ID: 323033
Sample Name: Receipt#502.exe
Cookbook: default.jbs
Time: 08:33:26
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

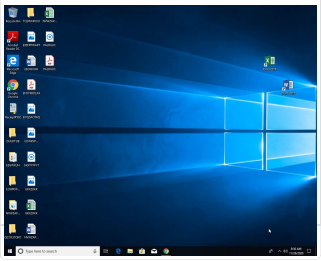
Analysis Report Receipt#502.exe

Overview

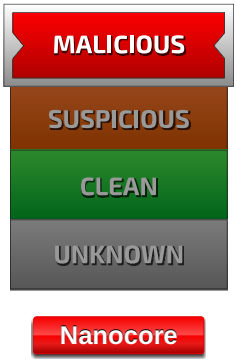
General Information

Sample Name:	Receipt#502.exe
Analysis ID:	323033
MD5:	e2e26573196fd44.
SHA1:	8a2fc9e82c11d23.
SHA256:	40fe69be55041a8.
Tags:	exe NanoCore nVpn RAT

Most interesting Screenshot:



Detection

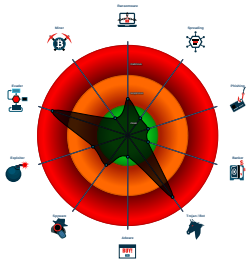


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- Receipt#502.exe (PID: 4636 cmdline: 'C:\Users\user\Desktop\Receipt#502.exe' MD5: E2E26573196FD444C8845D29E73A6B00)
  - schtasks.exe (PID: 1384 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NeKPJNb' /XML 'C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5476 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - RegSvcs.exe (PID: 5480 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000005.00000003.261720988.000000000429 3000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x211a:$a: NanoCore • 0x213f:$a: NanoCore • 0x2198:$a: NanoCore • 0x12335:$a: NanoCore • 0x1235b:$a: NanoCore • 0x123b7:$a: NanoCore • 0x1f20c:$a: NanoCore • 0x1f265:$a: NanoCore • 0x1f298:$a: NanoCore • 0x1f4c4:$a: NanoCore • 0x1f540:$a: NanoCore • 0x1fb59:$a: NanoCore • 0x1fca2:$a: NanoCore • 0x20176:$a: NanoCore • 0x2045d:$a: NanoCore • 0x20474:$a: NanoCore • 0x237fd:$a: NanoCore • 0x24bb7:$a: NanoCore • 0x24c01:$a: NanoCore • 0x2585b:$a: NanoCore • 0x2ae40:$a: NanoCore
00000000.00000002.254057757.0000000003CD 8000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13056d:$x1: NanoCore.ClientPluginHost • 0x1305aa:$x2: IClientNetworkHost • 0x1340dd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.254057757.0000000003CD 8000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.254057757.0000000003CD 8000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1302d5:$a: NanoCore • 0x1302e5:$a: NanoCore • 0x130519:$a: NanoCore • 0x13052d:$a: NanoCore • 0x13056d:$a: NanoCore • 0x130334:$b: ClientPlugin • 0x130536:$b: ClientPlugin • 0x130576:$b: ClientPlugin • 0x13045b:$c: ProjectData • 0x130e62:$d: DESCrypto • 0x13882e:$e: KeepAlive • 0x13681c:$g: LogClientMessage • 0x132a17:$i: get_Connected • 0x131198:$j: #=q • 0x1311c8:$j: #=q • 0x1311e4:$j: #=q • 0x131214:$j: #=q • 0x131230:$j: #=q • 0x13124c:$j: #=q • 0x13127c:$j: #=q • 0x131298:$j: #=q
00000000.00000002.254741913.0000000003EC 2000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1e881d:$x1: NanoCore.ClientPluginHost • 0x1e885a:$x2: IClientNetworkHost • 0x1ec38d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 8 entries				

