



ID: 319578
Sample Name:
tn9jVPvlMSqAUX5.exe
Cookbook: default.jbs
Time: 13:05:51
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report tn9jVPvlMSqAUX5.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
Contacted IPs 14
Public 14
Private 15
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 17
Static File Info 19
General 19
File Icon 20
Static PE Info 20
General 20

Entrypoint Preview 20
Data Directories 22
Sections 22
Resources 22
Imports 22
Version Infos 22
Network Behavior 23
Snort IDS Alerts 23
TCP Packets 23
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: tn9jVPvlMSqAUX5.exe PID: 6228 Parent PID: 5876 25
General 25
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 27
Analysis Process: schtasks.exe PID: 4812 Parent PID: 6228 28
General 28
File Activities 28
File Read 28
Analysis Process: conhost.exe PID: 5108 Parent PID: 4812 28
General 28
Analysis Process: tn9jVPvlMSqAUX5.exe PID: 940 Parent PID: 6228 28
General 28
File Activities 29
File Created 29
File Deleted 29
File Written 30
File Read 30
Analysis Process: vbc.exe PID: 5852 Parent PID: 940 31
General 31
File Activities 31
File Created 31
File Written 31
Analysis Process: vbc.exe PID: 2228 Parent PID: 940 32
General 32
File Activities 32
File Created 32
File Written 32
File Read 34
Disassembly 34
Code Analysis 34

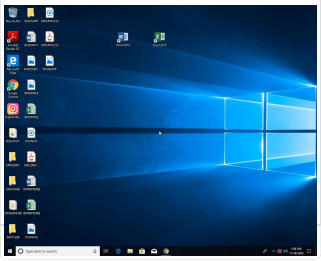
Analysis Report tn9jVPvlMSqAUX5.exe

Overview

General Information

Sample Name:	tn9jVPvlMSqAUX5.exe
Analysis ID:	319578
MD5:	afd45440cb1c77e..
SHA1:	36b35c3ca9db09..
SHA256:	babf0fe64b0415f...
Tags:	ESP exe geo NanoCore RAT

Most interesting Screenshot:



Detection



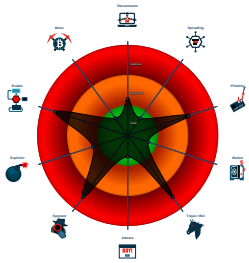
Nanocore
MailPassView

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected MailPassView
- Yara detected Nanocore RAT
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- tn9jVPvlMSqAUX5.exe (PID: 6228 cmdline: 'C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe' MD5: AFD45440CB1C77E2EBE1F2247573D04A)
  - schtasks.exe (PID: 4812 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\PEcoOLaILWJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpECFC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - tn9jVPvlMSqAUX5.exe (PID: 940 cmdline: {path} MD5: AFD45440CB1C77E2EBE1F2247573D04A)
    - vbc.exe (PID: 5852 cmdline: 'c:\windows\microsoft.net\framework\v2.0.50727\vbc.exe' /shtml 'C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 2228 cmdline: 'c:\windows\microsoft.net\framework\v2.0.50727\vbc.exe' /shtml 'C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.779662410.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000000.00000002.680469030.0000000004A3C000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x24525d:$x1: NanoCore.ClientPluginHost • 0x24529a:$x2: IClientNetworkHost • 0x248dcd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.680469030.0000000004A3C000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.680469030.0000000004A3C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x244fc5:$a: NanoCore • 0x244fd5:$a: NanoCore • 0x245209:$a: NanoCore • 0x24521d:$a: NanoCore • 0x24525d:$a: NanoCore • 0x245024:$b: ClientPlugin • 0x245226:$b: ClientPlugin • 0x245266:$b: ClientPlugin • 0x123e6f:$c: ProjectData • 0x24514b:$c: ProjectData • 0x124ba9:$d: DESCrypto • 0x245b52:$d: DESCrypto • 0x24d51e:$e: KeepAlive • 0x24b50c:$g: LogClientMessage • 0x247707:$i: get_Connected • 0x245e88:$j: #=q • 0x245eb8:$j: #=q • 0x245ed4:$j: #=q • 0x245f04:$j: #=q • 0x245f20:$j: #=q • 0x245f3c:$j: #=q
00000000.00000002.679213235.00000000038CE000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
12.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
13.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
13.2.vbc.exe.400000.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	

Sigma Overview

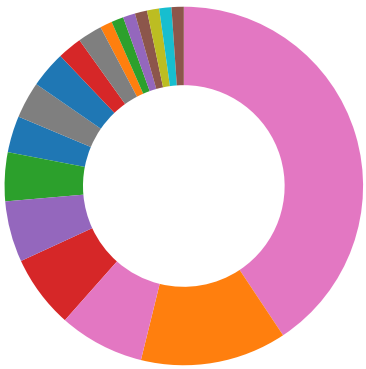
System Summary:



Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

Copyright null 2020

AV Detection:



- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:



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

E-Banking Fraud:



- Yara detected Nanocore RAT

System Summary:



- Malicious sample detected (through community Yara rule)

Boot Survival:



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

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



- Yara detected AntiVM_3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:



- Injects a PE file into a foreign processes

Stealing of Sensitive Information:



- Yara detected MailPassView
- Yara detected Nanocore RAT
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Instant Messenger accounts or passwords
- Tries to steal Mail credentials (via file access)
- Tries to steal Mail credentials (via file registry)
- Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

