ID: 402887
Sample Name: TT COPY pdf.exe
Cookbook: default.jbs
Time: 15:23:19
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report TT COPY pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 5
Malware Configuration 5
Threatname: NanoCore 5
Yara Overview 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 8
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Data Obfuscation: 8
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 9
Stealing of Sensitive Information: 9
Remote Access Functionality: 9
Mitre Att&ck Matrix 9
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 16
General 16
File Icon 17

Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 19
Resources 19
Imports 20
Version Infos 20
Network Behavior 20
Snort IDS Alerts 20
TCP Packets 20
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 22
Analysis Process: TT COPY pdf.exe PID: 5640 Parent PID: 5680 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 25
Analysis Process: schtasks.exe PID: 6160 Parent PID: 5640 25
General 25
File Activities 26
File Read 26
Analysis Process: conhost.exe PID: 6176 Parent PID: 6160 26
General 26
Analysis Process: TT COPY pdf.exe PID: 6240 Parent PID: 5640 26
General 26
File Activities 27
File Created 27
File Deleted 27
File Written 28
File Read 28
Disassembly 28
Code Analysis 29

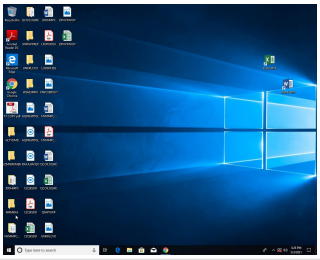
Analysis Report TT COPY pdf.exe

Overview

General Information

Sample Name:	TT COPY pdf.exe
Analysis ID:	402887
MD5:	5c59c6fb72b449b..
SHA1:	85974547f519bab.
SHA256:	0b39f5e8244f6d2..
Tags:	exe NanoCore RAT
Infos:	

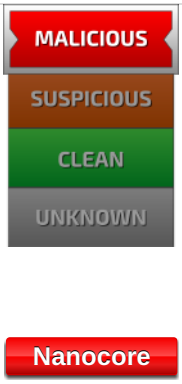
Most interesting Screenshot:



Errors

- Sigma runtime error: Invalid condition: true && ! filter Rule: System File Execution Location Anomaly
- Sigma runtime error: Invalid condition: (false && ! false) or Rule: Executable Used by PlugX in Uncommon Location
- Sigma syntax error: Rules are missing titles
- Sigma runtime error: Invalid condition: false && true or Rule: Suspicious WMI Execution
- Sigma runtime error: Invalid condition: not false && false Rule: Using SettingSyncHost.exe as LOLBin
- Sigma runtime error: Invalid condition: not true && false Rule: Using SettingSyncHost.exe as LOLBin
- Sigma runtime error: Invalid condition: false || (selection_wevtutil_binary && selection_wevtutil_command) Rule: Suspicious Eventlog Clear or Configuration Using Wevtutil
- Sigma runtime error: Invalid condition: false && false or Rule: Suspicious WMI Execution