Sigma Overview

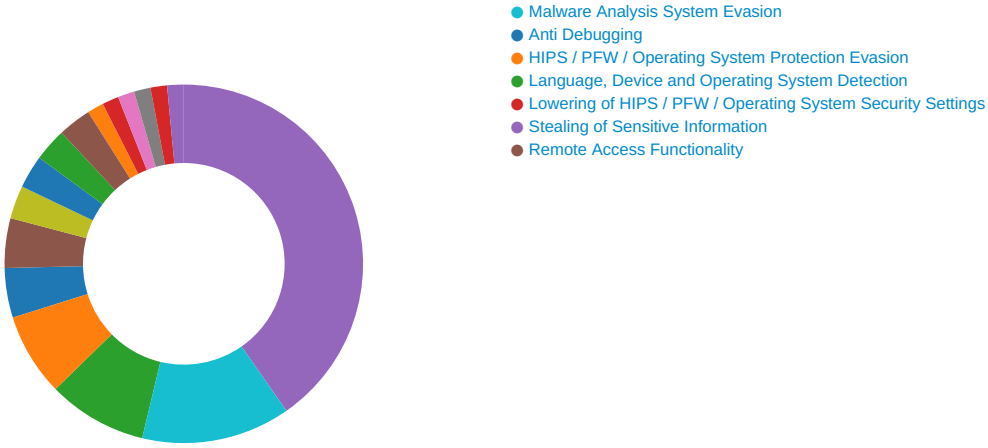
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection



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

Networking:

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

Uses dynamic DNS services

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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

