ID: 323809
Sample Name: checklist pdf.exe
Cookbook: default.jbs
Time: 15:23:56
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

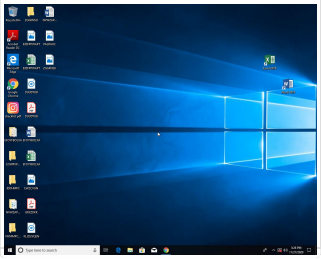
Analysis Report checklist pdf.exe

Overview

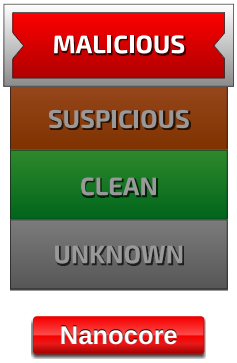
General Information

Sample Name:	checklist pdf.exe
Analysis ID:	323809
MD5:	33fb3c28df0f678…
SHA1:	ab7fbfdaf59bf4d6..
SHA256:	5295f63f8452d5a..
Tags:	exe NanoCore

Most interesting Screenshot:



Detection

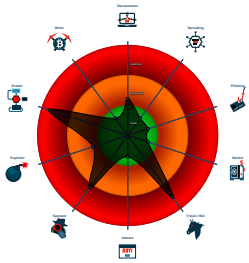


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code references suspic…
- Contains functionality to log keystro…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- checklist pdf.exe (PID: 4728 cmdline: 'C:\Users\user\Desktop\checklist pdf.exe' MD5: 33FB3C28DF0F678C7C6EF72E7E748CB1)
  - schtasks.exe (PID: 6100 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\PUalpOJlfJW' /XML 'C:\Users\user\AppData\Local\Temp\tmpECD4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - checklist pdf.exe (PID: 4648 cmdline: {path} MD5: 33FB3C28DF0F678C7C6EF72E7E748CB1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.501688763.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000002.501688763.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.501688763.000000000040 2000.00000040.00000001.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:$j: #=q
00000000.00000002.249652144.00000000039C 9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x130445:$x1: NanoCore.ClientPluginHost • 0x130482:$x2: IClientNetworkHost • 0x133fb5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.249652144.00000000039C 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.checklist pdf.exe.5440000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
3.2.checklist pdf.exe.5440000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
3.2.checklist pdf.exe.59b0000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
3.2.checklist pdf.exe.59b0000.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
3.2.checklist pdf.exe.59b0000.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

Sigma Overview

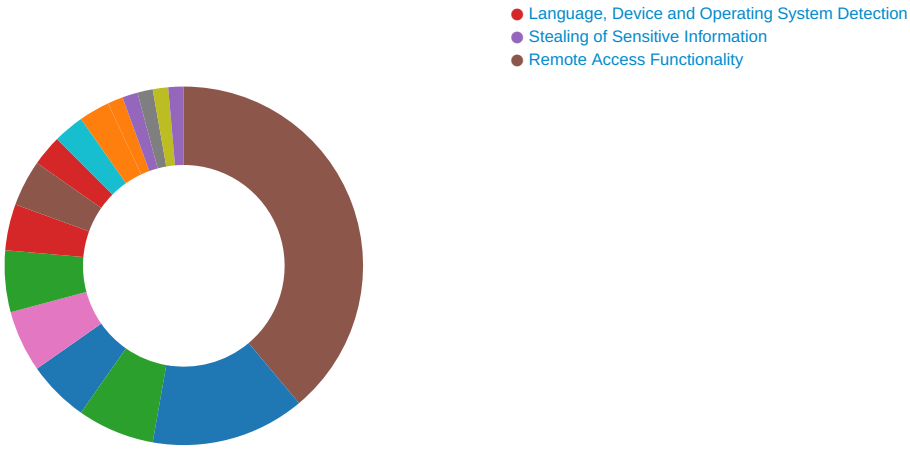
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- 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