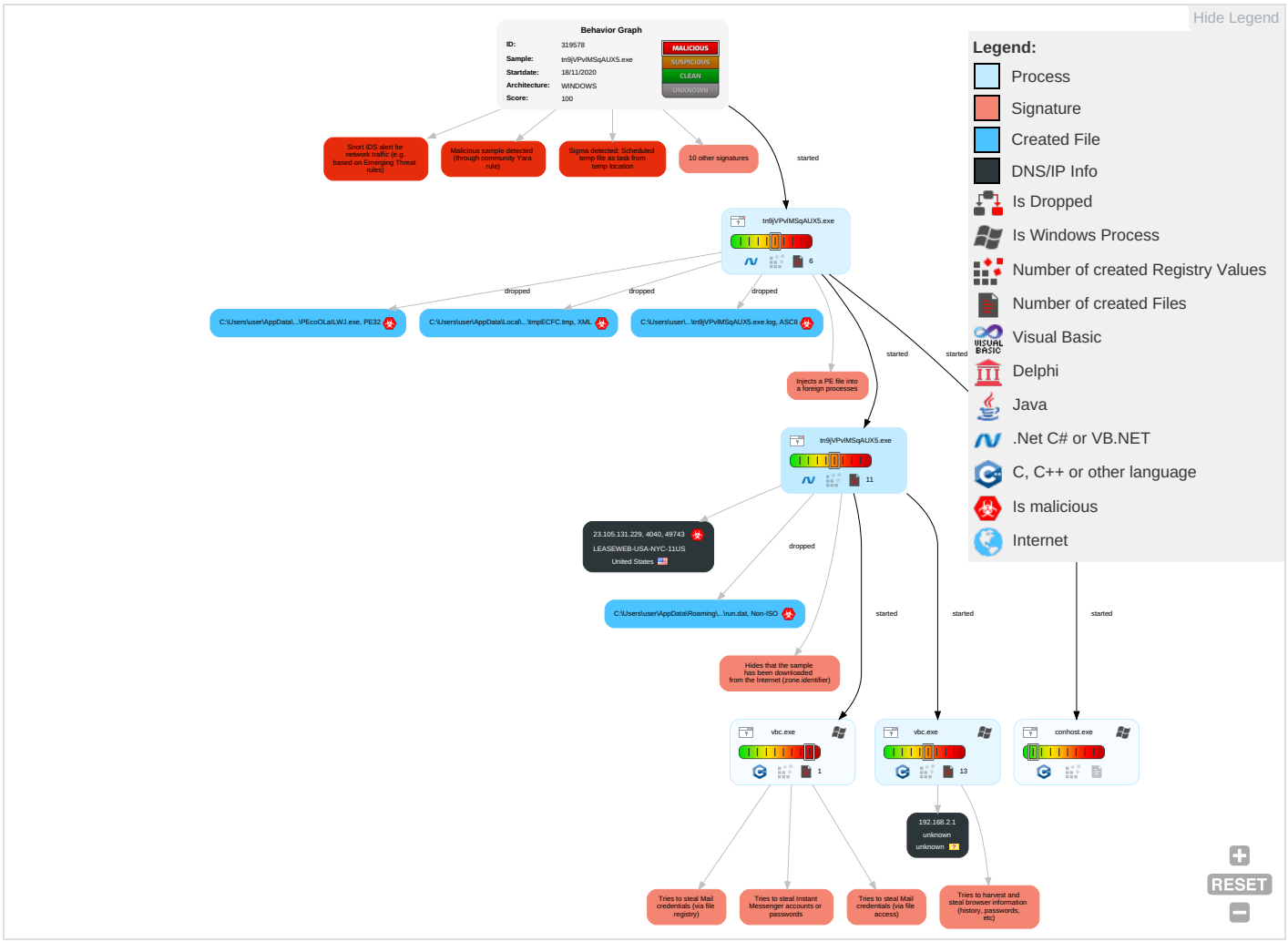


- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Native API 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Process Injection 1 1 1	Obfuscated Files or Information 4	Credentials In Files 1	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Remote Access Software 1	Ex Tra Lo
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1	NTDS	System Information Discovery 1 8	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonation	SII Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rc Ba

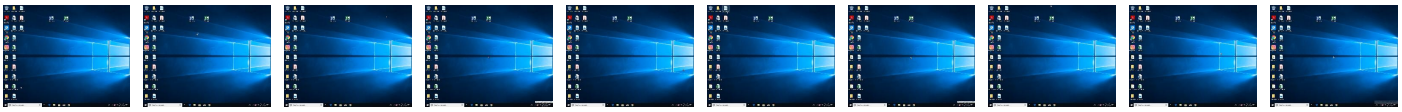
Behavior Graph



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
tn9jVPvlMSqAUX5.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\PEcoOLaILWJ.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnG	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypo	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.comtud	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comTC;	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypoooM	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.comter;	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comlay	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.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fonts.comx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl-p	0%	Avira URL Cloud	safe	
http://www.carterandcone.comic	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr=	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.agfamonotype.c	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.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.fonts.comnte	0%	Avira URL Cloud	safe	
http://www.fontbureau.comzana	0%	Avira URL Cloud	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.sajatypeworks.comuct	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sandoll.co.kr/c	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comhly	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krndo:	0%	Avira URL Cloud	safe	
http://www.tiro.comR	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn3	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