Detection



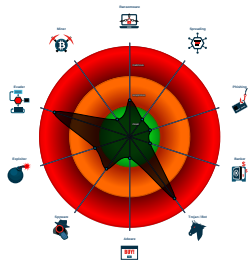
Nanocore

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: BlueMashroom DLL…
- Sigma detected: NanoCore
- Sigma detected: NotPetya Ransomw…
- Sigma detected: QBot Process Crea…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Sigma detected: Exchange Exploita…
- Sigma detected: Mustang Panda Dro…
- Sigma detected: Raccine Uninstall
- Sigma detected: Suspicious Schedu…
- Sigma detected: Windows 10 Sched…
- Tries to detect sandboxes and other…
- Uses schtasks.exe or at.exe to add …
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…
- Contains functionality to detect virtu…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- TT COPY pdf.exe (PID: 5640 cmdline: 'C:\Users\user\Desktop\TT COPY pdf.exe' MD5: 5C59C6FB72B449BD3E52B628C7C46002)
  - schtasks.exe (PID: 6160 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kAozQG' /XML 'C:\Users\user\AppData\Local\Temp\tmp2D06.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - TT COPY pdf.exe (PID: 6240 cmdline: C:\Users\user\Desktop\TT COPY pdf.exe MD5: 5C59C6FB72B449BD3E52B628C7C46002)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "97a824b7-e666-4a22-b2e3-fb501d91",
  "Group": "king",
  "Domain1": "23.105.131.171",
  "Domain2": "",
  "Port": 4040,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "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"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.523106408.00000000058E0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000007.00000002.523106408.00000000058E0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000007.00000002.523106408.00000000058E0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.267284448.00000000039D9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f86a5:$x1: NanoCore.ClientPluginHost • 0x22aec5:$x1: NanoCore.ClientPluginHost • 0x1f86e2:$x2: IClientNetworkHost • 0x22af02:$x2: IClientNetworkHost • 0x1fc215:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x22ea35:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.267284448.00000000039D9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.TT COPY pdf.exe.3a79c68.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x157a3d:$x1: NanoCore.ClientPluginHost • 0x18a25d:$x1: NanoCore.ClientPluginHost • 0x157a7a:$x2: IClientNetworkHost • 0x18a29a:$x2: IClientNetworkHost • 0x15b5ad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x18ddcd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.TT COPY pdf.exe.3a79c68.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.TT COPY pdf.exe.3a79c68.2.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1577a5:$a: NanoCore • 0x1577b5:$a: NanoCore • 0x1579e9:$a: NanoCore • 0x1579fd:$a: NanoCore • 0x157a3d:$a: NanoCore • 0x189fc5:$a: NanoCore • 0x189fd5:$a: NanoCore • 0x18a209:$a: NanoCore • 0x18a21d:$a: NanoCore • 0x18a25d:$a: NanoCore • 0x157804:$b: ClientPlugin • 0x157a06:$b: ClientPlugin • 0x157a46:$b: ClientPlugin • 0x18a024:$b: ClientPlugin • 0x18a226:$b: ClientPlugin • 0x18a266:$b: ClientPlugin • 0xad9a1:$c: ProjectData • 0x15792b:$c: ProjectData • 0x18a14b:$c: ProjectData • 0x158332:$d: DESCrypto • 0x18ab52:$d: DESCrypto
7.2.TT COPY pdf.exe.3eeff1c.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.TT COPY pdf.exe.3eeff1c.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
Click to see the 36 entries				

Sigma Overview

System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: NanoCore

Sigma detected: NotPetya Ransomware Activity

Sigma detected: QBot Process Creation

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Exchange Exploitation Activity

Sigma detected: Mustang Panda Dropper

Sigma detected: Raccine Uninstall

Sigma detected: Suspicious Scheduled Task Creation Involving Temp Folder

Sigma detected: Windows 10 Scheduled Task SandboxEscaper 0-day

Sigma detected: PowerShell Script Run in AppData

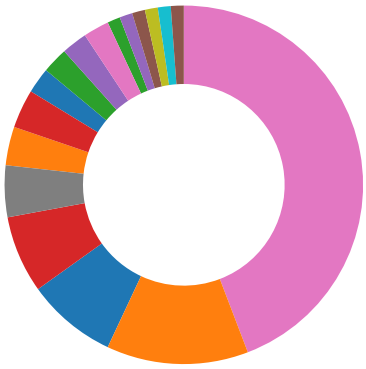
Sigma detected: Suspicious Copy From or To System32

Sigma detected: Change Default File Association

Sigma detected: Data Compressed - Powershell

Signature Overview

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



Click to jump to signature section

AV Detection:

- 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

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)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

