ID: 357256
Sample Name: receipt.exe
Cookbook: default.jbs
Time: 10:51:33
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

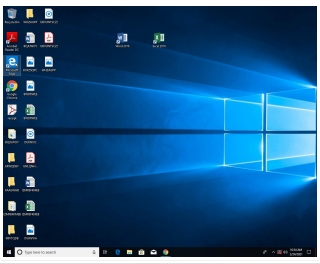
Analysis Report receipt.exe

Overview

General Information

Sample Name:	receipt.exe
Analysis ID:	357256
MD5:	a4a4bc6e3283ec..
SHA1:	2114e1c9fbbc3ff…
SHA256:	962debf4655a791.
Tags:	exe NanoCore RAT USPS
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

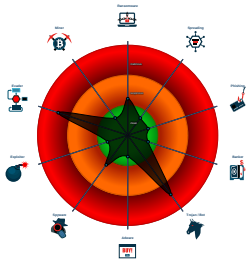
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Icon mismatch, binary includes an ic…
- 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 Nanocore RAT
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- receipt.exe (PID: 7032 cmdline: 'C:\Users\user\Desktop\receipt.exe' MD5: A4A4BC6E3283ECC66CD4A4DC864ACD9A)
  - schtasks.exe (PID: 5728 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CjkDta' /XML 'C:\Users\user\AppData\Local\Temp\tmp15FF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6664 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - RegSvcs.exe (PID: 6632 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
- dhcpmon.exe (PID: 6296 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.698303043.0000000003F26000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x9d885:$x1: NanoCore.ClientPluginHost • 0x9d8c2:$x2: IClientNetworkHost • 0xa13f5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.698303043.0000000003F26000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.698303043.0000000003F26000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x9d5ed:$a: NanoCore • 0x9d5fd:$a: NanoCore • 0x9d831:$a: NanoCore • 0x9d845:$a: NanoCore • 0x9d885:$a: NanoCore • 0x9d64c:$b: ClientPlugin • 0x9d84e:$b: ClientPlugin • 0x9d88e:$b: ClientPlugin • 0x9d773:$c: ProjectData • 0x9e17a:$d: DESCrypto • 0xa5b46:$e: KeepAlive • 0xa3b34:$g: LogClientMessage • 0x9fd2f:$i: get_Connected • 0x9e4b0:$j: #=q • 0x9e4e0:$j: #=q • 0x9e4fc:$j: #=q • 0x9e52c:$j: #=q • 0x9e548:$j: #=q • 0x9e564:$j: #=q • 0x9e594:$j: #=q • 0x9e5b0:$j: #=q
00000000.00000002.695413546.0000000003A98000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1fe0ad:$x1: NanoCore.ClientPluginHost • 0x1fe0ea:$x2: IClientNetworkHost • 0x201c1d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.695413546.0000000003A98000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.receipt.exe.3c85f20.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.receipt.exe.3c85f20.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.receipt.exe.3c85f20.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.receipt.exe.3c85f20.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.receipt.exe.3c85f20.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 8 entries				

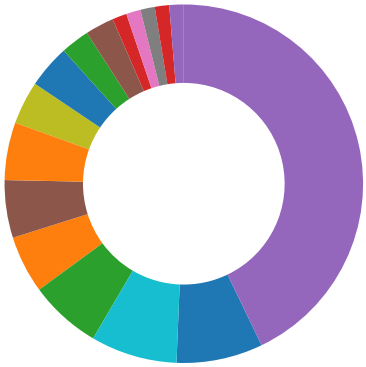
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