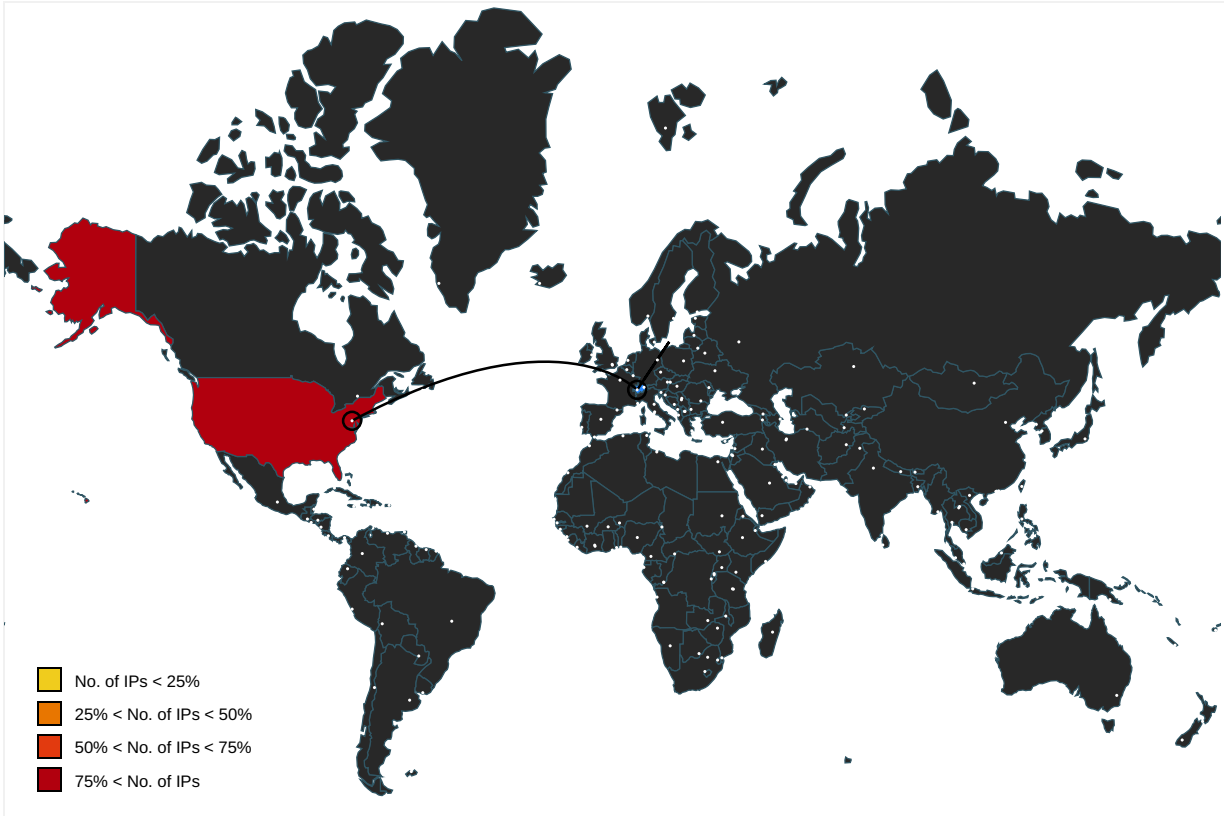
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersC	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664049989.0000000005BE9000.00000004.00000001.sdmp	false		high
http://www.tiro.com	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658966784.0000000005BEE000.00000004.00000001.sdmp, tn9jVPvlMSqAUX5.exe, 00000000.00000003.659291239.0000000005BEE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnG	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658458272.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comypo	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658966784.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656319398.0000000005BCB000.00000004.00000001.sdmp, tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comtud	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comC	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658966784.0000000005BEE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersj	tn9jVPvlMSqAUX5.exe, 00000000.00000003.661745512.0000000005BEB000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designerse	tn9jVPvlMSqAUX5.exe, 00000000.00000003.662154281.0000000005BEB000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTC;	tn9jVPvlMSqAUX5.exe, 00000000.00000003.659131617.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comypoooM	tn9jVPvlMSqAUX5.exe, 00000000.00000003.659460402.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comter;	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658966784.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://login.yahoo.com/config/login	vbc.exe	false		high
http://www.fonts.com	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656517087.0000000005BCB000.00000004.00000001.sdmp, tn9jVPvlMSqAUX5.exe, 00000000.00000003.656388352.0000000005BCB000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comlay	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658966784.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/	vbc.exe, vbc.exe, 0000000D.00000002.779662410.0000000000400000.00000040.00000001.sdmp, vbc.exe, 0000000D.00000002.779579503.0000000000195000.00000004.00000010.sdmp, 43ogpuf5.fhl.12.dr, wsrpbxdq.ypo.13.dr	false		high
http://www.urwpp.de	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersp	tn9jVPvlMSqAUX5.exe, 00000000.00000003.662779891.0000000005BE9000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comx	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656388352.0000000005BCB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl-p	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658175442.0000000005BED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerst	tn9jVPvlMSqAUX5.exe, 00000000.00000003.662154281.0000000005BEB000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comic	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658966784.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664193689.0000000005BE9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comalsd	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr=	tn9jVPvlMSqAUX5.exe, 00000000.00000003.657584628.0000000005BB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.agfamonotype.c	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	tn9jVPvlMSqAUX5.exe, 00000000.00000003.665387814.0000000005BBD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658931796.0000000005BEE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comnte	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656388352.0000000005BCB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comzana	tn9jVPvlMSqAUX5.exe, 00000000.00000002.681755462.0000000005BB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	tn9jVPvlMSqAUX5.exe, 00000000.00000003.664377780.0000000005BB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comuct	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656319398.0000000005BCB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kr/c	tn9jVPvlMSqAUX5.exe, 00000000.00000003.657584628.0000000005BB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658458272.0000000005BB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658175442.0000000005BED000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	tn9jVPvlMSqAUX5.exe, 00000000.00000003.662728113.0000000005BEB000.00000004.00000001.sdmp, tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comhly	tn9jVPvlMSqAUX5.exe, 00000000.00000003.659016913.0000000005BEE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krndo:	tn9jVPvlMSqAUX5.exe, 00000000.00000003.657584628.0000000005BB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comR	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656781448.0000000005BCB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn3	tn9jVPvlMSqAUX5.exe, 00000000.00000003.658458272.0000000005BB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	tn9jVPvlMSqAUX5.exe, 00000000.00000002.681755462.0000000005BB0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	tn9jVPvlMSqAUX5.exe, 00000000.00000002.683195015.0000000006B20000.00000002.00000001.sdmp	false		high
http://www.tiro.comc	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656781448.0000000005BCB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.coma	tn9jVPvlMSqAUX5.exe, 00000000.00000003.656687566.0000000005BCB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319578
Start date:	18.11.2020
Start time:	13:05:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tn9jVPvlMSqAUX5.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:	20
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.phis.troj.spyw.evad.winEXE@8/9@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.5% (good quality ratio 33.1%) • Quality average: 72.8% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 91% • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Copyright null 2020