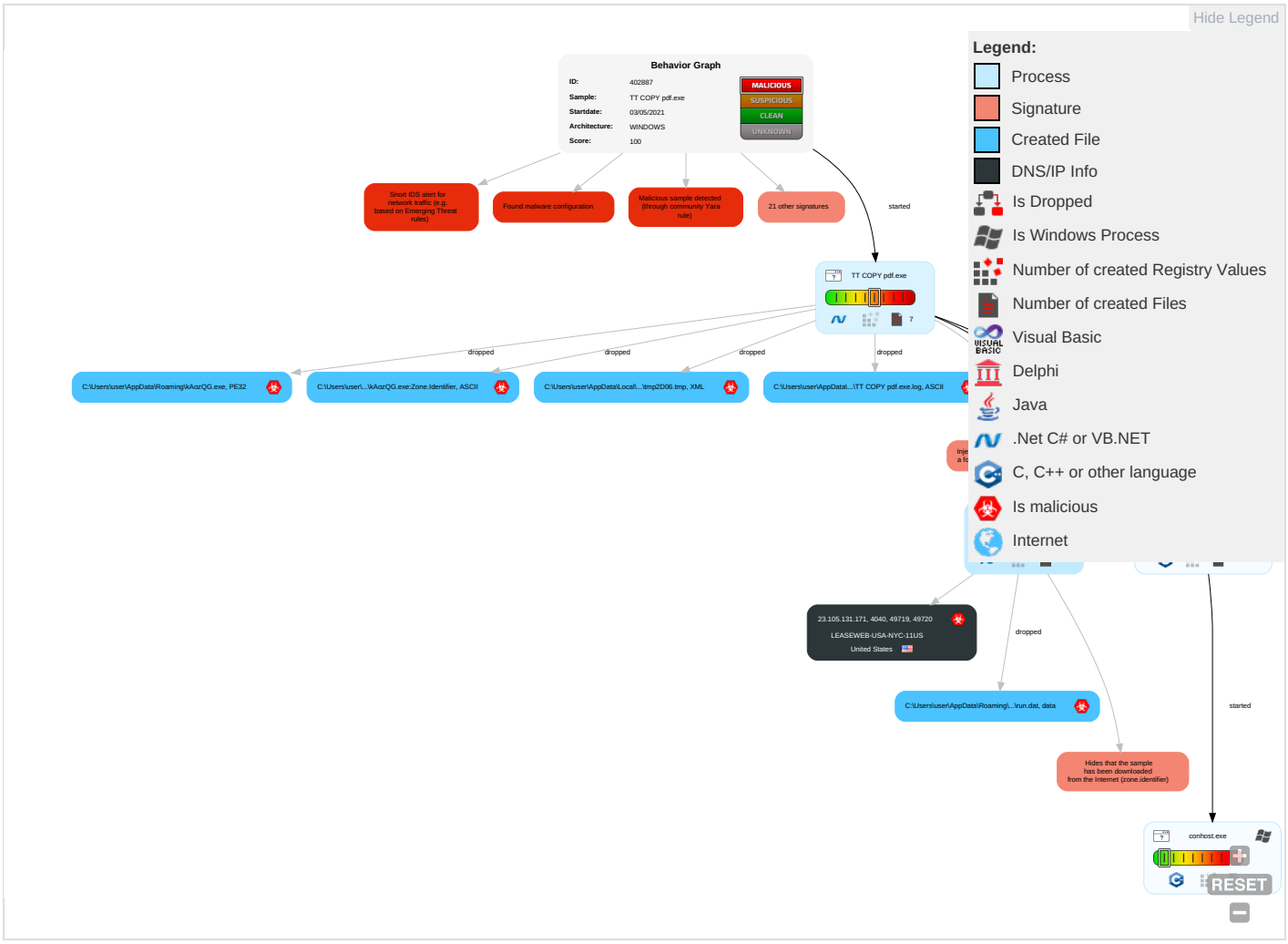
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
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	Application Layer Protocol 1	SIM C Swap
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	Fallback Channels	Manip Device Comm
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	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
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	Downg Insecu Protoc