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

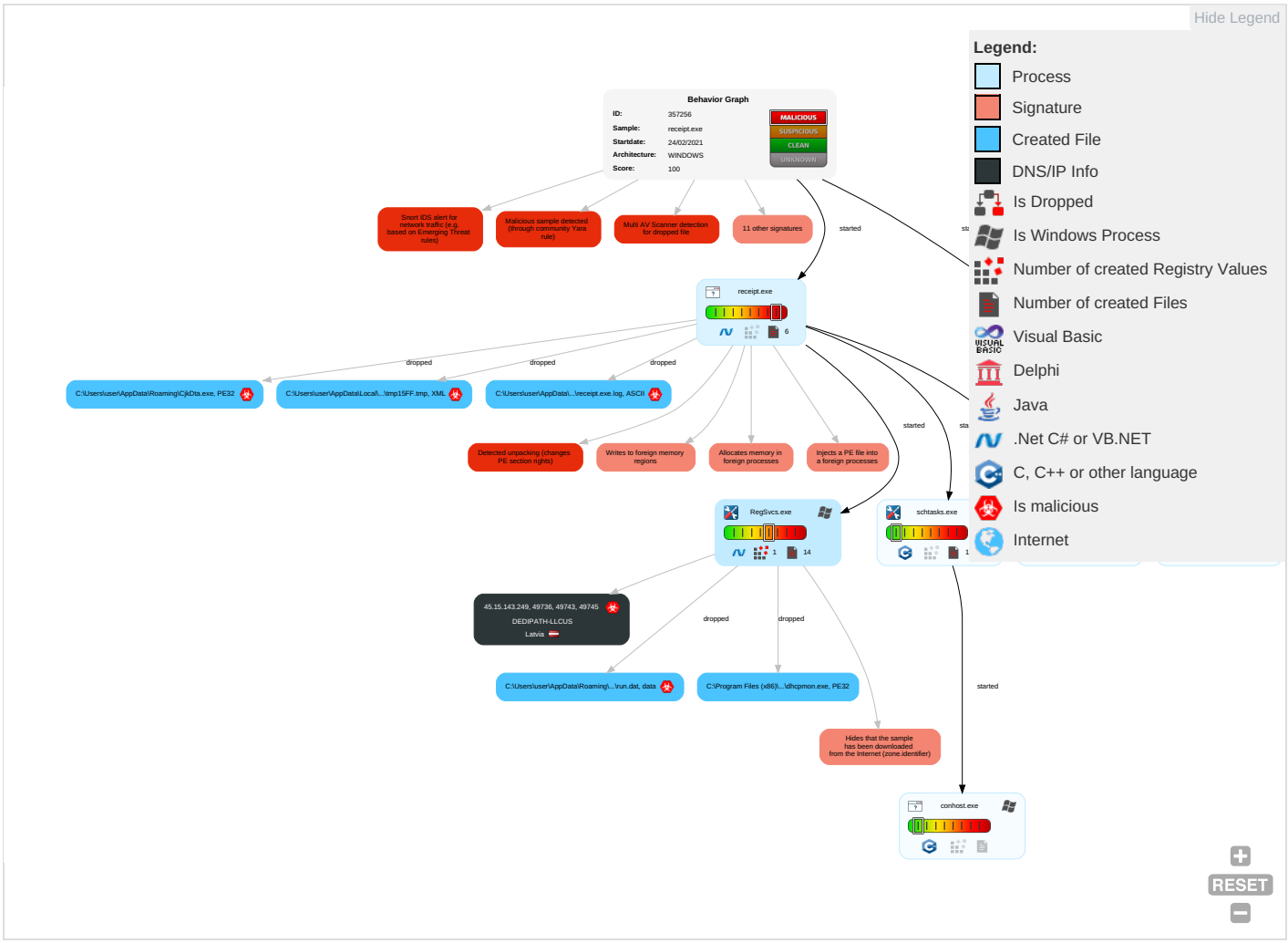
Yara detected Nanocore RAT

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 2	OS Credential Dumping	Security Software Discovery 1 3	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Process Injection 3 1 1	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	DLL Side-Loading 1	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
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	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	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 4	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/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
receipt.exe	43%	Virustotal		Browse
receipt.exe	31%	ReversingLabs	Win32.Trojan.Wacatac	
receipt.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CjkDta.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\CjkDta.exe	31%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.receipt.exe.410000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTF	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sakkal.comt=	0%	Avira URL Cloud	safe	
http://www.tiro.comN==0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/anaz	0%	Avira URL Cloud	safe	
http://www.urwpp.deFTm=	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.comepko	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.founder.com.cn/cn:	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0tr	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTN(	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/;	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.comldu	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.carterandcone.comel	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deN==0	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	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.com=	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.fontbureau.coml	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiva	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	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.jiyu-kobo.co.jp/V	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/I	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldf;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/C	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.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/I	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