Simulations

Behavior and APIs

Time	Type	Description
13:06:49	API Interceptor	961x Sleep call for process: tn9jVPvlMSqAUX5.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.105.131.229	LaCaixa_Aviso.exe	Get hash	malicious	Browse	
	L0caDBOEgr.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	HLiw2LPA8i.rtf	Get hash	malicious	Browse	• 192.253.246.143
	TDToxqrclL.exe	Get hash	malicious	Browse	• 23.105.131.177
	Ziiq5tl3CT.exe	Get hash	malicious	Browse	• 23.105.131.239
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.246.143
	ORDER INQUIRY.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Purchase Order 4500033557.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	SecuriteInfo.com.Trojan.DownLoader35.34609.25775.exe	Get hash	malicious	Browse	• 192.253.246.138
	Proof_of_payment.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	invoice tax.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	SHIPPING DOCUMENTS.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 192.253.246.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.246.143
	HDyADDoI3I.exe	Get hash	malicious	Browse	• 192.253.246.143
	11.exe	Get hash	malicious	Browse	• 173.234.155.145
	53C29QAJnd.exe	Get hash	malicious	Browse	• 173.234.155.145
	OMQZvmAmCj.exe	Get hash	malicious	Browse	• 173.234.155.145
	gH4o5FCHAE.exe	Get hash	malicious	Browse	• 173.234.155.145
	SHIPPING INVOICE.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	DOCUMENTO WAYBILL.exe	Get hash	malicious	Browse	• 23.105.131.133
	Proof Of Payment.exe	Get hash	malicious	Browse	• 23.105.131.129

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\tn9jVPvlMSqAUX5.exe.log	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.271473536084351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2u7x5I6Hi0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2I3rOz2T
MD5:	C3EC08CD6BEA8576070D5A52B4B6D7D0
SHA1:	40B95253F98B3CC5953100C0E71DAC7915094A5A
SHA-256:	28B314C3E5651414FD36B2A65B644A2A55F007A34A536BE17514E12CEE5A091B
SHA-512:	5B0E6398A092F08240DC6765425E16DB52F32542FF7250E87403C407E54B3660EF93E0EAD17BA2CEF6B666951ACF66FA0EAD61FB52E80867DDD398E8258DED2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Web\d 05d469d89b319a068f2123e7e6f8621\System.Web.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4 bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	5.166440724009737
Encrypted:	false
SSDEEP:	12:BMQkS9xyR4VrR1LEIJ9yuNJmcfNXbYmvmAwYxZwgJwnbnyAwoE:WlS9v5N9ZmcfSYm0XwgynbnyF
MD5:	69B2A2E17E78D24ABEE9F1DE2F04811A
SHA1:	D19C109704E83876AB3527457F9418A7D053AA33
SHA-256:	1B1491F21E64681F8FDC27B2265E2274FB7813EECB6AD8B446D2E431F6300EDD
SHA-512:	EB7269979BC4187520636FE3D7B3089F2C7C02E81C4CE2A738ADE680F72C61C67FE9577EEAA09D3CA93F34B60BE8C434D2CFBFED6566E783F6611279F056150
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">..<html><head><title>Email Accounts List</title></head>..<body>.. <h3>Email Accounts List</h3>.. <h4>Created by using Mail PassView</h4><p><table border="1" cellpadding="5"><tr bgcolor="E0E0E0">..<t h>Name..<th>Application..<th>Email..<th>Server..<th>Server Port..<th>Secured..<th>Type..<th>User..<th>Password..<th>Profile..<th>Password Strength..<th>SMTP Ser ver..<th>SMTP Server Port..</table>....</body></html>