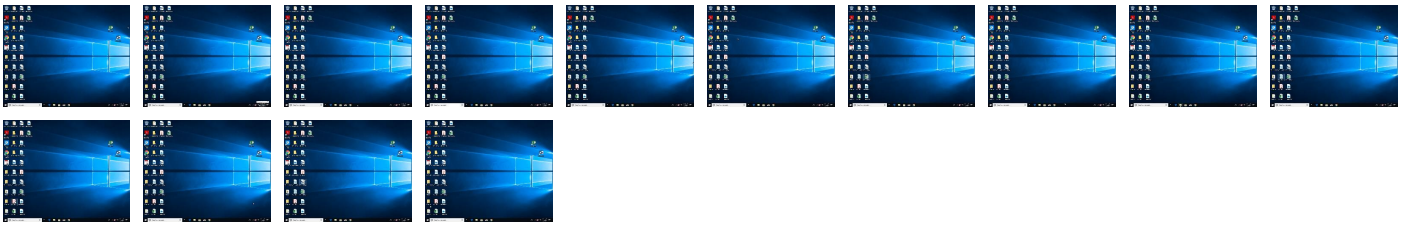
Behavior Graph



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
TT COPY pdf.exe	19%	ReversingLabs	Win32.Trojan.AgentTesla	
TT COPY pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kAozQG.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kAozQG.exe	19%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.TT COPY pdf.exe.58e0000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
7.2.TT COPY pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
23.105.131.171	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
23.105.131.171	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	TT COPY pdf.exe, 00000000.00000002.266683810.00000000029D1000.00000004.00000001.sdmp	false		high
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	TT COPY pdf.exe, 00000000.00000002.266683810.00000000029D1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402887
Start date:	03.05.2021
Start time:	15:23:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TT COPY 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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/6@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 77.5% • Quality standard deviation: 11.1%
HCA Information:	• Successful, ratio: 98% • 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 • 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.
Errors:	• Sigma runtime error: Invalid condition: true && ! filter Rule: System File Execution Location Anomaly • Sigma runtime error: Invalid condition: (false && ! false) or Rule: Executable Used by PlugX in Uncommon Location • Sigma syntax error: Rules are missing titles • Sigma runtime error: Invalid condition: false && true or Rule: Suspicious WMI Execution • Sigma runtime error: Invalid condition: not false && false Rule: Using SettingSyncHost.exe as LOLBin • Sigma runtime error: Invalid condition: not true && false Rule: Using SettingSyncHost.exe as LOLBin • Sigma runtime error: Invalid condition: false || (selection_wevtutil_binary && selection_wevtutil_command) Rule: Suspicious Eventlog Clear or Configuration Using Wevtutil • Sigma runtime error: Invalid condition: false && false or Rule: Suspicious WMI Execution

Simulations

Behavior and APIs

Time	Type	Description
15:24:22	API Interceptor	1008x Sleep call for process: TT COPY pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.105.131.171	transfer pdf.exe	Get hash	malicious	Browse	
	DHLAWB# 9284880911 pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	transfer pdf.exe	Get hash	malicious	Browse	• 23.105.131.171
	DHLAWB# 9284880911 pdf.exe	Get hash	malicious	Browse	• 23.105.131.171
	PO.pdf.exe	Get hash	malicious	Browse	• 23.105.131.190
	PO.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	SecuriteInfo.com.Trojan.Win32.Save.a.29244.exe	Get hash	malicious	Browse	• 23.105.131.161
	ZBgnuLqtOd.exe	Get hash	malicious	Browse	• 23.105.131.161
	ZE9u48l6N4.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO copy.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	invoice&packing list.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO.PDF.exe	Get hash	malicious	Browse	• 23.105.131.161
	PO copy.pdf.exe	Get hash	malicious	Browse	• 23.105.131.161
	Ordem urgente AWB674653783- FF2453,PDF.exe	Get hash	malicious	Browse	• 23.105.131.132
	Remittance FormDoc.exe	Get hash	malicious	Browse	• 23.19.227.243
	Presupuesto de orden urgente KTX88467638,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	Dringende Bestellung Zitat CTX88467638,pdf.exe	Get hash	malicious	Browse	• 23.105.131.132
	shipping document.exe	Get hash	malicious	Browse	• 23.105.131.207
	6V9espP5wD.exe	Get hash	malicious	Browse	• 23.105.131.195
	NVAbIqNO9h.exe	Get hash	malicious	Browse	• 23.105.131.209
	UUGCfhIdFD.exe	Get hash	malicious	Browse	• 23.105.131.228