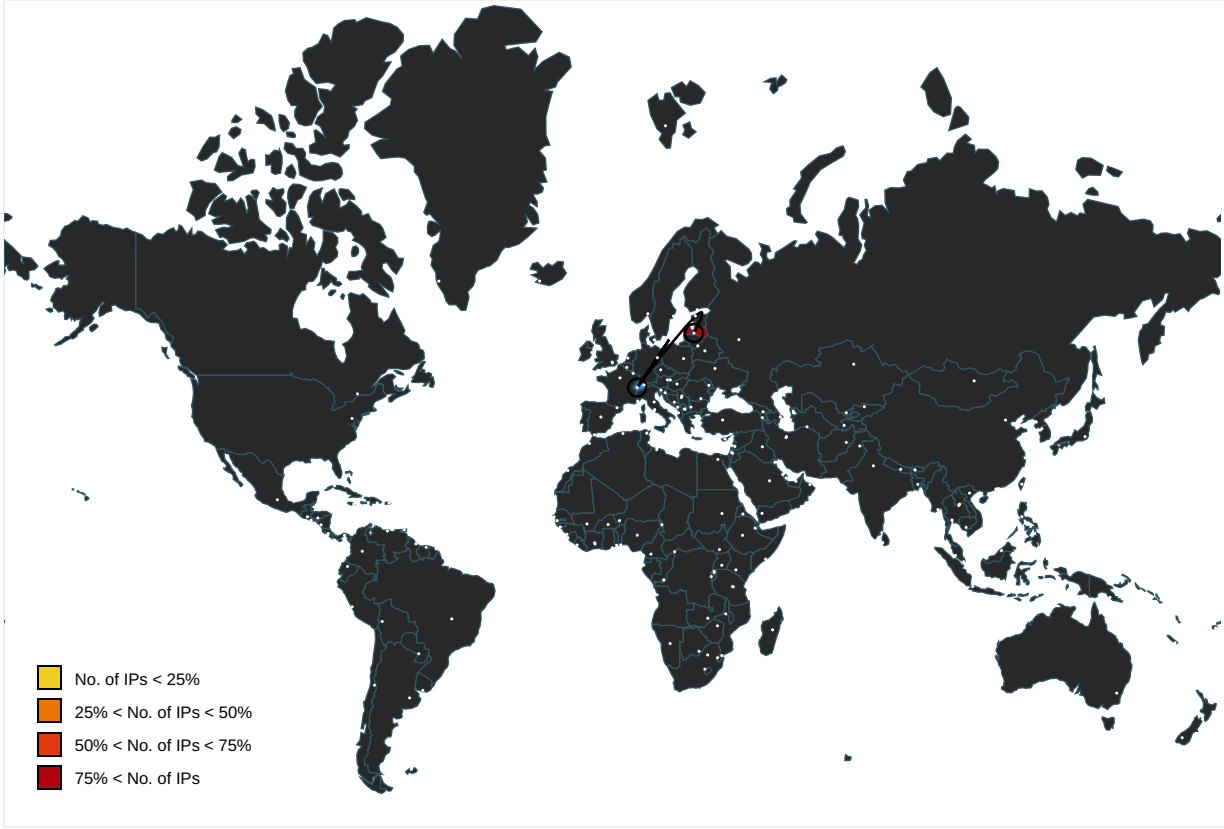
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.coml.TTF	receipt.exe, 00000000.00000003.653972981.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comt=	receipt.exe, 00000000.00000003.649702876.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.comN==0	receipt.exe, 00000000.00000003.648660858.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers?	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersE	receipt.exe, 00000000.00000003.655160906.00000000052BF000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/anaz	receipt.exe, 00000000.00000003.649726282.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deFTm=	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comepko	receipt.exe, 00000000.00000002.699420600.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn:	receipt.exe, 00000000.00000003.647614140.00000000052AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0tr	receipt.exe, 00000000.00000003.649726282.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	receipt.exe, 00000000.00000003.648538472.00000000052B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersP	receipt.exe, 00000000.00000003.651625918.00000000052BF000.00000004.00000001.sdmp, receipt.exe, 00000000.00000003.651542933.00000000052BF000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnTN(	receipt.exe, 00000000.00000003.647816511.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com.	receipt.exe, 00000000.00000003.648039451.00000000052B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comalsF	receipt.exe, 00000000.00000003.654868204.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coml1	receipt.exe, 00000000.00000003.651507255.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/;	receipt.exe, 00000000.00000003.649569000.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers_	receipt.exe, 00000000.00000003.651099578.00000000052BF000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/	receipt.exe, 00000000.00000003.651051823.00000000052AE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comldu	receipt.exe, 00000000.00000002.699420600.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comel	receipt.exe, 00000000.00000003.648538472.00000000052B4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/%	receipt.exe, 00000000.00000003.649569000.00000000052B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kr	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deN==0	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deDPlease	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	receipt.exe, 00000000.00000003.648039451.00000000052B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com=	receipt.exe, 00000000.00000003.652761536.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coma	receipt.exe, 00000000.00000003.648097931.00000000052B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coml	receipt.exe, 00000000.00000002.699420600.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsiva	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	receipt.exe, 00000000.00000003.653972981.00000000052AE000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	receipt.exe, 00000000.00000003.656612702.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/V	receipt.exe, 00000000.00000003.649496258.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers~	receipt.exe, 00000000.00000003.654447369.00000000052BF000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/I	receipt.exe, 00000000.00000003.649726282.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comldf;	receipt.exe, 00000000.00000003.651125862.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/C	receipt.exe, 00000000.00000003.649726282.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	receipt.exe, 00000000.00000003.649726282.00000000052B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	receipt.exe, 00000000.00000003.652420790.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/l	receipt.exe, 00000000.00000003.656612702.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deC	receipt.exe, 00000000.00000003.651014423.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	receipt.exe, 00000000.00000003.647713348.00000000052AF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	receipt.exe, 00000000.00000003.652003773.00000000052AE000.00000004.00000001.sdmp, receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.come	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm;	receipt.exe, 00000000.00000003.653260424.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.monotype.	receipt.exe, 00000000.00000003.659671357.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/m	receipt.exe, 00000000.00000003.649569000.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers$	receipt.exe, 00000000.00000003.660320142.00000000052B9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comm	receipt.exe, 00000000.00000003.653972981.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	receipt.exe, 00000000.00000003.649726282.00000000052B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Curs%	receipt.exe, 00000000.00000003.649098670.00000000052B3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cno.	receipt.exe, 00000000.00000003.647991891.00000000052B4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	receipt.exe, 00000000.00000002.701125233.0000000005F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comals	receipt.exe, 00000000.00000003.655351438.00000000052AE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/d	receipt.exe, 00000000.00000003.649496258.00000000052B3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	receipt.exe, 00000000.00000003.651023261.00000000052BF000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comsief	receipt.exe, 00000000.00000003.653260424.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comE.TTF	receipt.exe, 00000000.00000003.653972981.00000000052AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.15.143.249	unknown	Latvia		35913	DEDIPATH-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357256
Start date:	24.02.2021
Start time:	10:51:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	receipt.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/11@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 7% (good quality ratio 3.5%) • Quality average: 29.8% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 80% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:52:29	API Interceptor	1x Sleep call for process: receipt.exe modified
10:52:44	API Interceptor	815x Sleep call for process: RegSvcs.exe modified
10:52:46	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.15.143.249	oMWv1Zof2y.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	oMWv1Zof2y.exe	Get hash	malicious	Browse	• 45.15.143.249
	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 193.239.147.77
	2-090000000900.exe	Get hash	malicious	Browse	• 193.239.147.103
	CHT International.exe	Get hash	malicious	Browse	• 45.145.185.209
	PO 20191003.exe	Get hash	malicious	Browse	• 45.145.185.209
	SecuriteInfo.com.Trojan.DownloaderNET.117.13478.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownloaderNET.117.10549.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownloaderNET.117.21662.exe	Get hash	malicious	Browse	• 193.239.147.103
	SecuriteInfo.com.Trojan.DownloaderNET.117.16476.exe	Get hash	malicious	Browse	• 193.239.147.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	f733jX7bkz.exe	Get hash	malicious	Browse	• 193.239.147.165
	TfRB8EdIBv.exe	Get hash	malicious	Browse	• 193.239.147.165
	AmazonSetup.exe	Get hash	malicious	Browse	• 45.145.185.40
	PO 20191003.exe	Get hash	malicious	Browse	• 45.145.185.209
	Server.exe	Get hash	malicious	Browse	• 171.22.116.126
	5tE5R0eVwq.exe	Get hash	malicious	Browse	• 45.145.185.153
	eYwQ9loD5Q.exe	Get hash	malicious	Browse	• 45.15.170.154
	SecuriteInfo.com.Trojan.Packed2.42841.8000.exe	Get hash	malicious	Browse	• 45.145.185.153
	SecuriteInfo.com.Trojan.GenericKD.36275553.12090.doc	Get hash	malicious	Browse	• 45.145.185.167
	Tax Invoice.exe	Get hash	malicious	Browse	• 139.28.235.223
	payment_slip_ receipt.doc	Get hash	malicious	Browse	• 193.239.147.103

