIRY.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Purchase Order 4500033557.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	SecuriteInfo.com.Trojan.DownLoader35.34609.25775.exe	Get hash	malicious	Browse	• 192.253.246.138
	Proof_of_payment.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	invoice tax.xlsm	Get hash	malicious	Browse	• 23.105.131.217

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SHIPPING DOCUMENTS.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 192.253.246.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.246.143
	HDyADDoI3I.exe	Get hash	malicious	Browse	• 192.253.246.143
	11.exe	Get hash	malicious	Browse	• 173.234.155.145
	53C29QAJnd.exe	Get hash	malicious	Browse	• 173.234.155.145
	OMQZvmAmCj.exe	Get hash	malicious	Browse	• 173.234.155.145

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NXKfWP9SPF0XHRu.exe.log

Process:	C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.271473536084351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2u7x5I6Hi0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2I3rOz2T
MD5:	C3EC08CD6BEA8576070D5A52B4B6D7D0
SHA1:	40B95253F98B3CC5953100C0E71DAC7915094A5A
SHA-256:	28B314C3E5651414FD36B2A65B644A2A55F007A34A536BE17514E12CEE5A091B
SHA-512:	5B0E6398A092F08240DC6765425E16DB52F32542FF7250E87403C407E54B3660EF93E0EAD17BA2CEF6B666951ACF66FA0EAD61FB52E80867DDD398E8258DED2
Malicious:	**true**
Reputation:	moderate, very likely benign file
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_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Web\d05d469d89b319a068f2123e7e6f8621\System.Web.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp10AA.tmp

Process:	C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.176645564878553
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB9tn:cbhH7MlNQ8/rydbz9I3YODOLNdq3F
MD5:	FA36D3CC836AD8E1BADA121233E83614
SHA1:	0DE7C6F513638E8B5E51C10C120D72BE6597FE08
SHA-256:	0B393495206B3678363CAAE0231816475DAB2549E90F3F0F4C604B87BB20CB52
SHA-512:	70DB8009383D2B11EED52570BAD37F5C30265EE8C8327E8582BA5118F14E17812FB61F69BE7C2B8E4114AB6B335CFE746442B30CEA58E95BD1DF22D36CF1630
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp10AA.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:tLujP:5CP
MD5:	E78B48E8D621A403BFAB625F1C92B04C
SHA1:	E7A09F8F0B049DD57A0540A4AF40AF6A5D523676
SHA-256:	D898054E52D71F403A89EB5D4B16B2E5221320ADE9D664FA3C8D72FC25D3DF8B
SHA-512:	810437550F308D974262BDBE620BFC9DAC23AB85E044B9972ED8BC4CCBA66E617B1AC1389E1A56E0919B10176CC63EC495B4A472DD0CB9A0CC4F70137F819B0
Malicious:	**true**
Reputation:	low
Preview:	.=.....H

C:\Users\user\AppData\Roaming\ynSazlVxDpCRe.exe	
Process:	C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1117184
Entropy (8bit):	7.378881785743249
Encrypted:	false
SSDEEP:	12288:VyrKywLz229e7sGJ3UogQpht8LFOcc6WkFR+wn3+0vCi/2mD0eIjAgC46H3Wsmij:VV29I19pv8bWkbr3nd2+sgT3c05s
MD5:	444332A61D888AC4F80DB03B3C2129E9
SHA1:	5D518F814C09B15B35CD9BA5D20D0892BD8EF90B
SHA-256:	611C893208D8BF06031DA708A44EC749B89B069AD1E84C14625B02BCCB4998A0
SHA-512:	699618863E73B9A748A54002847817C66D4582D70CB740C13AC24AD8C26AC050CA68A2B4BF84AA5594977B30B37EAA4B60D361B3C7C0E4D35A77AB66CF12DA6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q._.....0.....D.....~.... .....@.. .....@.....0...K.....A.....`..... ..... ..H.....text..... ..... ..`.rsrc....A.....B.....@..@.reloc.....`.....@..B.....`.....H.....H,.....5.....U.?...%....*..>M|.u?Ls..5....|...C..Z.P.z.....D.uj.b.....h...q...N...Tf.J!.L.i...uU.p../rR./oe....;...?0....B..>e.K.A..(.0.....TZ.....h;P8.....vc.Q.s<.sp+..K.*....~..;...4..bn..`e,<s.E&f...4.=..N.C..P.x.g.G..s?...e.....r.b.P8M.....KbN.....d~.u..5..F.:..y..^g.....X....V.:..@.....4+.Y7.}:_.rC'.....9..A...\.....c1..S....b.;...:.....fc+.....":(..V

