ID: 357332
Sample Name: Items_02559-02663.pdf.exe
Cookbook: default.jbs
Time: 13:12:27
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

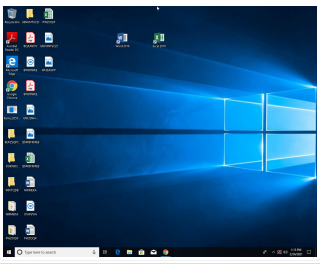
Analysis Report Items_02559-02663.pdf.exe

Overview

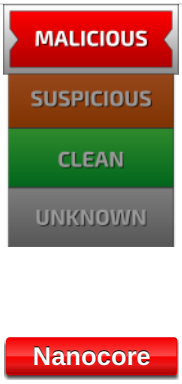
General Information

Sample Name:	Items_02559-02663.pdf.exe
Analysis ID:	357332
MD5:	69b99b73945755..
SHA1:	0b4a98cf7c2cf5f…
SHA256:	0a31dde9dd611d..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



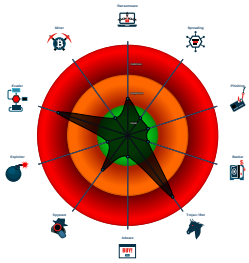
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Items_02559-02663.pdf.exe (PID: 1680 cmdline: 'C:\Users\user\Desktop\Items_02559-02663.pdf.exe' MD5: 69B99B73945755DF4628529E5A1BF6F8)
  - schtasks.exe (PID: 1900 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jZWRPYaLXncddo' /XML 'C:\Users\user\AppData\Local\Temp\tmp71AB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Items_02559-02663.pdf.exe (PID: 2920 cmdline: {path} MD5: 69B99B73945755DF4628529E5A1BF6F8)
  - Items_02559-02663.pdf.exe (PID: 1440 cmdline: {path} MD5: 69B99B73945755DF4628529E5A1BF6F8)
    - schtasks.exe (PID: 5716 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Items_02559-02663.pdf.exe (PID: 472 cmdline: C:\Users\user\Desktop\Items_02559-02663.pdf.exe 0 MD5: 69B99B73945755DF4628529E5A1BF6F8)
  - schtasks.exe (PID: 5688 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jZWRPYaLXncddo' /XML 'C:\Users\user\AppData\Local\Temp\tmpBA1E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Items_02559-02663.pdf.exe (PID: 5880 cmdline: {path} MD5: 69B99B73945755DF4628529E5A1BF6F8)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "063b6e17-4321-4269-bf57-df94b570da06",
  "Group": "GIFT",
  "Domain1": "wilsonzz.webredirect.org",
  "Domain2": "thanks001.ddns.net",
  "Port": 9036,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.908925138.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.908925138.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.908925138.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000002.687231789.0000000003B89000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1085d:$x1: NanoCore.ClientPluginHost • 0xff29d:$x1: NanoCore.ClientPluginHost • 0x1089a:$x2: IClientNetworkHost • 0xff2da:$x2: IClientNetworkHost • 0x143cd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x102e0d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000000.00000002.687231789.0000000003B8 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.Items_02559-02663.pdf.exe.2df1408.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
4.2.Items_02559-02663.pdf.exe.2df1408.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
7.2.Items_02559-02663.pdf.exe.48396d0.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
7.2.Items_02559-02663.pdf.exe.48396d0.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
7.2.Items_02559-02663.pdf.exe.48396d0.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 47 entries				

Sigma Overview

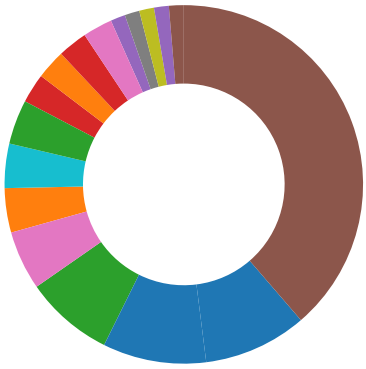
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Compliance
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Uses an obfuscated file name to hide its real file extension (double extension)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