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	oMWv1Zof2y.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
	QTxFuxF5NQ.exe	Get hash	malicious	Browse	
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	
	Vietnam Order.exe	Get hash	malicious	Browse	
	Dhl Shipping Document.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	byWuWAR5FD.exe	Get hash	malicious	Browse	
	parcel_images.exe	Get hash	malicious	Browse	
	0712020.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	zC3edqmNNt.exe	Get hash	malicious	Browse	
	Shipping Document.pdf..exe	Get hash	malicious	Browse	
	PPR & CPR_HEA_DECEMBER 4 2020.exe	Get hash	malicious	Browse	
	AdministratorDownloadsBL,.rar.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: YoWPu2BQzA9FeDd.exe, Detection: malicious, Browse • Filename: M5QDAaK9yM.exe, Detection: malicious, Browse • Filename: oMWv1Zof2y.exe, Detection: malicious, Browse • Filename: TdX45jQWjj.exe, Detection: malicious, Browse • Filename: QTxFuxF5NQ.exe, Detection: malicious, Browse • Filename: a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe, Detection: malicious, Browse • Filename: 3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe, Detection: malicious, Browse • Filename: Vietnam Order.exe, Detection: malicious, Browse • Filename: Dhl Shipping Document.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: byWuWAR5FD.exe, Detection: malicious, Browse • Filename: parcel_images.exe, Detection: malicious, Browse • Filename: 0712020.exe, Detection: malicious, Browse • Filename: JfRbEbUkpV39K4L.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: zC3edqmNNt.exe, Detection: malicious, Browse • Filename: Shipping Document.pdf..exe, Detection: malicious, Browse • Filename: PPR & CPR_HEA_DECEMBER 4 2020.exe, Detection: malicious, Browse • Filename: AdministratorDownloadsBL,.rar.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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