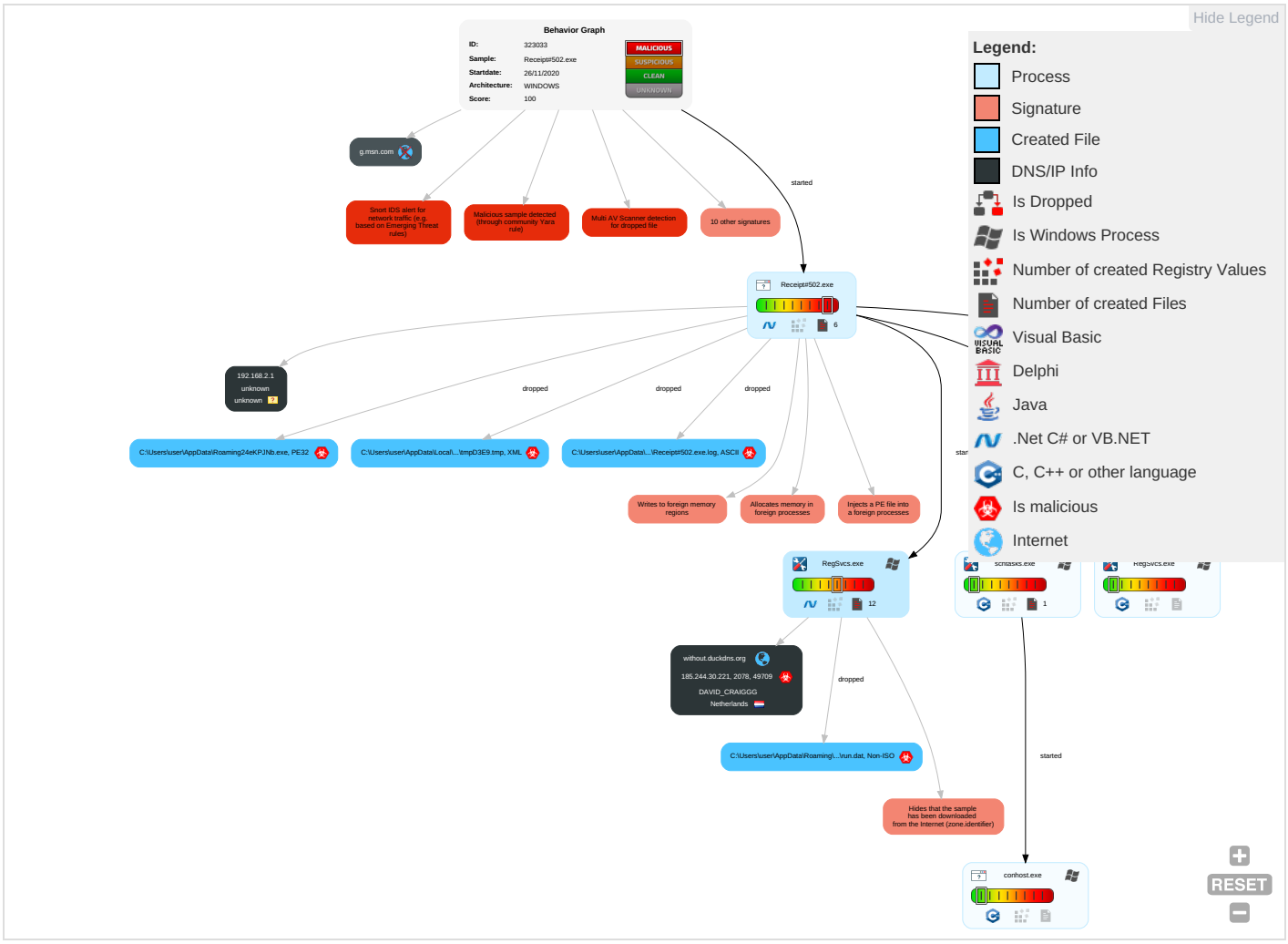
Detected Nanocore Rat

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	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir 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 Locat
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	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

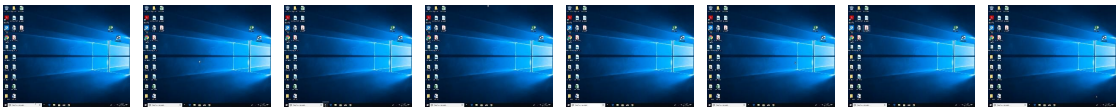
Behavior Graph



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
Receipt#502.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.Ursu	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NeKPJNb.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.Ursu	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnIT	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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.carterandcone.comes	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiv	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-uGu	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.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	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.fontbureau.comldF	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.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comasv	0%	Avira URL Cloud	safe	
http://www.monotype.m	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/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/O	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.carterandcone.comn-uh	0%	Avira URL Cloud	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.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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.founder.com.cn/cnteI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/Z	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Z	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	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	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.carterandcone.comu	0%	Avira URL Cloud	safe	
http://www.carterandcone.coms	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.carterandcone.coma-e	0%	Avira URL Cloud	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.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/w	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/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
without.duckdns.org	185.244.30.221	true	true		unknown
g.msn.com	unknown	unknown	false		high