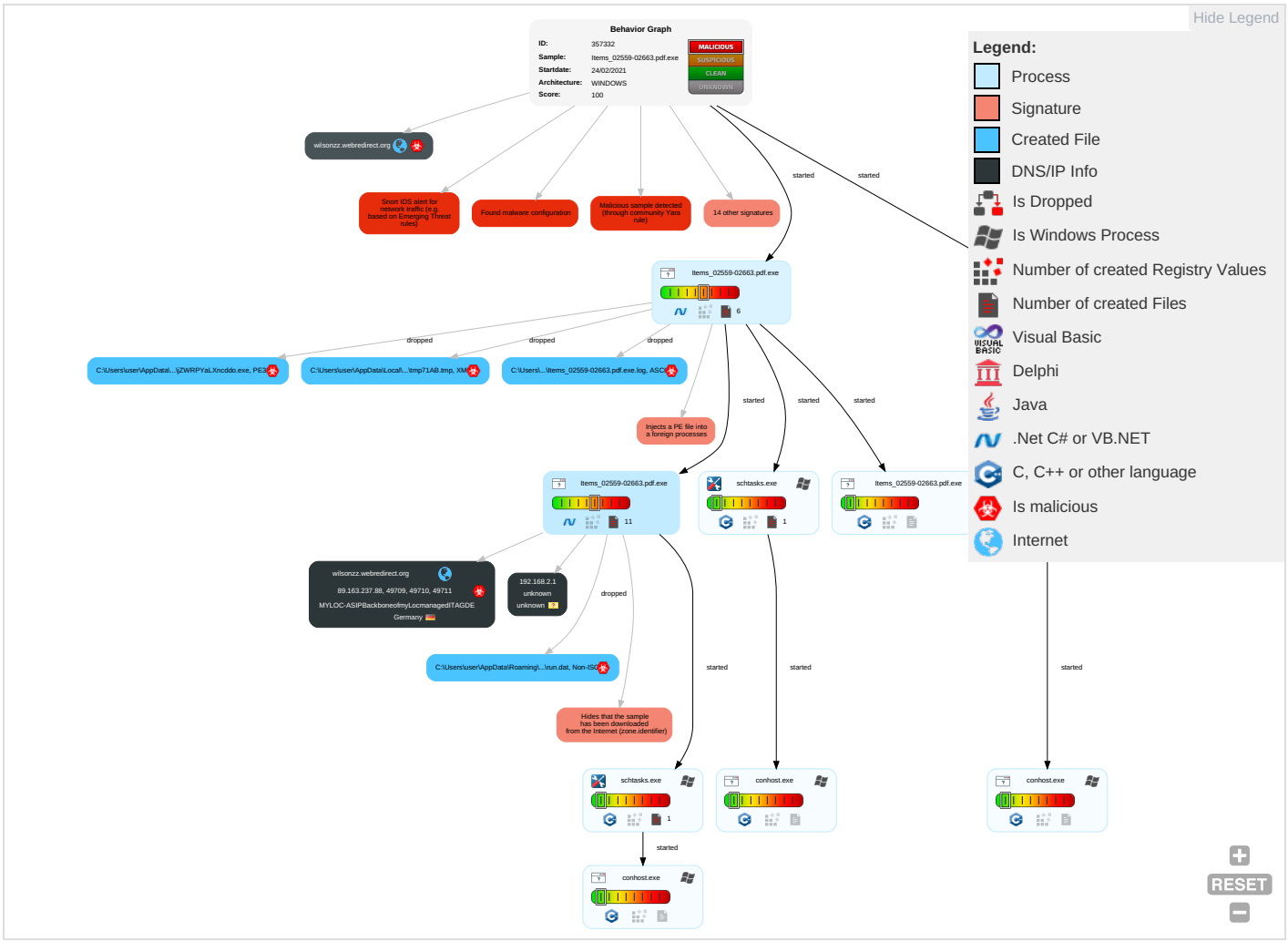
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 2 1	Security Software Discovery 1 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
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
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

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
Items_02559-02663.pdf.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	
Items_02559-02663.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jZWRPYaLXncddo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\jZWRPYaLXncddo.exe	23%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Items_02559-02663.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.Items_02559-02663.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

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	
thanks001.ddns.net	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.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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.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.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.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	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	
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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
wilsonzz.webredirect.org	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wilsonzz.webredirect.org	89.163.237.88	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
thanks001.ddns.net	true	• Avira URL Cloud: safe	unknown
wilsonzz.webredirect.org	true	• Avira URL Cloud: safe	unknown