C:\Users\user\AppData\Local\Temp\tmp15FF.tmp	
Process:	C:\Users\user\Desktop\receipt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.173941092991223
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp15FF.tmp	
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGrtn:cbhK79lNQR/rydbz9I3YODOLNdq3S
MD5:	326073424F138CC1885296C478A8924E
SHA1:	CE52D5D40A74406D6FCAAB315E518DBBA52C70E7
SHA-256:	1DDD684BF5D1A1E85B77B51B630B021342754D36F3CD7AD13E46F1262BD62186
SHA-512:	E009D02B48E5EA00E137A84488CAFF4A05E6F6AEAD606EC5507387600845DD8EFB0FA52C4E3240FD1C7FFD21FB303F912FA57AA6747B3583E6D76AD08365CF0 2
Malicious:	**true**
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>true

C:\Users\user\AppData\Roaming\CjkDta.exe	
Process:	C:\Users\user\Desktop\receipt.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	577536
Entropy (8bit):	7.796026251145376
Encrypted:	false
SSDEEP:	12288:SncU0euEk1BdSfVfDpr26vgOIWO2UUA+4ZPZ4x07dtSvz:SGdkV2V0cSxOdtSL
MD5:	A4A4BC6E3283ECC66CD4A4DC864ACD9A
SHA1:	2114E1C9FBBC3FFA9921338E09DEFF202ABA01BF
SHA-256:	962DEBF4655A7917256AD3234217B1927A2C88AFD4631ED8258121C5B9E2DFEE
SHA-512:	B45EA70E2D6FAA54AE5FC6A26158B47A5B51C7064D85C9ED7C1F632924CC0D6A82D50D5A68D46CA7060427D59625EE4E447CC7892F8B924335CFEAC849A8A3 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....M5`.............0......@.......@...`... ....@.. ....` ............@.................................i..W.......................... .......................................................@..............`..H...........3(.G7gV..,... ....@....text........`.......2............. ..`.rsrc..............................@..@.reloc....... ....@..B............@...................... ..`... ....

<table>
<tr><th colspan="2">C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat</th></tr>
<tr><td>Process:</td><td>C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1488</td></tr>
<tr><td>Entropy (8bit):</td><td>6.997351629001838</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:IQnybgCIC9oE/3blQnybgCIC9oE/3blQnybgCIC9oE/3blQnybgCIC9oE/3blQnT:IkXCNlkXCNlkXCNlkXCNlkXCNlkXCg</td></tr>
<tr><td>MD5:</td><td>C9F2440AA7796CD29110666CC178E7F4</td></tr>
<tr><td>SHA1:</td><td>BC55644B59BE9DA50D3BE05129C2FB38A703DF6A</td></tr>
<tr><td>SHA-256:</td><td>5CAF3D80729A320F4B71B72BAEFD1096C257821EA9996A9AE4F811206B3D8307</td></tr>
<tr><td>SHA-512:</td><td>FFDBE91785DB3E47F3F4361E8CE0CD920F5B913E1F2379000555575DF40EB6747C3B0A92B5235FC54BDB3DDC48C68921EEEAFBF46BB4882F71AA889634EDBD 1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>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..+......*............S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\...X........s^.;...m/.,7X.. v"B..#.T.F L...h.....t 5.|ZGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\ ...X........s^.;...m/.,7X..v"B..#.T.F L...h.....t 5.|ZGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\...X........s^.;...m/.,7X..v"B..#.T.F L...h.....t 5.|ZGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K. &....q$.7....."....F... .N.k.C.X.D.^.....u.\...X........s^.;...m/.,7X..v"B..#.T.F L...h.....t 5.|ZGj.h\.3.</td></tr>
</table>

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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:g4V:g4V
MD5:	0DA39798C7C07335778F7D2F0F1FC776