URLs from Memory and Binaries

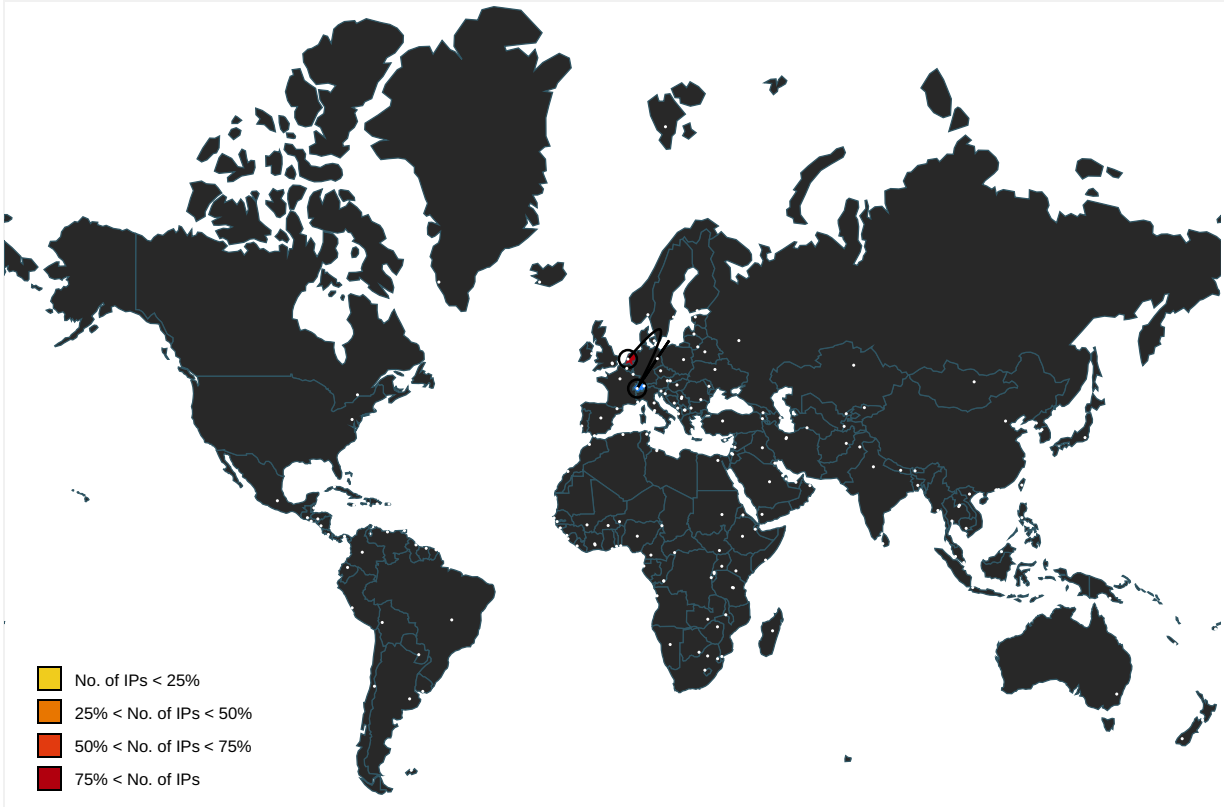
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnIT	Receipt#502.exe, 00000000.00000003.237720086.0000000004F8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comes	Receipt#502.exe, 00000000.00000003.238614597.0000000004F7400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comsiv	Receipt#502.exe, 00000000.00000003.241721705.0000000004F7200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-uGu	Receipt#502.exe, 00000000.00000003.238533764.0000000004F7400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comessed	Receipt#502.exe, 00000000.00000003.241721705.0000000004F7200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Receipt#502.exe, 00000000.00000003.238406656.0000000004F7200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comldF	Receipt#502.exe, 00000000.00000003.240885938.0000000004F7200.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersers	Receipt#502.exe, 00000000.00000003.241659047.0000000004FA500.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersx=	Receipt#502.exe, 00000000.00000003.241857098.0000000004FA500.00000004.00000001.sdmp	false		high
http://www.fontbureau.comasv	Receipt#502.exe, 00000000.00000003.251857385.0000000004F7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.m	Receipt#502.exe, 00000000.00000003.243733741.0000000004FA900.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersd	Receipt#502.exe, 00000000.00000003.240614990.0000000004FA500.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Receipt#502.exe, 00000000.00000003.239418396.0000000004F7C00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/O	Receipt#502.exe, 00000000.00000003.239418396.0000000004F7C00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comn-uh	Receipt#502.exe, 00000000.00000003.238422196.0000000004F7900.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.	Receipt#502.exe, 00000000.00000003.238273524.0000000004F8600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersn	Receipt#502.exe, 00000000.00000003.241857098.0000000004FA500.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnttel	Receipt#502.exe, 00000000.00000003.237720086.0000000004F8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/Z	Receipt#502.exe, 00000000.00000003.239418396.0000000004F7C00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnd	Receipt#502.exe, 00000000.00000003.237743636.000000000114B00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Z	Receipt#502.exe, 00000000.00000003.239054630.0000000004F7500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Receipt#502.exe, 00000000.00000003.240885938.0000000004F7200.00000004.00000001.sdmp	false		high
http://www.fontbureau.comF	Receipt#502.exe, 00000000.00000003.241721705.0000000004F7200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comd	Receipt#502.exe, 00000000.00000003.238614597.0000000004F7400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	Receipt#502.exe, 00000000.00000003.239418396.0000000004F7C00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/H	Receipt#502.exe, 00000000.00000003.239054630.0000000004F7500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comu	Receipt#502.exe, 00000000.00000003.238533764.0000000004F7400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coms	Receipt#502.exe, 00000000.00000003.238533764.0000000004F7400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Receipt#502.exe, 00000000.00000003.239054630.0000000004F7500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coma-e	Receipt#502.exe, 00000000.00000003.238533764.0000000004F7400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	Receipt#502.exe, 00000000.00000003.251857385.0000000004F7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	Receipt#502.exe, 00000000.00000003.241721705.0000000004F7200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/?	Receipt#502.exe, 00000000.00000003.239418396.0000000004F7C00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/w	Receipt#502.exe, 00000000.00000003.239054630.0000000004F7500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Receipt#502.exe, 00000000.00000002.256398475.000000000512000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers-	Receipt#502.exe, 00000000.00000003.240941777.0000000004FA500.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	Receipt#502.exe, 00000000.0000 0002.256398475.000000000512000 0.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/r	Receipt#502.exe, 00000000.0000 0003.239054630.0000000004F7500 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.monotype.	Receipt#502.exe, 00000000.0000 0003.242763996.0000000004FA500 0.00000004.00000001.sdmp, Rece ipt#502.exe, 00000000.00000003 .242740004.0000000004FA5000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	Receipt#502.exe, 00000000.0000 0003.251857385.0000000004F7000 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Receipt#502.exe, 00000000.0000 0003.239054630.0000000004F7500 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	Receipt#502.exe, 00000000.0000 0003.238223808.0000000004F8300 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Receipt#502.exe, 00000000.0000 0002.256398475.000000000512000 0.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/h	Receipt#502.exe, 00000000.0000 0003.239418396.0000000004F7C00 0.00000004.00000001.sdmp	false		unknown
http://www.carterandcone.comtrWv	Receipt#502.exe, 00000000.0000 0003.238614597.0000000004F7400 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Receipt#502.exe, 00000000.0000 0003.240647661.0000000004FA500 0.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers$=	Receipt#502.exe, 00000000.0000 0003.241659047.0000000004FA500 0.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersf=	Receipt#502.exe, 00000000.0000 0003.241049835.0000000004FA500 0.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.30.221	unknown	Netherlands		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323033
Start date:	26.11.2020
Start time:	08:33:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Receipt#502.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:	24
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@8/8@2/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 92.122.144.200, 104.43.139.144, 51.11.168.160, 52.147.198.201, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.103.5.159, 104.43.193.48, 52.142.114.176, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net • 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
08:34:25	API Interceptor	2x Sleep call for process: Receipt#502.exe modified
08:34:29	API Interceptor	1018x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	New PO 64739 (UK).exe	Get hash	malicious	Browse	• 185.140.53.207
	90987948.exe	Get hash	malicious	Browse	• 185.244.30.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 185.140.53.149
	PO456789.exe	Get hash	malicious	Browse	• 185.244.30.212
	kelvinx.exe	Get hash	malicious	Browse	• 185.140.53.132
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Receipt#502.exe.log