C:\Users\user\AppData\Local\Temp\tmpECFC.tmp	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.180401522136723
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGltn:cbhK79lNQR/rydbz9I3YODOLNdq3u
MD5:	228F35FD2A67C0B22B41D42B4C2F10F6
SHA1:	33E121CF192B7B3CB6960A5CC054277E071F7E4A
SHA-256:	6EECB36A770C3E13E8C58F56D8B8557667B2108265B61AB3F5F0F321CD2D2A11
SHA-512:	A2F02938F0B699F124A2B294A9FF4AA3F35F6453DE02B363B819FA470014A87E337997DBC8148F0A765A3168A20A1BD8075AFC007E1681E47397444FA3D55B2E
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	HTML document, Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	
Category:	dropped
Size (bytes):	926
Entropy (8bit):	3.5897431793749606
Encrypted:	false
SSDEEP:	24:QAl45i94TBYTCvq4A3Y7eOhv8UFaoQBIn4+pS:a5icwVTOhnFaoQ+n4+4
MD5:	919E671C3D5959A91EF2D4C377D2B2FF
SHA1:	B1202B19512BBD390D3D5164792501C87BB42C41
SHA-256:	D2E079DF7CF6388315368BA79BF099AD2FF5428AF51BF5ABF2D99A2D7C5EB651
SHA-512:	F3298256372BEAB8EFE81B2E08D3B3869281F625DE1EE13189C6B95EB2134D223DF6F64CC9E490DD6B52A53AA936ADC17BD5DFE4E50EE0FE420F3EBAE27638 1C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..<.!.D.O.C.T.Y.P.E. .H.T.M.L. .P.U.B.L.I.C. .".-.//.W.3.C.//.D.T.D. .H.T.M.L. .3...2. .F.i.n.a.l.//.E.N.".>.....<.h.t.m.l.>.<.h.e.a.d.>.<.t.i.t.l.e.>.W.e.b. .B.r.o.w.s.e.r. .P.a.s.s.w.o.r.d.s.<./.t.i.t.l.e.>.<./.h.e.a.d.>.....<.b.o.d.y.>..... .<.h.3.>.W.e.b. .B.r.o.w.s.e.r. .P.a.s.s.w.o.r.d.s.<./.h.3.>.....<.b.r.>.<.h.4.>.C.r.e.a.t.e.d. .b.y. .u.s.i.n.g. .<.a. .h.r.e.f.=.".h.t.t.p.:. //.w.w.w...n.i.r.s.o.f.t...n.e.t./.". .t.a.r.g.e.t.=.".n.e.w.w.i.n.".>.W.e.b.B.r.o.w.s.e.r.P.a.s.s.V.i.e.w.</.a.>.</.h.4.>.<.p.>.<.t.a.b.l.e. .b.o.r.d.e.r.=.".1.". .c.e.l.l.p.a.d.d.i.n.g.=.".5.".>. <.t.r. .b.g.c.o.l.o.r.=.".E.0.E.0.E.0.".>.....<.t.h.>.U.R.L.....<.t.h.>.W.e.b. .B.r.o.w.s.e.r.....<.t.h.>.U.s.e.r. .N.a.m.e.....<.t.h.>.P.a.s.s.w.o.r.d.....<.t.h.>.P.a.s.s.w.o.r.d. .S.t.r.e. n.g.t.h.....<.t.h.>.U.s.e.r. .N.a.m.e. .F.i.e.l.d.....<.t.h.>.P.a.s.s.w.o.r.d. .F.i.e.l.d.....<./.t.a.b.l.e.>.....<./.b.o.d.y.>.<./.h.t.m.l.>.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356 A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:TVqt:T0t
MD5:	B1ADE59B3659FA064C8FAA74E453DDEF
SHA1:	9843CA8533A9B0A78354C73B2A5338D98EC824D1
SHA-256:	58E2D4D1C4B6292CCE8BED81F764BC5483A48696E2708719893C0B05FAC2A9B9
SHA-512:	429AC6A1155919E171805F27B9EF314777C825229961A441CFA41313E6349196959256B99F4B7D66F8C20DA6B703DF1825B397FC437A41625B41728EBA4434B2
Malicious:	**true**
Preview:	}TGp...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44 F8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\PEcoOLaILWJ.exe	
Process:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1105920
Entropy (8bit):	7.366130613090411
Encrypted:	false
SSDEEP:	24576:7ba+A+AUUspAkNKhHP/+JY/5AUA8bWkb7:7IApAkYuJ85DW0
MD5:	AFD45440CB1C77E2EBE1F2247573D04A
SHA1:	36B35C3CA9DB092DD6A1CF157625475FA2226E05
SHA-256:	BABF0FE64B0415F9EAABFA1AA91F1FBED20BC21BA93F3514F18FDC298D6CB54F
SHA-512:	1C11CF324550A3198A75E5BDCC1FA0789EE8DBA2DFC90E8FF17280B5F2326DD6EA906BC9A6A387CE1C7E7875D5DB105CC2A2335A573E9FD4FDF07121EBEB5 D3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P.._.....0.....D..... .....@.. .....@..... ..@.....O.....A..... ....H.....text...$.... ....`.rsrc....A.....B.....@..@.reloc..... .....@..B.....H.....8Y.....A...}.,.T..1..`4...N.Y-F..pU.TW..+R..Y.^.i...)..^9....3...).^....>.L..!.;.....i7.EG..>...+...tZL. ..._...^x....n.bK..R.(.b|..U!c.c....]^d.....<..$....|.us.1.3...%]..._...M.L...\}{`[.!`n.^."BU.S..h.C..n.D}...e.....I..^.<.....t.r..j9F...,..n...a.W.._7ZH.}...7.amqEB<.mp/.n_.w-...g.w.... .O..W...w...).&.".%.d.....;t*...g.S.IC..T..Z-j.U...B?.).+....e....e..q...T..%..7.xx.J.\.m>D*..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.366130613090411
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	tn9jVPvlMSqAUX5.exe
File size:	1105920
MD5:	afd45440cb1c77e2ebe1f2247573d04a
SHA1:	36b35c3ca9db092dd6a1cf157625475fa2226e05
SHA256:	babf0fe64b0415f9eaabfa1aa91f1fbed20bc21ba93f3514f18fdc298d6cb54f