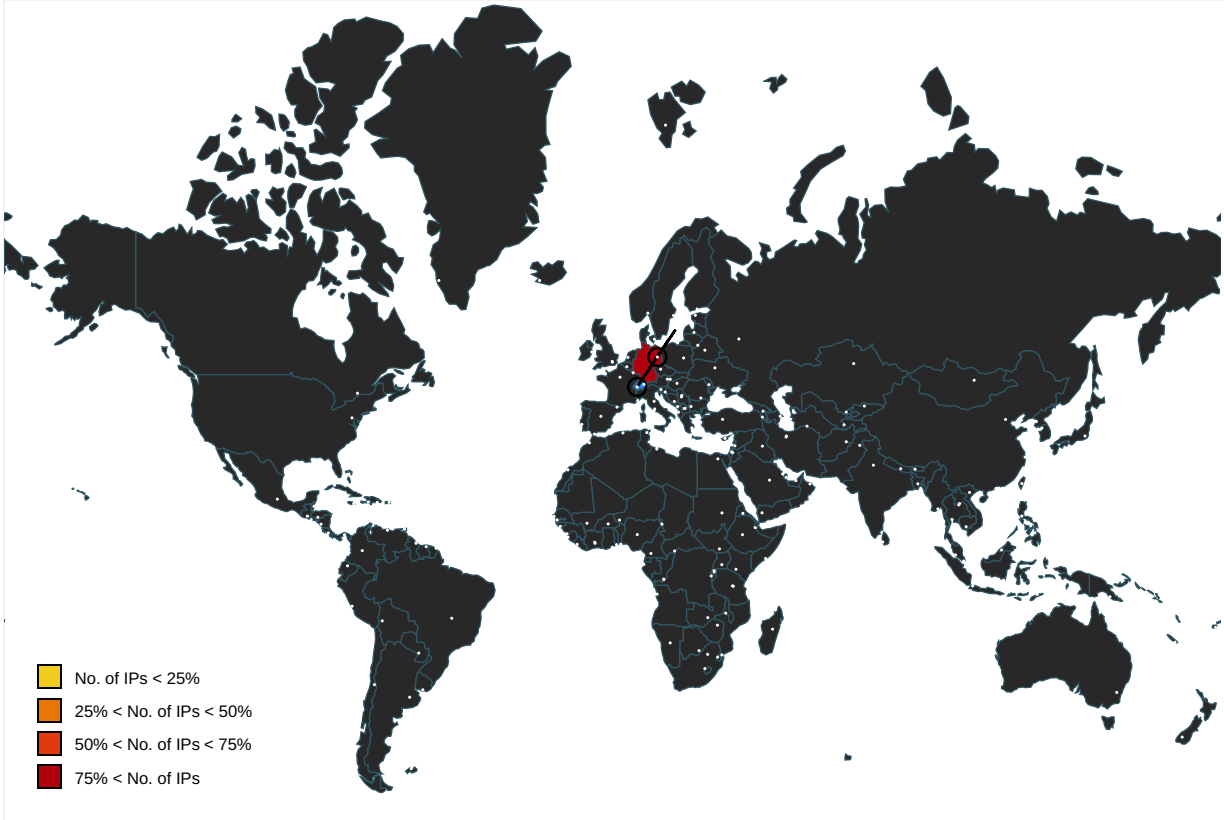
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.monotype.	Items_02559-02663.pdf.exe, 00000000.00000003.650108891.00000000C7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Items_02559-02663.pdf.exe, 00000000.00000002.684003114.00000000002C1F000.00000004.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.720737165.0000000003361000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Items_02559-02663.pdf.exe, 00000000.00000002.690720943.00000000055F0000.00000002.00000001.sdmp, Items_02559-02663.pdf.exe, 00000007.00000002.726617404.00000000062D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
89.163.237.88	unknown	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357332
Start date:	24.02.2021
Start time:	13:12:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Items_02559-02663.pdf.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:	11
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@17/10@18/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 53.1% • Quality standard deviation: 27.7%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 104.43.139.144, 13.64.90.137, 8.253.207.120, 67.26.17.254, 8.250.151.254, 8.248.121.254, 8.248.125.254 • Excluded domains from analysis (whitelisted): skypedataprdcoleus17.cloudapp.net, skypedataprdcolwus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net, skypedataprdcolcus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:13:17	API Interceptor	922x Sleep call for process: Items_02559-02663.pdf.exe modified
13:13:33	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Items_02559-02663.pdf.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MYLOC-ASIPBackboneofmyLocmanagedITAGDE	Bank Transfer Slip.exe	Get hash	malicious	Browse	• 91.212.153.84
	BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	JMG Memo-Circular No 018-21.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 62.141.37.17
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FickerStealer.exe	Get hash	malicious	Browse	• 89.163.225.172
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 89.163.210.141
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 89.163.140.102
	TaskAudio Driver.exe	Get hash	malicious	Browse	• 193.111.198.220
	Z8363664.doc	Get hash	malicious	Browse	• 89.163.210.141
	OhGodAnETHlargementPill2.exe	Get hash	malicious	Browse	• 193.111.198.220
	godflex-r2.exe	Get hash	malicious	Browse	• 193.111.198.220