Process:	C:\Users\user\Desktop\Receipt#502.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\tmpD3E9.tmp

Process:	C:\Users\user\Desktop\Receipt#502.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.172014291604984
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBNETltn:cbhC7ZlNQF/rydbz9I3YODOLNdq3sS
MD5:	F033691D15512FA356BEDDA42A45D54B
SHA1:	5B87117DDF17EC4B3E69080974D503997D1603D3
SHA-256:	B80844A420C52AC3E1ADF3778CB3F173BBF7904D87273DA4C7DAEAE2130FF74E
SHA-512:	8EC8BA2E4675657A6494E51BED3A5E65848F7396BE907DE7DDD2D6C939A77C92890DDC2CB6A5862D3A446E7AC1D77A913660229C9F6E589A4764359097F463D
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp	
Reputation:	low
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>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385 1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.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:am:am
MD5:	36331463881AC56549683D2481AC3E0C
SHA1:	35AD2749C9954148597145788A856ACE95B7A02E
SHA-256:	D7D3BDD45709C39129DD43B58A1DDC433AF3BA02A7F7771BB71803692E2440C2
SHA-512:	679A30939F5E3BE3404D283AC743A27DB5840C815787A7805346D56203E542AD1BB32D2C0027B766D4069647B461EB8323CBA207490823CFBA013A375EA9C0DA
Malicious:	**true**
Reputation:	low
Preview:	..v%)..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	64