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TT COPY pdf.exe.log

Process:	C:\Users\user\Desktop\TT COPY pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TT COPY pdf.exe.log

Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F 8
Malicious:	**true**
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

C:\Users\user\AppData\Local\Temp\tmp2D06.tmp

Process:	C:\Users\user\Desktop\TT COPY pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.172308050226336
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBdYtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3q
MD5:	92AE123C43B9118A157C6477DE51F190
SHA1:	BD3D84B3C0ABF082DD803ACE91AD9F95EAA170BF
SHA-256:	4FFAFB8ABE72A998C286BFAFB3288EC2CFD1F5029DE737FE298015B781F95FF0
SHA-512:	BB94339B70FF6CE7FDD060A00DB5966162053DE2858D5206F9F1BE5F5A224410DF6987198507439ACDACAC582431867942372EB24FB8E9AC05E9CEB8FA580F3
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>t

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

Process:	C:\Users\user\Desktop\TT COPY pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	928
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtw:Ik/lCrwfk/lCrwfk/lCrwfk/lCrw8
MD5:	CCB690520E68EE385ACC0ACFE759AFFC
SHA1:	33F0DA3F55E5B3C5AC19B61D31471CB60BCD5C96
SHA-256:	166154225DAB5FCB79C1CA97D371B159D37B83FBC0ADABCD8EBA98FA113A7A3B
SHA-512:	AC4F3CF1F8F460745D37E6350861C2FBCDDCC1BBDE0A48FB361BFBF5B1EBF10A05F798A72CE413FCA073FF8108955353DDBCBD9D50CED6CDAE231C67A28F DA3
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\TT COPY pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Encrypted:	false
SSDEEP:	3:r8:r8
MD5:	2DEDC34235C5260F4D29ECFE8E9F7C2B
SHA1:	3C68D1B9BD902EF465531028D4A212CC2D45D0EF
SHA-256:	51F73BE61DCC9973EDA643C38632AA52C5E8E63391050625D4CB5CC9789A2A01
SHA-512:	A92A0A52162300C3EAB9F971481DA753E1E8DA7845DBCF937C05C93943B815688CED61FCB77795DE1308EE1CB6C352AD51D1CABCD26A83154B81933C42313C2
Malicious:	**true**
Reputation:	low
Preview:	...7...H

C:\Users\user\AppData\Roaming\kAozQG.exe	
Process:	C:\Users\user\Desktop\TT COPY pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	906752
Entropy (8bit):	7.6609636801645715
Encrypted:	false
SSDEEP:	24576:Dg1zTaZViWg3XO7OJYidZ7x0oTSZikoIErs:DS/aZVHoXO72h0odgErs
MD5:	5C59C6FB72B449BD3E52B628C7C46002
SHA1:	85974547F519BABCDD3F8D5A68BA18930F09D46D
SHA-256:	0B39F5E8244F6D24DBF99914E31907F8E560C6612544A692EC97480C5C9FE371
SHA-512:	8C4B83A321E0AF75E9F3C77A10D41E005401E6747A92BBF3F251B76663267D5A6C917801AA791AF964DDB0F5740735CFBFD71BBA1A4E91DFCEDE3B132A9750FA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[.`.....P..x...\..... .....@.. ..... ..... .@.....O.....Y..... ..... ..H.....text....w... ...x..... ..`.rsrc....Y.....Z...z.....@..@.relo c.....@..B.....H.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... ....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r7..p ~....o-...(.....t$....+..*...0..&.....(....rE..p~....o-...(.....