General

SHA512:	1c11cf324550a3198a75e5bdcc1fa0789ee8dba2dfc90e8ff17280b5f2326dd6ea906bc9a6a387ce1c7e7875d5db105cc2a2335a573e9fd4fdf07121ebeb5fd3
SSDEEP:	24576:7ba+A+AUUspAkNKhHP/+JY/5AUA8bWkb7:7IApAkYuJ85DW0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P..._.....0.....D..... ....@.. .....@.....@.....

File Icon



Icon Hash:	f8c492aaaa92dcfe

Static PE Info

General

Entrypoint:	0x50b91e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB4A450 [Wed Nov 18 04:34:24 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10b8cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10c000	0x41a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x112000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x109924	0x109a00	False	0.690261948529	data	7.37322926627	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x41a8	0x4200	False	0.503373579545	data	5.44979825616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x112000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10c190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x10c5f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0x10d6a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3771611807, next used block 3167566498		
RT_GROUP_ICON	0x10fc48	0x30	data		
RT_VERSION	0x10fc78	0x344	data		
RT_MANIFEST	0x10ffbc	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 2017
Assembly Version	1.0.0.0

Description	Data
InternalName	.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Clinic Management System
ProductVersion	1.0.0.0
FileDescription	Clinic Management System
OriginalFilename	.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/18/20-13:07:14.815072	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	4040	192.168.2.4	23.105.131.229

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:06:55.213327885 CET	49737	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:06:58.221419096 CET	49737	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:04.221538067 CET	49737	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:14.434274912 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:14.791302919 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:14.791554928 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:14.815072060 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:15.291202068 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:15.351821899 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:15.360234976 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:15.700900078 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:15.701033115 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:16.191437960 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:16.191616058 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:16.691195965 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:16.710350037 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:16.710412025 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:16.710454941 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:16.710541964 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:16.721476078 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:16.721690893 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.161082983 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.161459923 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.161626101 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.162801981 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.171910048 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.172077894 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.172097921 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.172195911 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.172274113 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.172318935 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.172487020 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.172621965 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.561261892 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.562504053 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.562623978 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.563653946 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.573633909 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.573781967 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.574276924 CET	4040	49743	23.105.131.229	192.168.2.4

Copyright null 2020

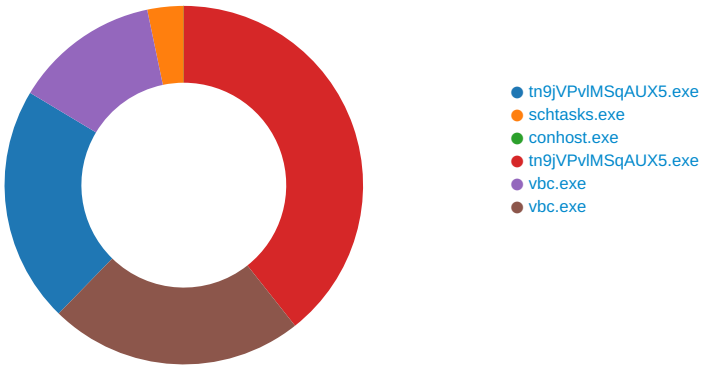
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:07:17.577894926 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.578031063 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.578466892 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.578686953 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.578764915 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.579381943 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.579993963 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.580073118 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.580177069 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.580723047 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.580785036 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.581855059 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.582202911 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.582266092 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.584845066 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.594513893 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.594599009 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.974112988 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.975322008 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.975430012 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.976998091 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.977057934 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.977102995 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.977142096 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.987185001 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.987333059 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.987674952 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.987719059 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.987791061 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.987849951 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.987972975 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.988032103 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.989358902 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.997730017 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.997781038 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.997883081 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.998070002 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.998131990 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.998140097 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.998270035 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.998332977 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:17.999049902 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:17.999933958 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.000030994 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:18.072355032 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.092437983 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.092479944 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.092505932 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.092592955 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:18.092732906 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.092818975 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:18.092844963 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.092927933 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:18.092958927 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.093053102 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.093121052 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:18.093163013 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.093288898 CET	4040	49743	23.105.131.229	192.168.2.4
Nov 18, 2020 13:07:18.093350887 CET	49743	4040	192.168.2.4	23.105.131.229
Nov 18, 2020 13:07:18.093390942 CET	4040	49743	23.105.131.229	192.168.2.4

Copyright null 2020

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: tn9jVPvlMSqAUX5.exe PID: 6228 Parent PID: 5876