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\NeKPJNb.exe	
Process:	C:\Users\user\Desktop\Receipt#502.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	696832
Entropy (8bit):	7.224549357162399
Encrypted:	false
SSDEEP:	12288:lb4JO3lL2iNNOhnc4PrvIpMdd2lBKiIQulBt8LFSERr:lb4JO3lL1XWHv9dd2lEiIQ0P88E
MD5:	E2E26573196FD444C8845D29E73A6B00
SHA1:	8A2FC9E82C11D234E74846451B12C73D69DEA955
SHA-256:	40FE69BE55041A8607BF2596D0FA649AB26F6D6BD6973FB955F14F4E8A066B6C
SHA-512:	02906FAFFE3BB49E0A936F5D07215FFE8B7CC28B2F65536E17B1B6204AA7966998B4A70BB09BF5A1FDFAA6EFEF6F729FBEABB1A2E3C540CD1965F73EDABC8B78
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0..... ... .@.. .....@..@.....O.... ..<..... ....H.....text... ....`.rsrc...<.... .....@..@.reloc.....@..B.....H.....r...c.....x.....F.....0..G.....}.....(.....(.....s....}.....{.....o.....(.....{.....{....o.....*..0.....(.....{....{.....(.....~....vl.....,..{....{....o.....{....{.....o....o.....{....(....}.....o.....3..{....{....o.....+....,@..{....{....o....s.....{.....{....{....o.....{....{....o.....*...{....(....o ....{....~....o!....*...{....("...o ....{....~....o!....*...0..+.....,..{.....+.....,..{.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.224549357162399

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Receipt#502.exe
File size:	696832
MD5:	e2e26573196fd444c8845d29e73a6b00
SHA1:	8a2fc9e82c11d234e74846451b12c73d69dea955
SHA256:	40fe69be55041a8607bf2596d0fa649ab26f6d6bd6973fb955f14f4e8a066b6c
SHA512:	02906faffe3bb49e0a936f5d07215ffe8b7cc28b2f65536e17b1b6204aa7966998b4a70bb09bf5a1fdfaa6efef6f729fbeabb1a2e3c540cd1965f73edabc8b78
SSDEEP:	12288:lb4JO3lL2iNNOhnc4PrvIpMdd2lBKiIQulBt8LFSERr:lb4JO3lL1XWHv9dd2lEiIQ0P88E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0..... ... .@.. .....@.....

File Icon

Icon Hash:	68f0e46cecf4e1e3

Static PE Info

General

Entrypoint:	0x481c1a
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:	0x5FBEF892 [Thu Nov 26 00:36:34 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x81bc8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x29f3c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	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	0x7fc20	0x7fe00	False	0.842004979228	data	7.75101312154	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x29f3c	0x2a000	False	0.128830682664	data	4.0760655749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	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	0x822b0	0x1f33	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x841e4	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x94a0c	0x94a8	data		
RT_ICON	0x9deb4	0x5488	data		
RT_ICON	0xa333c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 47359, next used block 4282318848		
RT_ICON	0xa7564	0x25a8	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa9b0c	0x10a8	data		
RT_ICON	0xaabb4	0x988	data		
RT_ICON	0xab53c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xab9a4	0x84	data		
RT_VERSION	0xaba28	0x328	data		
RT_MANIFEST	0xabd50	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

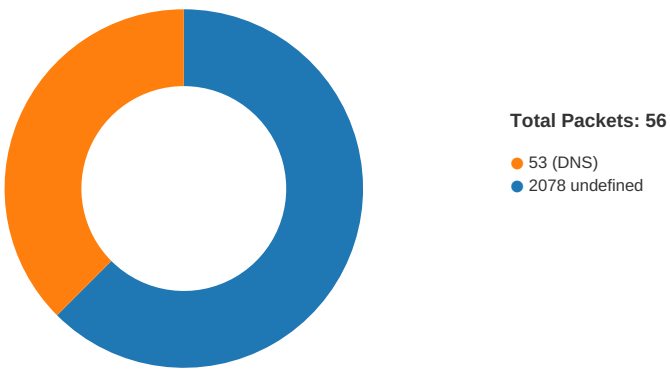
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 - 2020
Assembly Version	1.0.0.0
InternalName	Wd.exe
FileVersion	1.0.0.0
CompanyName	Vendetta Inc.
LegalTrademarks	
Comments	
ProductName	Aku Form
ProductVersion	1.0.0.0
FileDescription	Aku Form
OriginalFilename	Wd.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-08:34:31.641727	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	2078	192.168.2.5	185.244.30.221