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA1:	2979F0AA7FF28CFE7584A74C6317F94D07951BE6
SHA-256:	D636D85F4DA64AB2A21322F373E0ACA6777B89A31D778B303AD8C434E1E75FA9
SHA-512:	F148C85A2C0A80EC9E23E92CEDD5E6ED6E0CC2E7BE40CB46784B7E0348044E03149D44565184C2AB050D155A4DCEE6B9299A589666C8A1D21E4C20CE5479B3B
Malicious:	**true**
Preview:	......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:	3:9bzY6oRDlvYk:RzWDl3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
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
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
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):	433672
Entropy (8bit):	**7.9996054300907025**
Encrypted:	**true**
SSDEEP:	12288:FYbLHD8RJ3R1u49pIS86MXt8c2m6FeMlYr:Fczqr9enDXmcUBlg
MD5:	4D8AF7EC17CA5B66A617E00BB0C80481
SHA1:	EC2FE147F5370DADADFF076D4043390C7B2A45C7
SHA-256:	4251EF3033BB49F05311505FF955ED0989BA17C04F93B4DE47428A59FDFD33CB
SHA-512:	81EE1ABA97A13874A2EEC9C501633087E949C861F08E956225E44CBFF3FD61C2404DC36110D4BBBAF14D73EB3E568BE97F1947311D518290FF42C81641B332B1
Malicious:	false
Preview:	.....O.....\8..5N..`S.]..[r.$*>.\.#v&..$.....Z.i..M.Mn5.@..@...3.R..Y...}>C.b....Z.....K..^.d...Z...K.#...dn$e ..XP.^.#.....V...dB.Kn.Y.c..-k....M.D...Q.S..R.X....._...Zz...#.=<.V.NHZq.h..ON..oq.:...,7H...../..Q..R.u6.."....<.`..z.5b($..9.CF.F1...o?.h.}....;Ay....kL}7...I.-.}..D&...C....%.J..+..1.5.a..lh....s.....G..?..9^0e...p..FCvNt.e...B/...y.h.G.0..o,Q.2[.....e.P8.....yr...*..Q..*..../..S..m.....\.wA.a1.]...oW.....PY..h....f:.....Ss.....\.8...@R._A...M..X....V.f).]z..u{.z-....W...NaT+.&:...1.D../.7..\.S..z..!.....#..F.d.....*.m'.....6.2....:H...bd]..._.....}.n.=...l.7%r.>...B.Q.K..q...Ex.6.6....P..^...i...Mx...;g...,t..fCd.\.b....e{.\...Y=4.....+..T....j}..|66g.s...z...Y.kTi..?Xy...5\...SO..W.U.3A.$.l..{.D...no.E..v.2.:..a..hdhO..t.w.k..T|Po.....D?..mG.[.2.;....+...8.6.h!..w.3...w.o.....|....f.v.to.B.{`o..a.....f.cu.....?....."...u..EA...^)W..z..jtU{^.....5#....y.s.....e.l..&...%...

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145

\Device\ConDrv	
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071BE
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.796026251145376
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	receipt.exe
File size:	577536
MD5:	a4a4bc6e3283ecc66cd4a4dc864acd9a
SHA1:	2114e1c9fbbc3ffa9921338e09deff202aba01bf
SHA256:	962debf4655a7917256ad3234217b1927a2c88afd4631e8258121c5b9e2dfee
SHA512:	b45ea70e2d6faa54ae5fc6a26158b47a5b51c7064d85c9ed7c1f632924cc0d6a82d50d5a68d46ca7060427d59625ee4e447cc7892f8b924335cfeac849a8a355
SSDEEP:	12288:SncU0euEk1BdSfVfDpr26vgOIWO2UUA+4ZPZ4x07dtSvz:SGdkV2V0cSxOdtSL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....M5`.....0.....@.....@...`... ....@.. .....`.....@.....

File Icon

Icon Hash:	c4c2c4dcf4c672bc

Static PE Info

General

Entrypoint:	0x49400a
Entrypoint Section:	
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:	0x60354D8E [Tue Feb 23 18:46:38 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4

General	
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 [00494000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16914	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x80000	0x10ec8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x92000	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	0x94000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x16000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
3(G7gV	0x2000	0x12ce4	0x12e00	False	1.00040097268	data	7.99735306844	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x16000	0x68900	0x68a00	False	0.94687359991	data	7.96127820812	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x10ec8	0x11000	False	0.131333295037	data	4.37885859623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x92000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x94000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x80130	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x90958	0x14	data		
RT_VERSION	0x9096c	0x36c	data		
RT_MANIFEST	0x90cd8	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 Neudesic 2017
Assembly Version	1.0.0.0
InternalName	CsY.exe
FileVersion	1.0.0.0
CompanyName	Neudesic
LegalTrademarks	
Comments	
ProductName	VectorBasedDrawing
ProductVersion	1.0.0.0
FileDescription	VectorBasedDrawing
OriginalFilename	CsY.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-10:52:47.506328	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	7890	192.168.2.4	45.15.143.249
02/24/21-10:52:53.781107	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:00.216165	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:07.041786	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:13.112569	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:19.175131	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	7890	192.168.2.4	45.15.143.249

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-10:53:25.317441	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:31.414875	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:37.354295	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:43.292313	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:49.283746	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	7890	192.168.2.4	45.15.143.249
02/24/21-10:53:55.488604	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	7890	192.168.2.4	45.15.143.249
02/24/21-10:54:01.591516	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	7890	192.168.2.4	45.15.143.249
02/24/21-10:54:07.590336	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	7890	192.168.2.4	45.15.143.249
02/24/21-10:54:13.590416	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	7890	192.168.2.4	45.15.143.249
02/24/21-10:54:19.562525	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	7890	192.168.2.4	45.15.143.249
02/24/21-10:54:25.518443	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	7890	192.168.2.4	45.15.143.249