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Items_02559-02663.pdf.exe.log	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1311
Entropy (8bit):	5.137743702844662
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Y0u1kaxtn:cbk4oL600QydbQxIYODOLedq3hDj
MD5:	2CB7C82A649468334E3AC9C286999C53
SHA1:	86F1D65CA2595D717E2FC67F2F064E8AF6F20F89
SHA-256:	64A1FE728F630ADEBE57FBFA6EB1DA4F9B38DDD815C9758C2DC743D19E9CBC3E
SHA-512:	B2E5E5B6CE3733586ADE0C9F23318F3DE58CDA06B88CBF8073F69C0CC3B0AE9BEE2920A768906F2665CA32AAAEB35CF6E30D5CA66B1C60CDD05AA59B79377A5C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp71AB.tmp	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.188267571798794
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGdtn:cbhK79lNQR/rydbz9l3YODOLNdq34
MD5:	265EB6B9D687D7DFEA6503E02D65C940
SHA1:	A2C93785E51DB7BF98DC0469D5F5F4CCCB6E9526
SHA-256:	6FAA626806DEE34DEB3EAE73915BD8C9452F04D19F785C84C8936DD86754059C
SHA-512:	69A786F717BBC7BEDD6FA760CCE15A7CEC96F9616808D4AB462156E9B65B76AC0494546E83837A355ED6CB5A7570642697483885F8CEC12209FB2F6906A65898
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\Local\Temp\tmpBA1E.tmp	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.188267571798794
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGdtn:cbhK79lNQR/rydbz9l3YODOLNdq34
MD5:	265EB6B9D687D7DFEA6503E02D65C940
SHA1:	A2C93785E51DB7BF98DC0469D5F5F4CCCB6E9526
SHA-256:	6FAA626806DEE34DEB3EAE73915BD8C9452F04D19F785C84C8936DD86754059C
SHA-512:	69A786F717BBC7BEDD6FA760CCE15A7CEC96F9616808D4AB462156E9B65B76AC0494546E83837A355ED6CB5A7570642697483885F8CEC12209FB2F6906A65898
Malicious:	false
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\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC68
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+ .2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?. ..A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH }..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f. ..p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:Zot:mt
MD5:	78D87C90B6290A2B5AC730E21857A636
SHA1:	7F2397E26E56320B7D29A2EA56AF2315EBB5ECF7
SHA-256:	A8C767EFF7AC0ABBBA818D11488D4D5D8D8A72B8BEA2DE743E0CC37B9AC06398
SHA-512:	F83E4B95CDDA9DC47C9D3D9780A7CA0346CED7996BAFF6A6011E961030F830249BF3CAA5E1DB108B6B77E77C8B47A9855299C92543429A165FE3EA6423DE1E 4
Malicious:	**true**
Reputation:	low
Preview:	.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671 CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a........~.~.......3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i......~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v."".v.......#..X.a....../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz......(...o......b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<..,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O..........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?...........b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i..........$....$........CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.5199746782469115

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat

Encrypted:	false
SSDEEP:	3:oNt+WfWsuKfMrQC:oNwvsuuMrQC
MD5:	E180244A81F8CE52CE654E64B183D082
SHA1:	36C89CD921CB760B029DA4F6102D3588232982FC
SHA-256:	00CB24367F72D6074CB5201ADB3F208B1ED7D29E1DAC42D38023E505A4A56C09
SHA-512:	0AD3E451827BA0C41574C5937B891CE4D763492255FE003F4B855C087AE15AA7734E3090AC0B6EDF161527B9A691B2710EEC7BBA6706EF0447ED332AEA11261(
Malicious:	false
Preview:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe