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.378881785743249
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	NXKfWP9SPF0XHRu.exe
File size:	1117184
MD5:	444332a61d888ac4f80db03b3c2129e9
SHA1:	5d518f814c09b15b35cd9ba5d20d0892bd8ef90b

General

SHA256:	611c893208d8bf06031da708a44ec749b89b069ad1e84c14625b02bccb4998a0
SHA512:	699618863e73b9a748a54002847817c66d4582d70cb74 c13ac24ad8c26ac050ca68a2b4bf84aa5594977b30b37eaa4b60d361b3c7c0e4d35a77ab66cf12da67
SSDEEP:	12288:VyrKywLz229e7sGJ3UogQpht8LFOcc6WkFR+wn3+0vCi/2mD0eIjAgC46H3Wsmij:VV29l19pv8bWkbr3nd2+sgT3c05s
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...q.._..............0......D......~.... ....@.. ....@................................

File Icon

Icon Hash:	f8c492aaaa92dcfe

Static PE Info

General

Entrypoint:	0x50e47e
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:	0x5FB4A371 [Wed Nov 18 04:30:41 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10e430	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x110000	0x41a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x116000	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	0x10c484	0x10c600	False	0.694556539648	data	7.38603476189	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x110000	0x41a8	0x4200	False	0.503551136364	data	5.45014806784	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x116000	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	0x110190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1105f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0x1116a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3771611807, next used block 3167566498		
RT_GROUP_ICON	0x113c48	0x30	data		
RT_VERSION	0x113c78	0x344	data		
RT_MANIFEST	0x113fbc	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

Description	Data
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	u.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Clinic Management System
ProductVersion	1.0.0.0
FileDescription	Clinic Management System
OriginalFilename	u.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 14:25:05.655561924 CET	49707	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:05.762923956 CET	4040	49707	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:06.269063950 CET	49707	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:06.376255989 CET	4040	49707	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:06.878592014 CET	49707	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:06.985805988 CET	4040	49707	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:11.036412954 CET	49711	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:11.143027067 CET	4040	49711	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:11.644598007 CET	49711	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:11.751352072 CET	4040	49711	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:12.253920078 CET	49711	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:12.360694885 CET	4040	49711	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:16.381172895 CET	49712	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:16.487755060 CET	4040	49712	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:16.988778114 CET	49712	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:17.095190048 CET	4040	49712	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:17.598263979 CET	49712	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:17.704638004 CET	4040	49712	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:21.709471941 CET	49713	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:21.816246033 CET	4040	49713	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:22.317313910 CET	49713	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:22.424000978 CET	4040	49713	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:22.926789999 CET	49713	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:23.033458948 CET	4040	49713	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:27.039275885 CET	49714	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:27.145787954 CET	4040	49714	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:27.645889997 CET	49714	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:27.752454042 CET	4040	49714	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:28.255383968 CET	49714	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:28.363981962 CET	4040	49714	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:32.384649992 CET	49715	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:32.491986036 CET	4040	49715	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:33.005712032 CET	49715	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:33.113073111 CET	4040	49715	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:33.615221977 CET	49715	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:33.722516060 CET	4040	49715	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:37.851440907 CET	49716	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:37.958148003 CET	4040	49716	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:38.459316969 CET	49716	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:38.566000938 CET	4040	49716	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:39.068857908 CET	49716	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:39.175647020 CET	4040	49716	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:43.180646896 CET	49718	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:43.284518003 CET	4040	49718	23.105.131.214	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 14:25:43.787796021 CET	49718	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:43.891825914 CET	4040	49718	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:44.397327900 CET	49718	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:44.501189947 CET	4040	49718	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:48.509617090 CET	49719	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:48.612853050 CET	4040	49719	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:49.116368055 CET	49719	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:49.219748020 CET	4040	49719	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:49.726284981 CET	49719	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:49.829591990 CET	4040	49719	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:53.849896908 CET	49720	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:53.956172943 CET	4040	49720	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:54.460562944 CET	49720	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:54.567054987 CET	4040	49720	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:55.069973946 CET	49720	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:55.176698923 CET	4040	49720	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:59.181191921 CET	49721	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:59.284069061 CET	4040	49721	23.105.131.214	192.168.2.7
Nov 18, 2020 14:25:59.789201975 CET	49721	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:25:59.892447948 CET	4040	49721	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:00.398818970 CET	49721	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:00.501836061 CET	4040	49721	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:04.605669975 CET	49722	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:04.712171078 CET	4040	49722	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:05.227189064 CET	49722	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:05.333668947 CET	4040	49722	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:05.836596012 CET	49722	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:05.943167925 CET	4040	49722	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:09.948410034 CET	49723	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:10.056273937 CET	4040	49723	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:10.571996927 CET	49723	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:10.679358959 CET	4040	49723	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:11.196446896 CET	49723	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:11.303950071 CET	4040	49723	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:15.307607889 CET	49724	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:15.411216021 CET	4040	49724	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:15.915965080 CET	49724	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:16.019602060 CET	4040	49724	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:16.525095940 CET	49724	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:16.628814936 CET	4040	49724	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:20.667470932 CET	49725	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:20.770468950 CET	4040	49725	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:21.275284052 CET	49725	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:21.378113985 CET	4040	49725	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:21.884706020 CET	49725	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:21.987725973 CET	4040	49725	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:25.997817993 CET	49726	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:26.104825020 CET	4040	49726	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:26.619509935 CET	49726	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:26.726696014 CET	4040	49726	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:27.228938103 CET	49726	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:27.336147070 CET	4040	49726	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:31.341444969 CET	49727	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:31.447765112 CET	4040	49727	23.105.131.214	192.168.2.7
Nov 18, 2020 14:26:31.948226929 CET	49727	4040	192.168.2.7	23.105.131.214
Nov 18, 2020 14:26:32.054521084 CET	4040	49727	23.105.131.214	192.168.2.7