C:\Users\user\AppData\Roaming\kAozQG.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\TT COPY pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6609636801645715

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	TT COPY pdf.exe
File size:	906752
MD5:	5c59c6fb72b449bd3e52b628c7c46002
SHA1:	85974547f519babcdd3f8d5a68ba18930f09d46d
SHA256:	0b39f5e8244f6d24dbf99914e31907f8e560c6612544a692ec97480c5c9fe371
SHA512:	8c4b83a321e0af75e9f3c77a10d41e005401e6747a92bbf3f251b76663267d5a6c917801aa791af964ddb0f5740735cfbfd71bba1a4e91dfcede3b132a9750fa
SSDEEP:	24576:Dg1zTaZViWg3XO7OJYidZ7x0oTSZikoIErs:DS/aZVHoXO72h0odgErs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...[.`.....P..x...\..... .....@.. ....@.....

File Icon

Icon Hash:	1d1949485b2d1e1e

Static PE Info

General

Entrypoint:	0x4d9712
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:	0x608FF45B [Mon May 3 13:02:19 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd96c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xda000	0x598c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe0000	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	0xd7718	0xd7800	False	0.849151682135	data	7.69430817012	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xda000	0x598c	0x5a00	False	0.353776041667	data	4.54268336105	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xda160	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294901502		
RT_ICON	0xdb208	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_GROUP_ICON	0xdf430	0x22	data		
RT_VERSION	0xdf454	0x34c	data		
RT_MANIFEST	0xdf7a0	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 2009 - 2021
Assembly Version	1.0.5.0
InternalName	EventTags.exe
FileVersion	1.0.5.0
CompanyName	Cendario
LegalTrademarks	
Comments	
ProductName	Forge Templer
ProductVersion	1.0.5.0
FileDescription	Forge Templer
OriginalFilename	EventTags.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-15:24:30.918264	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	4040	192.168.2.5	23.105.131.171
05/03/21-15:24:38.891607	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	4040	192.168.2.5	23.105.131.171
05/03/21-15:24:45.893883	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	4040	192.168.2.5	23.105.131.171
05/03/21-15:24:52.914072	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	4040	192.168.2.5	23.105.131.171
05/03/21-15:26:29.950949	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	4040	192.168.2.5	23.105.131.171

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 15:24:30.503123045 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:30.833909988 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:30.834101915 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:30.918263912 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:31.262438059 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:31.390827894 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:31.720134020 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:31.767025948 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:31.797579050 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.228486061 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.228569984 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.228790998 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.229001999 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.229042053 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.229078054 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.230318069 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.230395079 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.230513096 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.230573893 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.230597973 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.230659008 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.231997013 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.232072115 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.232079029 CEST	4040	49719	23.105.131.171	192.168.2.5

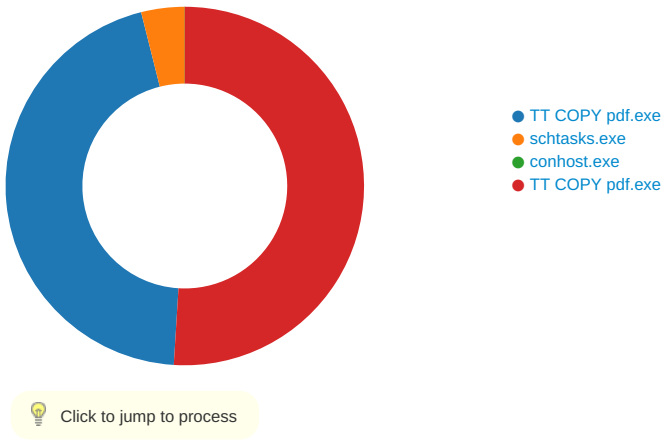
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 15:24:32.232145071 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.233521938 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.233561039 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.233608007 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.233633995 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.565164089 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.566549063 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.566694021 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.566776991 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.568584919 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.568681002 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.568696022 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.569204092 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.569262028 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.569305897 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.569802999 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.569946051 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.571118116 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.571337938 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.571425915 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.572271109 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.572540998 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.572628975 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.590037107 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.590208054 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.590271950 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.590358019 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.590512991 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.590646982 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.597157001 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.597269058 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.597349882 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.598556042 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.598632097 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.598702908 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.815001965 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.902785063 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.902865887 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.903785944 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.903841972 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.904007912 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.904066086 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.904623032 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.904685974 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.914709091 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.914766073 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.914891958 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.914963961 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.915288925 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.915338039 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.915934086 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.915982962 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.916174889 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.916230917 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.916404009 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.916452885 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.916769981 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.916840076 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.916882992 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.916929007 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.917529106 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.917582989 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.918248892 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.918337107 CEST	49719	4040	192.168.2.5	23.105.131.171