C:\Users\user\AppData\Roaming\jZWRPYaLXncddo.exe

Process:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	770048
Entropy (8bit):	7.94192338687656
Encrypted:	false
SSDEEP:	12288:YEY3LLUEMthvqNv06tdkkQjFXZhBPEw6S4ZR6UaG+SsOEgntReIwCzWcPKlTPTGl:ALCYNJN+FXpc/H6Ud+SxDXeIwlBRG16c
MD5:	69B99B73945755DF4628529E5A1BF6F8
SHA1:	0B4A98CF7C2CF5F1FB3480736A602EBE4BBB9746
SHA-256:	0A31DDE9DD611DE5AFEF82EAC6581588C5D8B034106A1F4EAC68958B8BD526C2
SHA-512:	779A27BC5456FD9A7EF27963DAF4310C100DB04B53FFF46346C14D69B2EC7456A3DEE49505A4B23A59BD4E434E8AE845CFE2FD8D4EE9421FFB19A8D983CC3C9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o.5`.....0..... .....@.. ..... ..... ..@.....4...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....h.....H.....Ho..t3.....4.....x2.....&.(.....*...0..9.....~.....,".r...p.....(....o....s.....~.....+..*....0.....~.....+..*"".....*.0 ..!.....(....r!..p~....o.....t.....+..*....0..!.....(....r1..p~....o.....t.....+..*....0.....r5..p.+..*..0.....rA..p.+..*".(.....*^..}.....(.....(%....**...(.....*..0..;.....rI..pr...p.(.....,..(.... ..+..s.....o .....(!.....*..0..I.....r...pr...p.(.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.94192338687656
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Items_02559-02663.pdf.exe
File size:	770048
MD5:	69b99b73945755df4628529e5a1bf6f8
SHA1:	0b4a98cf7c2cf5f1fb3480736a602ebe4bbb9746
SHA256:	0a31dde9dd611de5afef82eac6581588c5d8b034106a1f4eac68958b8bd526c2
SHA512:	779a27bc5456fd9a7ef27963daf4310c100db04b53fff46346c14d69b2ec7456a3dee49505a4b23a59bd4e434e8ae845cfe2fd8d4ee9421ffb19a8d983cc3c89
SSDEEP:	12288:YEY3LLUEMthvqNv06tdkkQjFXZhBPEw6S4ZR6UaG+SsOEgntReIwCzWcPKlTPTGl:ALCYNJN+FXpc/H6Ud+SxDXeIwlBRG16c
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o.5`.....0..... .....@.. ....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4bd586
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:	0x6035AC6F [Wed Feb 24 01:31:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbd534	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	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	0xbb58c	0xbb600	False	0.933682350734	data	7.94731147015	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x5b4	0x600	False	0.436197916667	data	4.24672884221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	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_VERSION	0xbe090	0x324	data		
RT_MANIFEST	0xbe3c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	4.0.0.0
InternalName	wA.exe
FileVersion	4.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ITP_RMSS
ProductVersion	4.0.0.0
FileDescription	ITP_RMSS
OriginalFilename	wA.exe

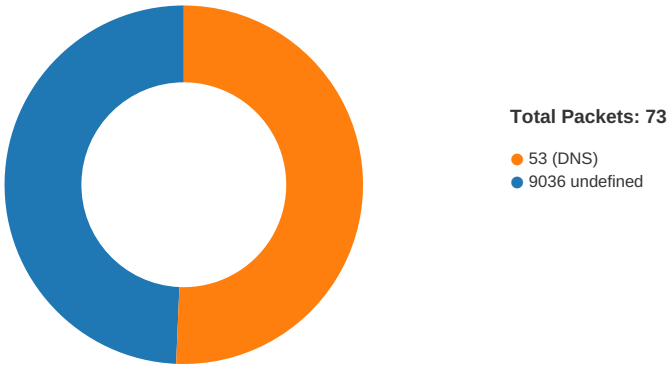
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-13:13:35.557410	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	9036	192.168.2.4	89.163.237.88

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-13:13:42.456581	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	9036	192.168.2.4	89.163.237.88
02/24/21-13:13:48.944286	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	9036	192.168.2.4	89.163.237.88
02/24/21-13:13:55.417376	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:02.308430	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:09.115026	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:15.121738	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:22.468708	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:28.451679	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:33.473501	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:39.501822	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:45.520035	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:50.510622	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	9036	192.168.2.4	89.163.237.88
02/24/21-13:14:56.537341	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	9036	192.168.2.4	89.163.237.88
02/24/21-13:15:02.624356	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	9036	192.168.2.4	89.163.237.88
02/24/21-13:15:07.507413	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	9036	192.168.2.4	89.163.237.88
02/24/21-13:15:13.608651	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	9036	192.168.2.4	89.163.237.88
02/24/21-13:15:19.571269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	9036	192.168.2.4	89.163.237.88