General

Start time:	13:06:42
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe'
Imagebase:	0xf70000
File size:	1105920 bytes
MD5 hash:	AFD45440CB1C77E2EBE1F2247573D04A
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: 00000000.00000002.680469030.0000000004A3C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.680469030.0000000004A3C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.680469030.0000000004A3C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.679213235.00000000038CE000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.679941870.000000000488D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.679941870.000000000488D000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.679941870.000000000488D000.00000004.00000001.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\PEcoOLaILWJ.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7D00403	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpECFC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71809869	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\tn9jVPvlMSqAUX5.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\tmpECFC.tmp	success or wait	1	7D0107A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\PEcoOLaILWJ.exe	unknown	1105920	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpECFC.tmp	unknown	1644	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 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	7D0068B	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\tn9jVPvlMSqAUX5.exe.log	unknown	641	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	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\tn9jVPvlMSqAUX5.exe	unknown	1105920	success or wait	1	7D0068B	ReadFile

Copyright null 2020

Analysis Process: schtasks.exe PID: 4812 Parent PID: 6228

General

Start time:	13:06:51
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\PEcoOLaILWJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpECFC.tmp'
Imagebase:	0x830000
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\tmpECFC.tmp	unknown	2	success or wait	1	83AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpECFC.tmp	unknown	1645	success or wait	1	83ABD9	ReadFile

Analysis Process: conhost.exe PID: 5108 Parent PID: 4812

General

Start time:	13:06:51
Start date:	18/11/2020
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: tn9jVPvlMSqAUX5.exe PID: 940 Parent PID: 6228

General

Start time:	13:06:52
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xde0000
File size:	1105920 bytes
MD5 hash:	AFD45440CB1C77E2EBE1F2247573D04A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000003.808207077.0000000004A24000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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	57F07A1	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	57F089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	57F07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	57F07A1	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	57F089B	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	57F089B	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	1	57F089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe:Zone.Identifier	success or wait	1	57F0B41	DeleteFileA

Copyright null 2020

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	7d 54 47 70 ba 8b d8 48	}TGp...H	success or wait	1	57F0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	57F0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426840	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^._.........B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	57F0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	57F0A53	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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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\tn9jVPvlMSqAUX5.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\tn9jVPvlMSqAUX5.exe	unknown	512	success or wait	1	7234BF06	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	57F0A53	ReadFile

Analysis Process: vbc.exe PID: 5852 Parent PID: 940

General

Start time:	13:07:37
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'c:\windows\microsoft.net\framework\v2.0.50727\vbc.exe' /shtml 'C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000C.00000002.774211357.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EFC	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	57	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 33 2e 32 20 46 69 6e 61 6c 2f 2f 45 4e 22 3e 0d 0a	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">..	success or wait	1	405F1D	WriteFile
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	94	3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 45 6d 61 69 6c 20 41 63 63 6f 75 6e 74 73 20 4c 69 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 20 3c 68 33 3e 45 6d 61 69 6c 20 41 63 63 6f 75 6e 74 73 20 4c 69 73 74 3c 2f 68 33 3e 0d 0a	<html><head><title>Email Accounts List</title></head>..<body>.. Email Accounts List ..	success or wait	1	405F1D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	100	3c 62 72 3e 3c 68 34 3e 43 72 65 61 74 65 64 20 62 79 20 75 73 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6e 69 72 73 6f 66 74 2e 6e 65 74 2f 22 20 74 61 72 67 65 74 3d 22 6e 65 77 77 69 6e 22 3e 4d 61 69 6c 20 50 61 73 73 56 69 65 77 3c 2f 61 3e 3c 2f 68 34 3e 3c 70 3e	 <h4>Created by using <a hr ef="http://www.nirsoft.net/" target="newwin">Mail PassView</h4><p>	success or wait	1	405F1D	WriteFile
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	57	3c 74 61 62 6c 65 20 62 6f 72 64 65 72 3d 22 31 22 20 63 65 6c 6c 70 61 64 64 69 6e 67 3d 22 35 22 3e 3c 74 72 20 62 67 63 6f 6c 6f 72 3d 22 45 30 45 30 45 30 22 3e 0d 0a	<table border="1" cellpadding="5"><tr bgcolor="E0E0E0">..	success or wait	1	405F1D	WriteFile
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	10	3c 74 68 3e 4e 61 6d 65 0d 0a	<th>Name..	success or wait	13	405F1D	WriteFile
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	10	3c 2f 74 61 62 6c 65 3e 0d 0a	</table>..	success or wait	1	405F1D	WriteFile
C:\Users\user\AppData\Local\Temp\43ogpuf5.fhl	unknown	16	0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e	..</body></html>	success or wait	1	405F1D	WriteFile