TCP Packets

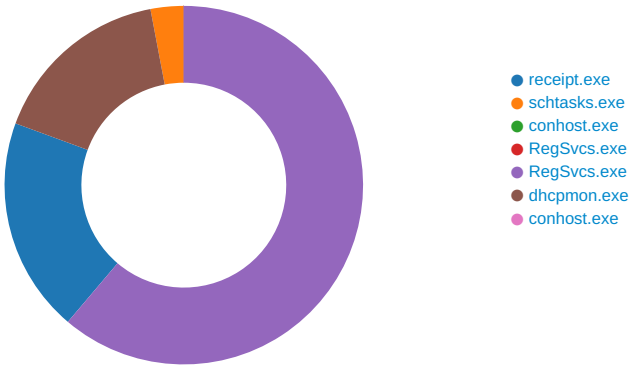
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 10:52:47.067248106 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:47.190197945 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:47.190323114 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:47.506328106 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:47.647924900 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:47.648315907 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:47.829463005 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:47.829793930 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:47.952914000 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:47.964724064 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.137679100 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.137999058 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.313610077 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.313962936 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.349737883 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.349807978 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.349838972 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.349867105 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.353349924 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.353440046 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.476177931 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.476227045 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.476253033 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.476275921 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.477191925 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.477231979 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.477247953 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.477256060 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.477267027 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.477278948 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.478059053 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.478080034 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.599980116 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600017071 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600033045 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600052118 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600069046 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600090027 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600107908 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600158930 CET	7890	49736	45.15.143.249	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 10:52:48.600222111 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.600240946 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.600438118 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600464106 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600508928 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600533962 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.600608110 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.600617886 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.601325989 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.603724957 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.603760004 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.603771925 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.603789091 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.604517937 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.722706079 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722738028 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722755909 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722771883 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722789049 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722809076 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722816944 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.722840071 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.722891092 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.722954988 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.722985029 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723020077 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723037958 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723069906 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723104000 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723133087 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723144054 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723220110 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723268032 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723305941 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723330975 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723335028 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723346949 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723387957 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723402023 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723454952 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723465919 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723476887 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723505020 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723521948 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.723607063 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.723614931 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.724112034 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.727200985 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727231979 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727247953 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727307081 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727350950 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727384090 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727410078 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.727421999 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.727421999 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727442026 CET	7890	49736	45.15.143.249	192.168.2.4
Feb 24, 2021 10:52:48.727473021 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.727477074 CET	49736	7890	192.168.2.4	45.15.143.249
Feb 24, 2021 10:52:48.727910042 CET	49736	7890	192.168.2.4	45.15.143.249

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: receipt.exe PID: 7032 Parent PID: 5824

General

Start time:	10:52:20
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\receipt.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\receipt.exe'
Imagebase:	0x410000
File size:	577536 bytes
MD5 hash:	A4A4BC6E3283ECC66CD4A4DC864ACD9A
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: 00000000.00000002.698303043.0000000003F26000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.698303043.0000000003F26000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.698303043.0000000003F26000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.695413546.0000000003A98000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.695413546.0000000003A98000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.695413546.0000000003A98000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\CjkDta.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4CE17C7	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp15FF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4CE0084	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\receipt.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp15FF.tmp	success or wait	1	4CE243E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\CjkDta.exe	unknown	577536	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 05 00 8e 4d 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 8c 06 00 00 40 02 00 00 00 00 00 0a 40 09 00 00 60 01 00 00 20 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 09 00 00 04 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....M5`.......... ....0......@.......@...`... .. ..@.. ....` ....@.................	success or wait	1	4CE1A4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp15FF.tmp	unknown	1639	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 6a 6f 6e 65 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 6e	<?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>.. </RegistrationIn	success or wait	1	4CE1A4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\receipt.exe.log	unknown	525	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	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Users\user\Desktop\receipt.exe	unknown	577536	success or wait	1	4CE1A4F	ReadFile

Analysis Process: schtasks.exe PID: 5728 Parent PID: 7032

General

Start time:	10:52:41
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CjkDta' /XML 'C:\Users\user\AppData\Local\Temp\tmp15FF.tmp'
Imagebase:	0xba0000
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\tmp15FF.tmp	unknown	2	success or wait	1	BAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp15FF.tmp	unknown	1640	success or wait	1	BAABD9	ReadFile

Analysis Process: conhost.exe PID: 5720 Parent PID: 5728

General

Start time:	10:52:42
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6664 Parent PID: 7032

General

Start time:	10:52:42
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x300000
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: 6632 Parent PID: 7032