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NXKfWP9SPF0XHRu.exe PID: 5952 Parent PID: 5616

General

Start time:	14:24:57
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe'
Imagebase:	0x1a0000
File size:	1117184 bytes
MD5 hash:	444332A61D888AC4F80DB03B3C2129E9
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: 00000000.00000002.253897211.0000000003B42000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.253897211.0000000003B42000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.253897211.0000000003B42000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.253518250.000000000398D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.253518250.000000000398D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.253518250.000000000398D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.251828506.0000000002994000.00000004.00000001.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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\ynSazlVxDpCRe.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5410403	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp10AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	89B2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NXKfWP9SPF0XHRu.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
unknown	success or wait	1	541112A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ynSazlVxDpCRe.exe	unknown	1117184	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 71 a3 b4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 c6 10 00 00 44 00 00 00 00 00 00 7e e4 10 00 00 20 00 00 00 00 11 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 11 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...q.._.......... ....0......D......~.... ....@.. ....@.................	success or wait	1	541068B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp10AA.tmp	unknown	1662	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	541068B	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\NXKfWP9SPF0XHRu.exe.log	unknown	641	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	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,"	success or wait	1	7273A33A	WriteFile

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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe	unknown	1117184	success or wait	1	541068B	ReadFile

Analysis Process: schtasks.exe PID: 6052 Parent PID: 5952

General

Start time:	14:25:01
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ynSazlVxDpCRe' /XML 'C:\Users\user\AppData\Local\Temp\tmp10AA.tmp'
Imagebase:	0xe50000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp10AA.tmp	unknown	2	success or wait	1	E5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp10AA.tmp	unknown	1663	success or wait	1	E5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6092 Parent PID: 6052

General

Start time:	14:25:02
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: NXKfWP9SPF0XHRu.exe PID: 768 Parent PID: 5952

General

Start time:	14:25:02
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x700000
File size:	1117184 bytes
MD5 hash:	444332A61D888AC4F80DB03B3C2129E9

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: 00000003.00000002.512257767.0000000005710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.512257767.0000000005710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.512257767.0000000005710000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.511185145.0000000003EE7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.511185145.0000000003EE7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.505689991.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.505689991.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.505689991.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.512006874.0000000005200000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.512006874.0000000005200000.00000004.00000001.sdmp, Author: Florian Roth
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	724660AC	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	724660AC	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	50407A1	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	504089B	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	50407A1	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	50407A1	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	724660AC	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	724660AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe:Zone.Identifier	success or wait	1	5040B41	DeleteFileA

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	d5 3d ee cb 10 8c d8 48	.=.....H	success or wait	1	5040A53	WriteFile

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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Users\user\Desktop\NXKfWP9SPF0XHRu.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5040A53	ReadFile

Disassembly

Code Analysis