Analysis Process: vbc.exe PID: 2228 Parent PID: 940

General

Start time:	13:07:39
Start date:	18/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'c:\windows\microsoft.net\framework\v2.0.50727\vbc.exe' /shtml 'C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.779662410.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407175	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	2	ff fe	..	success or wait	1	407BCF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	114	3c 00 21 00 44 00 4f 00 43 00 54 00 59 00 50 00 45 00 20 00 48 00 54 00 4d 00 4c 00 20 00 50 00 55 00 42 00 4c 00 49 00 43 00 20 00 22 00 2d 00 2f 00 2f 00 57 00 33 00 43 00 2f 00 2f 00 44 00 54 00 44 00 20 00 48 00 54 00 4d 00 4c 00 20 00 33 00 2e 00 32 00 20 00 46 00 69 00 6e 00 61 00 6c 00 2f 00 2f 00 45 00 4e 00 22 00 3e 00 0d 00 0a 00	<.!.D.O.C.T.Y.P.E. .H.T.M.L. .P.U.B.L.I.C. .".-././/.W.3.C././/.D.T.D. .H.T.M.L. .3...2. .F. i.n.a.l././/.E.N.".>.....	success or wait	1	407198	WriteFile
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	196	3c 00 68 00 74 00 6d 00 6c 00 3e 00 3c 00 68 00 65 00 61 00 64 00 3e 00 3c 00 74 00 69 00 74 00 6c 00 65 00 3e 00 57 00 65 00 62 00 20 00 42 00 72 00 6f 00 77 00 73 00 65 00 72 00 20 00 50 00 61 00 73 00 73 00 77 00 6f 00 72 00 64 00 73 00 3c 00 2f 00 74 00 69 00 74 00 6c 00 65 00 3e 00 3c 00 2f 00 68 00 65 00 61 00 64 00 3e 00 0d 00 0a 00 3c 00 62 00 6f 00 64 00 79 00 3e 00 0d 00 0a 00 20 00 3c 00 68 00 33 00 3e 00 57 00 65 00 62 00 20 00 42 00 72 00 6f 00 77 00 73 00 65 00 72 00 20 00 50 00 61 00 73 00 73 00 77 00 6f 00 72 00 64 00 73 00 3c 00 2f 00 68 00 33 00 3e 00 0d 00 0a 00	<.h.t.m.l.>.<.h.e.a.d.>.<.t.i.t.l.e.>.W.e.b. .B.r.o.w.s.e.r. .P.a.s.s.w.o.r.d.s.<./.t.i.t.l.e.>.<./.h.e.a.d.>.....<.b.o.d.y.>..... .<.h.3.>.W.e.b. .B.r.o.w.s.e.r. .P.a.s.s.w.o.r.d.s.<./.h.3.>.....	success or wait	1	407198	WriteFile
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	210	3c 00 62 00 72 00 3e 00 3c 00 68 00 34 00 3e 00 43 00 72 00 65 00 61 00 74 00 65 00 64 00 20 00 62 00 79 00 20 00 75 00 73 00 69 00 6e 00 67 00 20 00 3c 00 61 00 20 00 68 00 72 00 65 00 66 00 3d 00 22 00 68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 77 00 77 00 77 00 2e 00 6e 00 69 00 72 00 73 00 6f 00 66 00 74 00 2e 00 6e 00 65 00 74 00 2f 00 22 00 20 00 74 00 61 00 72 00 67 00 65 00 74 00 3d 00 22 00 6e 00 65 00 77 00 77 00 69 00 6e 00 22 00 3e 00 57 00 65 00 62 00 42 00 72 00 6f 00 77 00 73 00 65 00 72 00 50 00 61 00 73 00 73 00 56 00 69 00 65 00 77 00 3c 00 2f 00 61 00 3e 00 3c 00 2f 00 68 00 34 00 3e 00 3c 00 70 00 3e 00	<.b.r.>.<.h.4.>.C.r.e.a.t.e.d. .b.y. .u.s.i.n.g. .<.a. .h.r.e.f.=.".h.t.t.p.:././/.w.w.w...n.i.r.s.o.f.t...n.e.t./.". .t.a.r.g.e.t.=.".n.e.w.w.i.n.".>.W.e.b.B.r.o.w.s.e.r.P.a.s.s.V.i.e.w.<./.a.>.<./.h.4.>.<.p.>.	success or wait	1	407198	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	114	3c 00 74 00 61 00 62 00 6c 00 65 00 20 00 62 00 6f 00 72 00 64 00 65 00 72 00 3d 00 22 00 31 00 22 00 20 00 63 00 65 00 6c 00 6c 00 70 00 61 00 64 00 64 00 69 00 6e 00 67 00 3d 00 22 00 35 00 22 00 3e 00 3c 00 74 00 72 00 20 00 62 00 67 00 63 00 6f 00 6c 00 6f 00 72 00 3d 00 22 00 45 00 30 00 45 00 30 00 45 00 30 00 22 00 3e 00 0d 00 0a 00	<.t.a.b.l.e. .b.o.r.d.e.r.=.". 1.". .c.e.l.l.p.a.d.d.i.n.g.=. ".5.".>.<.t.r. .b.g.c.o.l.o.r. =.".E.0.E.0.E.0.".>.....	success or wait	1	407198	WriteFile
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	18	3c 00 74 00 68 00 3e 00 55 00 52 00 4c 00 0d 00 0a 00	<.t.h.>.U.R.L.....	success or wait	7	407198	WriteFile
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	20	3c 00 2f 00 74 00 61 00 62 00 6c 00 65 00 3e 00 0d 00 0a 00	<./.t.a.b.l.e.>.....	success or wait	1	407198	WriteFile
C:\Users\user\AppData\Local\Temp\wsrpbxdq.ypo	unknown	32	0d 00 0a 00 3c 00 2f 00 62 00 6f 00 64 00 79 00 3e 00 3c 00 2f 00 68 00 74 00 6d 00 6c 00 3e 00	....<./.b.o.d.y.>.<./.h.t.m.l.>.	success or wait	1	407198	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	414E52	ReadFile

Disassembly

Code Analysis

Copyright null 2020