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:34:31.474524975 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:31.582503080 CET	2078	49709	185.244.30.221	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:34:31.583118916 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:31.641726971 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:31.797629118 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:31.797771931 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:31.826636076 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:31.868154049 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:31.966736078 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:31.966922998 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.075277090 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.099747896 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.362883091 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.363248110 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.363298893 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.363347054 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.363384008 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.363431931 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.363519907 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.477133989 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.477185965 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.477261066 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.477319956 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.485071898 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.485132933 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.485179901 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.485254049 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.485286951 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.486920118 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.491051912 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.491157055 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.585505009 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.585623026 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.585702896 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.585853100 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.585900068 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.586067915 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.595840931 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.595899105 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596014023 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.596139908 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596177101 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596225977 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596241951 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.596275091 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596330881 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.596467018 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596515894 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.596566916 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.607662916 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.607717037 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.607781887 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.608422995 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.608700991 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.608805895 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.698178053 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.698373079 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.698409081 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.698502064 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.701559067 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.701848030 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.701894045 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.701953888 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.701992035 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702028990 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702042103 CET	49709	2078	192.168.2.5	185.244.30.221

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:34:32.702084064 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.702620029 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702658892 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702713966 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.702797890 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702914953 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702986002 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.702991009 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.703022957 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703108072 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.703111887 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703165054 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703200102 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703236103 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.703238010 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703274965 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703295946 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.703497887 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703538895 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703571081 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.703905106 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.703967094 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.704054117 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.704082966 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.704195976 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.720489025 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.720604897 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.720650911 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.720725060 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.720916033 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.721002102 CET	49709	2078	192.168.2.5	185.244.30.221
Nov 26, 2020 08:34:32.725481033 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.725653887 CET	2078	49709	185.244.30.221	192.168.2.5
Nov 26, 2020 08:34:32.725687981 CET	2078	49709	185.244.30.221	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:34:31.242402077 CET	62176	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:31.444324017 CET	53	62176	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:35.602926970 CET	59596	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:35.640588045 CET	53	59596	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:37.237322092 CET	65296	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:37.264524937 CET	53	65296	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:39.862066984 CET	63183	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:39.889306068 CET	53	63183	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:51.537843943 CET	60151	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:51.564810991 CET	53	60151	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:52.348002911 CET	56969	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:52.374954939 CET	53	56969	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:54.386253119 CET	55161	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:54.413346052 CET	53	55161	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:55.135413885 CET	54757	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:55.162417889 CET	53	54757	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:57.774050951 CET	49992	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:57.809693098 CET	53	49992	8.8.8.8	192.168.2.5
Nov 26, 2020 08:34:59.455619097 CET	60075	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:34:59.482768059 CET	53	60075	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:03.161185980 CET	55016	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:03.188561916 CET	53	55016	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:05.595487118 CET	64345	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:05.630959988 CET	53	64345	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:06.143502951 CET	57128	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:06.179116964 CET	53	57128	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:35:09.619523048 CET	54791	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:09.655287981 CET	53	54791	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:10.323987961 CET	50463	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:10.351022005 CET	53	50463	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:10.471493959 CET	50394	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:10.498734951 CET	53	50394	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:13.485687017 CET	58530	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:13.536479950 CET	53	58530	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:15.625456095 CET	53813	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:15.660779953 CET	53	53813	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:15.928908110 CET	63732	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:15.975043058 CET	53	63732	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:17.544102907 CET	57344	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:17.571263075 CET	53	57344	8.8.8.8	192.168.2.5
Nov 26, 2020 08:35:45.001585007 CET	54450	53	192.168.2.5	8.8.8.8
Nov 26, 2020 08:35:45.028789043 CET	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 08:34:31.242402077 CET	192.168.2.5	8.8.8.8	0xd3a8	Standard query (0)	without.duckdns.org	A (IP address)	IN (0x0001)
Nov 26, 2020 08:35:13.485687017 CET	192.168.2.5	8.8.8.8	0xd558	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