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 15:24:32.918483019 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.918533087 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.918927908 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.918986082 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.919127941 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.919198036 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.920212030 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.920274973 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.920568943 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.920620918 CEST	49719	4040	192.168.2.5	23.105.131.171
May 3, 2021 15:24:32.921133041 CEST	4040	49719	23.105.131.171	192.168.2.5
May 3, 2021 15:24:32.921190023 CEST	49719	4040	192.168.2.5	23.105.131.171

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: TT COPY pdf.exe PID: 5640 Parent PID: 5680

General

Start time:	15:24:21
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\TT COPY pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TT COPY pdf.exe'
Imagebase:	0x520000
File size:	906752 bytes
MD5 hash:	5C59C6FB72B449BD3E52B628C7C46002
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: 00000000.00000002.267284448.00000000039D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.267284448.00000000039D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.267284448.00000000039D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.266683810.00000000029D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\kAozQG.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Roaming\kAozQG.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2D06.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TT COPY pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2D06.tmp	success or wait	1	6CB16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kAozQG.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5b f4 8f 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 78 0d 00 00 5c 00 00 00 00 00 00 12 97 0d 00 00 20 00 00 00 a0 0d 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 0e 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... [..`.............P..x...\.......... ....@.. ....@................	success or wait	4	6CB1DD66	CopyFileW
C:\Users\user\AppData\Roaming\kAozQG.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2D06.tmp	unknown	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TT COPY 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	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: schtasks.exe PID: 6160 Parent PID: 5640

General

Start time:	15:24:25
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kAozQG' /XML 'C:\Users\user\AppData\Local\Temp\tmp2D06.tmp'
Imagebase:	0xda0000
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\tmp2D06.tmp	unknown	2	success or wait	1	DAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2D06.tmp	unknown	1644	success or wait	1	DAABD9	ReadFile

Analysis Process: conhost.exe PID: 6176 Parent PID: 6160

General

Start time:	15:24:26
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: TT COPY pdf.exe PID: 6240 Parent PID: 5640

General

Start time:	15:24:26
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\TT COPY pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\TT COPY pdf.exe
Imagebase:	0x8d0000
File size:	906752 bytes
MD5 hash:	5C59C6FB72B449BD3E52B628C7C46002
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: 00000007.00000002.523106408.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.523106408.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.523106408.00000000058E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.522969256.0000000005830000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.522969256.0000000005830000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.518288271.0000000002EA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.521801480.0000000003EE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.521801480.0000000003EE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.516107579.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.516107579.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.516107579.0000000000402000.00000040.00000001.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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB1BEFF	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	6CB11E60	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	6CB1BEFF	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	6CB1BEFF	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	3	6CB11E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\TT COPY pdf.exe:Zone.Identifier	success or wait	1	6CA92935	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	a7 b8 8a 37 82 0e d9 48	...7...H	success or wait	1	6CB11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	4	6CB11B4F	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\Desktop\TT COPY pdf.exe	unknown	4096	success or wait	1	6DC8D72F	unknown
C:\Users\user\Desktop\TT COPY pdf.exe	unknown	512	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DC8D72F	unknown

Disassembly

Code Analysis