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:13:35.358680010 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.380064011 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.380227089 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.557410002 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.598577023 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.625113964 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.649607897 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.690336943 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.764992952 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.765063047 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.769203901 CET	9036	49709	89.163.237.88	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:13:35.769248962 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.769303083 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.769304037 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.769330978 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.769334078 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.769357920 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.769367933 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.790576935 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790621042 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790642977 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790668011 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790690899 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790715933 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790719986 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.790751934 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790777922 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.790802956 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.790873051 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812535048 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812565088 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812588930 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812612057 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812642097 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812647104 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812668085 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812674999 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812699080 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812726974 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812731981 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812767029 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812777996 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812813997 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812839031 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812865973 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812891006 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812891006 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812912941 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812932968 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812944889 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812956095 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.812958956 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.812999964 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.835573912 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835643053 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835685968 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835726023 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835731030 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.835751057 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835777998 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.835789919 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835814953 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835838079 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835839033 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.835876942 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.835890055 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835913897 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835935116 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.835968971 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.835982084 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836005926 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836030006 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836061001 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836070061 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836093903 CET	9036	49709	89.163.237.88	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:13:35.836117029 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836117983 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836141109 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836158037 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836182117 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836205006 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836225986 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836234093 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836266041 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836267948 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836292982 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836317062 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836328030 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836340904 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836365938 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836369991 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836393118 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836417913 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836440086 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836440086 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836464882 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836486101 CET	49709	9036	192.168.2.4	89.163.237.88
Feb 24, 2021 13:13:35.836488962 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836513042 CET	9036	49709	89.163.237.88	192.168.2.4
Feb 24, 2021 13:13:35.836541891 CET	49709	9036	192.168.2.4	89.163.237.88

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:13:05.131644964 CET	59920	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:05.144365072 CET	53	59920	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:06.854136944 CET	57458	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:06.866487980 CET	53	57458	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:07.635777950 CET	50579	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:07.648597956 CET	53	50579	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:08.444322109 CET	65248	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:08.456315041 CET	53	65248	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:09.765423059 CET	53723	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:09.778301001 CET	53	53723	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:10.644164085 CET	64646	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:10.659591913 CET	53	64646	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:11.666393042 CET	65298	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:11.680917978 CET	53	65298	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:13.408221006 CET	59123	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:13.420507908 CET	53	59123	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:14.182230949 CET	54531	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:14.197181940 CET	53	54531	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:15.029716969 CET	49714	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:15.043313026 CET	53	49714	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:15.835571051 CET	58028	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:15.848443031 CET	53	58028	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:16.646267891 CET	53097	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:16.658747911 CET	53	53097	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:17.470582962 CET	49257	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:17.482456923 CET	53	49257	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:18.331350088 CET	62389	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:18.344394922 CET	53	62389	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:19.348400116 CET	49910	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:19.361630917 CET	53	49910	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:20.211576939 CET	55854	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:20.224864006 CET	53	55854	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:21.048191071 CET	64549	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:21.061738968 CET	53	64549	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:21.845335007 CET	63153	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 13:13:21.858378887 CET	53	63153	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:35.121257067 CET	52991	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:35.292083979 CET	53	52991	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:42.266710043 CET	53700	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:42.433168888 CET	53	53700	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:48.899710894 CET	51726	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:48.914328098 CET	53	51726	8.8.8.8	192.168.2.4
Feb 24, 2021 13:13:55.219964027 CET	56794	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:13:55.390961885 CET	53	56794	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:01.710227013 CET	56534	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:01.722053051 CET	53	56534	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:02.238163948 CET	56627	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:02.250988960 CET	53	56627	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:09.074867964 CET	56621	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:09.088027954 CET	53	56621	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:15.085726023 CET	63116	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:15.098505974 CET	53	63116	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:22.417701006 CET	64078	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:22.436132908 CET	53	64078	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:28.412439108 CET	64801	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:28.426688910 CET	53	64801	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:33.431617022 CET	61721	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:33.444726944 CET	53	61721	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:39.464747906 CET	51255	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:39.476856947 CET	53	51255	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:45.461611032 CET	61522	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:45.474519014 CET	53	61522	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:50.474667072 CET	52337	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:50.487652063 CET	53	52337	8.8.8.8	192.168.2.4
Feb 24, 2021 13:14:56.498562098 CET	55046	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:14:56.512487888 CET	53	55046	8.8.8.8	192.168.2.4
Feb 24, 2021 13:15:02.586545944 CET	49612	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:15:02.599725962 CET	53	49612	8.8.8.8	192.168.2.4
Feb 24, 2021 13:15:07.471865892 CET	49285	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:15:07.484658003 CET	53	49285	8.8.8.8	192.168.2.4
Feb 24, 2021 13:15:13.572782993 CET	50601	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:15:13.585798979 CET	53	50601	8.8.8.8	192.168.2.4
Feb 24, 2021 13:15:19.536489010 CET	60875	53	192.168.2.4	8.8.8.8
Feb 24, 2021 13:15:19.549335957 CET	53	60875	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 13:13:35.121257067 CET	192.168.2.4	8.8.8.8	0x9539	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:13:42.266710043 CET	192.168.2.4	8.8.8.8	0x49ac	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:13:48.899710894 CET	192.168.2.4	8.8.8.8	0x4a5f	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:13:55.219964027 CET	192.168.2.4	8.8.8.8	0x63f9	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:02.238163948 CET	192.168.2.4	8.8.8.8	0x77ff	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:09.074867964 CET	192.168.2.4	8.8.8.8	0xb207	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:15.085726023 CET	192.168.2.4	8.8.8.8	0x490f	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:22.417701006 CET	192.168.2.4	8.8.8.8	0xfe97	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:28.412439108 CET	192.168.2.4	8.8.8.8	0x8800	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:33.431617022 CET	192.168.2.4	8.8.8.8	0x5374	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:39.464747906 CET	192.168.2.4	8.8.8.8	0x7d1	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:45.461611032 CET	192.168.2.4	8.8.8.8	0x8527	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 13:14:50.474667072 CET	192.168.2.4	8.8.8.8	0x967e	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:56.498562098 CET	192.168.2.4	8.8.8.8	0x5f52	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:02.586545944 CET	192.168.2.4	8.8.8.8	0x4721	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:07.471865892 CET	192.168.2.4	8.8.8.8	0xe71f	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:13.572782993 CET	192.168.2.4	8.8.8.8	0x8222	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:19.536489010 CET	192.168.2.4	8.8.8.8	0x9f56	Standard query (0)	wilsonzz.webredirect.org	A (IP address)	IN (0x0001)