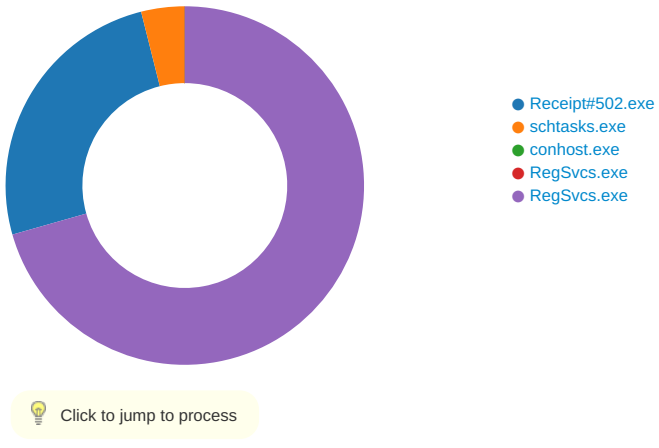
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 08:34:31.444324017 CET	8.8.8.8	192.168.2.5	0xd3a8	No error (0)	without.duckdns.org		185.244.30.221	A (IP address)	IN (0x0001)
Nov 26, 2020 08:35:13.536479950 CET	8.8.8.8	192.168.2.5	0xd558	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Receipt#502.exe PID: 4636 Parent PID: 5656

General

Start time:	08:34:20
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\Receipt#502.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Receipt#502.exe'
Imagebase:	0x560000
File size:	696832 bytes
MD5 hash:	E2E26573196FD444C8845D29E73A6B00
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: 00000000.00000002.254057757.0000000003CD8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254057757.0000000003CD8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254057757.0000000003CD8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.254741913.0000000003EC2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254741913.0000000003EC2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254741913.0000000003EC2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.253473397.0000000002D49000.00000004.00000001.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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\NeKPJNb.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7F50717	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	DEB2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Receipt#502.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp	success or wait	1	7F5138E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\NeKPJNb.exe	unknown	696832	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 92 f8 be 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 fe 07 00 00 a2 02 00 00 00 00 00 1a 1c 08 00 00 20 00 00 00 20 08 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 e0 0a 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......_.......... ....0.................. ... .@.. ....@.................	success or wait	1	7F5099F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp	unknown	1644	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 61 6c 66 6f 6e 73 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 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationI	success or wait	1	7F5099F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Receipt#502.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	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\Receipt#502.exe	unknown	696832	success or wait	1	7F5099F	ReadFile

Analysis Process: schtasks.exe PID: 1384 Parent PID: 4636

General

Start time:	08:34:26
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NeKPJNb' /XML 'C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp'
Imagebase:	0xa10000
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\tmpD3E9.tmp	unknown	2	success or wait	1	A1AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD3E9.tmp	unknown	1645	success or wait	1	A1ABD9	ReadFile

Analysis Process: conhost.exe PID: 1140 Parent PID: 1384

General

Start time:	08:34:27
Start date:	26/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RegSvcs.exe PID: 5476 Parent PID: 4636

General

Start time:	08:34:27
Start date:	26/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1e0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 5480 Parent PID: 4636

General

Start time:	08:34:28
Start date:	26/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7ff64e5e0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000005.00000003.261720988.0000000004293000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	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	72B860AC	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	51307A1	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	513089B	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	51307A1	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	51307A1	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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	513089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	513089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	513089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	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	5132E94	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	12CBF0E	DeleteFileW

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	2e d0 76 25 29 92 d8 48	..v%)..H	success or wait	1	5130A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	1	5130A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426832	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^._.....B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	5130A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	2	5130A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	1	5132E94	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	4	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5130A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5130A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	5130A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	5130A53	ReadFile

Disassembly

Code Analysis