General

Start time:	10:52:43
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa70000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	722760AC	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	722760AC	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	52A07A1	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	52A089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52A07A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	52A0B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52A07A1	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	52A07A1	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	722760AC	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	722760AC	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	52A089B	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	52A089B	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	52A089B	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 | synchronous io non alert | non directory file	success or wait	1	52A0B20	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	109BF0E	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	07 e6 1d ef a9 d8 d8 48	.....H	success or wait	1	52A0A53	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe</td><td>0</td><td>32768</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 b1 5b 01 00 03 00 40 05 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</td><td>MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@................ ....</td><td>success or wait</td><td>1</td><td>52A0B20</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat</td><td>unknown</td><td>248</td><td>47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 b0 f9 9a 0b bd fc a3 d0 89 94 e6 53 d6 54 79 e5 83 4b bd 26 f1 d3 e4 a5 0f 71 24 9d 37 8d c1 a6 ba 0b 22 a1 1d 8d d0 9e 46 9f bd 17 20 0e 4e f1 a8 6b f1 b9 43 97 58 c6 44 f7 5e 10 ed 12 fe f6 75 cd 5c 8e ed a5 d3 92 58 10 b2 7f 1d d3 8d b3 7f e2 73 5e ee 3b 9a 2e bf 6d 2f e7 2c 37 58 01 ca 83 76 22 42 ea 7f 23 e5 54 1d 46 20 4c ef 97 83 9f ba 68 f7 9f c2 8f a7 87 74 20 35 1d 7c 5a</td><td>Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b........4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+......*.... ....S.Ty..K.&.....q$.7. ...."......F... .N..k..C.X.D.^. ....u.\.....X.........s^.;...m /.,7X...v"B..#.T.F L.....h.... ..t 5.|Z</td><td>success or wait</td><td>1</td><td>52A0A53</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	433672	f5 ec cd 01 d2 e1 d2 c2 10 4f 02 de b7 c5 8d 0e b8 e2 19 5c 38 e3 e0 35 4e a8 a9 60 53 d0 5d ea fb 5b 72 f8 24 2a 3e c2 5c 94 23 76 26 f9 84 24 a5 d6 19 d8 c7 df f6 5a ef bd 69 f7 86 4d e9 4d 6e 35 1d 40 e8 d2 40 bd 10 97 33 fa 52 d1 b7 cb 59 d9 ac b5 d9 7d 3e 43 1e 62 92 ed 0a 8b 5a bc da c3 e6 d4 08 cb e5 4b 98 ac 5e ac 64 d2 e7 fd 5a ef fe 13 4b a8 23 af e7 1b 64 6e 24 65 20 0d 9e 58 50 02 5e fc 23 cc d5 bd ae 8a ea 17 d0 56 95 c5 12 64 42 ad 4b 6e e4 59 af 63 0b e6 2d 6b c5 07 18 d2 89 4d 0c 44 d0 8a 0a ac 51 de 53 87 bc 52 ca ad 58 8d 8f 0e e2 17 05 ec 19 f0 1a 5f f4 b2 bd 5a 7a b1 e5 b8 d0 23 08 3d 3c 08 56 e3 4e 48 5a 71 cc b9 68 99 13 4f 4e a3 dd 6f 71 c1 3a c5 18 1f 2c 37 48 da 07 f3 d0 f0 90 e6 2f fc ba 51 c3 d0 bf 52 1b 75 36 19 dd 81 22 b2 c4	.....O.....\8..5N..`S.]..[r.$*>.\.#v&..$.....Z..i..M.Mn5.@..@...3.R...Y....}>C.b....Z.....K..^.d...Z...K.#...dn$e ..XP.^.#.....V...dB.Kn.Y.c..-k.....M.D....Q.S..R..X....._...Zz....#.=<.V.NHZq..h..ON..oq.:...,7H...../..Q...R.u6..."..	success or wait	1	52A0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	248	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 b0 f9 9a 0b bd fc a3 d0 89 94 e6 53 d6 54 79 e5 83 4b bd 26 f1 d3 e4 a5 0f 71 24 9d 37 8d c1 a6 ba 0b 22 a1 1d 8d d0 9e 46 9f bd 17 20 0e 4e f1 a8 6b f1 b9 43 97 58 c6 44 f7 5e 10 ed 12 fe f6 75 cd 5c 8e ed a5 d3 92 58 10 b2 7f 1d d3 8d b3 7f e2 73 5e ee 3b 9a 2e bf 6d 2f e7 2c 37 58 01 ca 83 76 22 42 ea 7f 23 e5 54 1d 46 20 4c ef 97 83 9f ba 68 f7 9f c2 8f a7 87 74 20 35 1d 7c 5a	Gj.h\.3..A...5.x..&...i+...c(1.P..P.cLT....A.b.....4h...t.+..Z\.. .i..... S.....}FF.2..h..M+.....L.#.X..+.....*.....S.Ty..K.&.....q$.7.....".....F... .N..k..C.X.D.^.....u.\.....X.....s^.;...m/.,7X...v"B..#.T.F L.....h....t 5.|Z	success or wait	5	52A0A53	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	52A0A53	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	52A0B20	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	52A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	52A0A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	52A0C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 6296 Parent PID: 3424

General

Start time:	10:52:54
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xbf0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	12DA53F	WriteFile
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	12DA53F	WriteFile
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target applicat ion, error if it already exist s... /exapp	success or wait	3	12DA53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or interfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	12DA53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: conhost.exe PID: 5960 Parent PID: 6296

General

Start time:	10:52:55
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Disassembly

Code Analysis