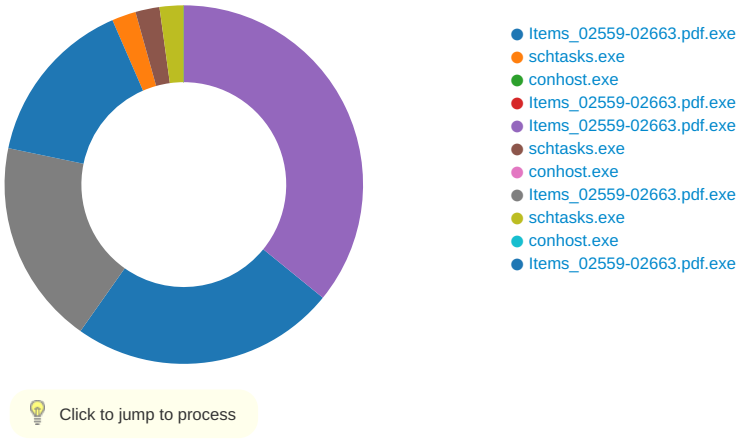
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 13:13:35.292083979 CET	8.8.8.8	192.168.2.4	0x9539	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:13:42.433168888 CET	8.8.8.8	192.168.2.4	0x49ac	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:13:48.914328098 CET	8.8.8.8	192.168.2.4	0x4a5f	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:13:55.390961885 CET	8.8.8.8	192.168.2.4	0x63f9	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:02.250988960 CET	8.8.8.8	192.168.2.4	0x77ff	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:09.088027954 CET	8.8.8.8	192.168.2.4	0xb207	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:15.098505974 CET	8.8.8.8	192.168.2.4	0x490f	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:22.436132908 CET	8.8.8.8	192.168.2.4	0xfe97	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:28.426688910 CET	8.8.8.8	192.168.2.4	0x8800	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:33.444726944 CET	8.8.8.8	192.168.2.4	0x5374	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:39.476856947 CET	8.8.8.8	192.168.2.4	0x7d1	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:45.474519014 CET	8.8.8.8	192.168.2.4	0x8527	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:50.487652063 CET	8.8.8.8	192.168.2.4	0x967e	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:14:56.512487888 CET	8.8.8.8	192.168.2.4	0x5f52	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:02.599725962 CET	8.8.8.8	192.168.2.4	0x4721	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:07.484658003 CET	8.8.8.8	192.168.2.4	0xe71f	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:13.585798979 CET	8.8.8.8	192.168.2.4	0x8222	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)
Feb 24, 2021 13:15:19.549335957 CET	8.8.8.8	192.168.2.4	0x9f56	No error (0)	wilsonzz.webredirect.org		89.163.237.88	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Items_02559-02663.pdf.exe PID: 1680 Parent PID: 5896

General

Start time:	13:13:11
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Items_02559-02663.pdf.exe'
Imagebase:	0x1e0000
File size:	770048 bytes
MD5 hash:	69B99B73945755DF4628529E5A1BF6F8
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: 00000000.00000002.687231789.0000000003B89000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.687231789.0000000003B89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.687231789.0000000003B89000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\jZWRPYaLXncddo.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp71AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Items_02559-02663.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp71AB.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jZWRPYaLXncddo.exe	unknown	770048	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 6f ac 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b6 0b 00 00 08 00 00 00 00 00 00 86 d5 0b 00 00 20 00 00 00 e0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...o.5`.......... ....0................. ....@.. ....@................	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp71AB.tmp	unknown	1647	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	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Items_02559-02663.pdf.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\Desktop\Items_02559-02663.pdf.exe	unknown	770048	success or wait	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 1900 Parent PID: 1680

General

Start time:	13:13:28
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jZWRPYaLXncddo' /XML 'C: \Users\user\AppData\Local\Temp\tmp71AB.tmp'
Imagebase:	0x230000
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\tmp71AB.tmp	unknown	2	success or wait	1	23AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp71AB.tmp	unknown	1648	success or wait	1	23ABD9	ReadFile

Analysis Process: conhost.exe PID: 3220 Parent PID: 1900

General

Start time:	13:13:28
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: Items_02559-02663.pdf.exe PID: 2920 Parent PID: 1680

General

Start time:	13:13:29
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3a0000
File size:	770048 bytes
MD5 hash:	69B99B73945755DF4628529E5A1BF6F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Items_02559-02663.pdf.exe PID: 1440 Parent PID: 1680

General

Start time:	13:13:29
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x990000
File size:	770048 bytes
MD5 hash:	69B99B73945755DF4628529E5A1BF6F8
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: 00000004.00000002.908925138.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.908925138.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.908925138.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.910239733.0000000002D61000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.910239733.0000000002D61000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C01BEFF	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	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	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	6C01BEFF	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	6C01BEFF	CreateDirectoryW
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	17	6C011E60	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	6C011E60	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	6C011E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	success or wait	1	6C016A95	DeleteFileW
C:\Users\user\Desktop\Items_02559-02663.pdf.exe:Zone.Identifier	success or wait	1	6BF92935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	b6 fa e9 99 bd d8 d8 48	.....H	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	unknown	1311	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	48	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 49 74 65 6d 73 5f 30 32 35 35 39 2d 30 32 36 36 33 2e 70 64 66 2e 65 78 65	C:\Users\user\Desktop\Items_02559-02663.pdf.exe	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	8	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C011B4F	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 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C011B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\Desktop\Items_02559-02663.pdf.exe	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Users\user\Desktop\Items_02559-02663.pdf.exe	unknown	512	success or wait	1	6D18D72F	unknown

Analysis Process: schtasks.exe PID: 5716 Parent PID: 1440

General

Start time:	13:13:31
Start date:	24/02/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp'
Imagebase:	0x230000
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\tmp1EF7.tmp	unknown	2	success or wait	1	23AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	unknown	1312	success or wait	1	23ABD9	ReadFile

Analysis Process: conhost.exe PID: 2860 Parent PID: 5716

General

Start time:	13:13:32
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: Items_02559-02663.pdf.exe PID: 472 Parent PID: 968

General

Start time:	13:13:33
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe 0
Imagebase:	0xf60000
File size:	770048 bytes
MD5 hash:	69B99B73945755DF4628529E5A1BF6F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.725225610.0000000004839000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.725225610.0000000004839000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.725225610.0000000004839000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpBA1E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBA1E.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBA1E.tmp	unknown	1647	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	6C011B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 5688 Parent PID: 472

General

Start time:	13:13:46
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jZWRPYaLXncddo' /XML 'C:\Users\user\AppData\Local\Temp\tmpBA1E.tmp'
Imagebase:	0x230000
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\tmpBA1E.tmp	unknown	2	success or wait	1	23AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBA1E.tmp	unknown	1648	success or wait	1	23ABD9	ReadFile

Analysis Process: conhost.exe PID: 5912 Parent PID: 5688

General

Start time:	13:13:47
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: Items_02559-02663.pdf.exe PID: 5880 Parent PID: 472

General

Start time:	13:13:47
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Items_02559-02663.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcf0000
File size:	770048 bytes
MD5 hash:	69B99B73945755DF4628529E5A1BF6F8
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: 0000000A.00000002.735464765.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.735464765.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.735464765.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.738210000.00000000041E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.738210000.00000000041E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.737807407.00000000031E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.737807407.00000000031E1000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Disassembly

Code Analysis