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

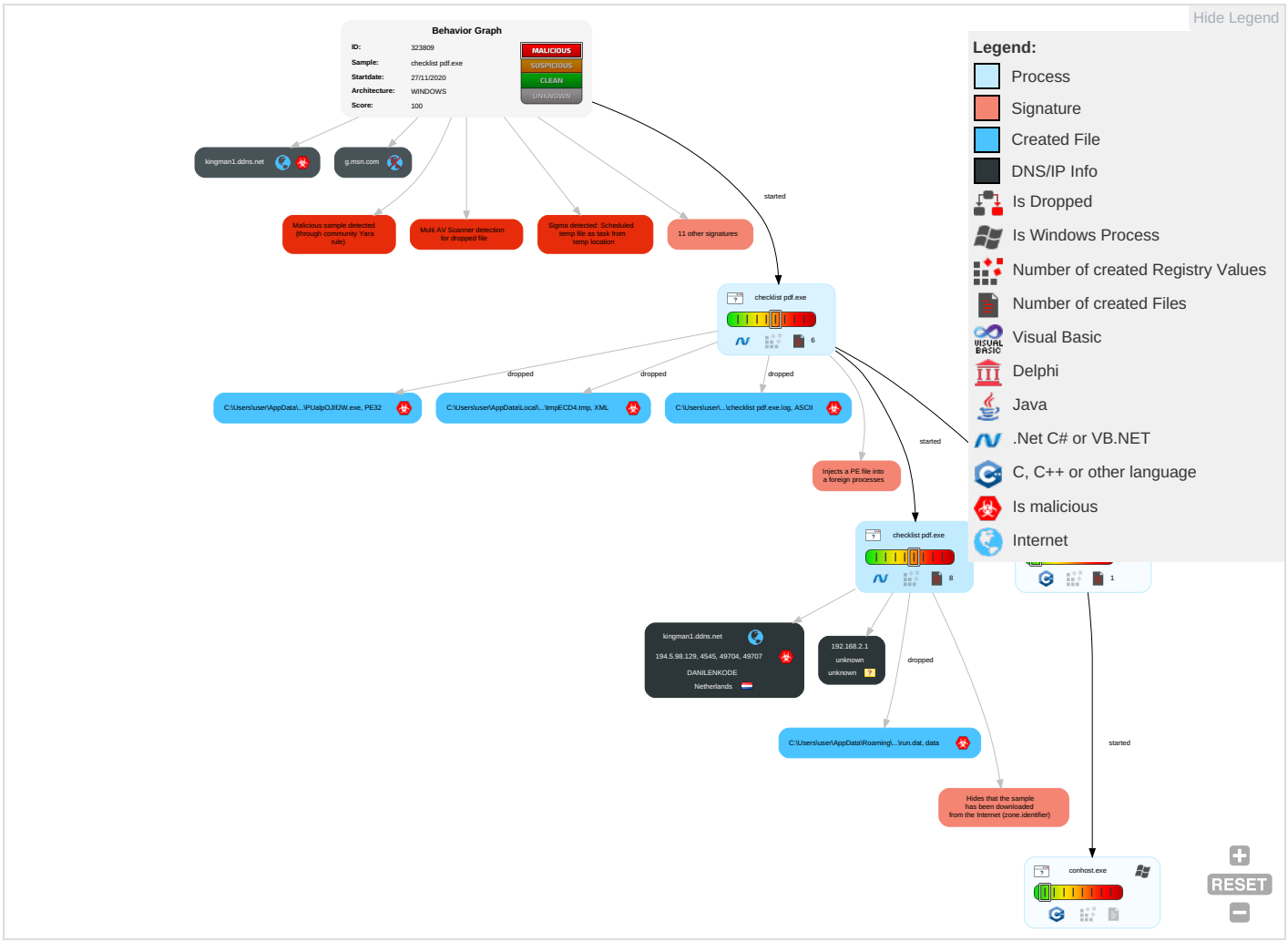
Detected Nanocore Rat

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	Native API 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	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)	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	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	Process Injection 1 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

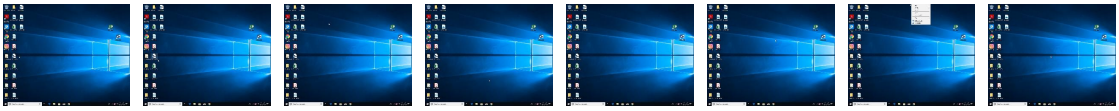
Behavior Graph



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
checklist pdf.exe	32%	Virustotal		Browse
checklist pdf.exe	38%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\PUalpOJIfJW.exe	38%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.checklist pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.checklist pdf.exe.59b0000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/J	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/E	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.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/E	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0s	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnM1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/v	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.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.jiyu-kobo.co.jp/v	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cna	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnb-n	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.comE	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.founder.com.c&	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.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
kingman1.ddns.net	194.5.98.129	true	true		unknown
g.msn.com	unknown	unknown	false		high

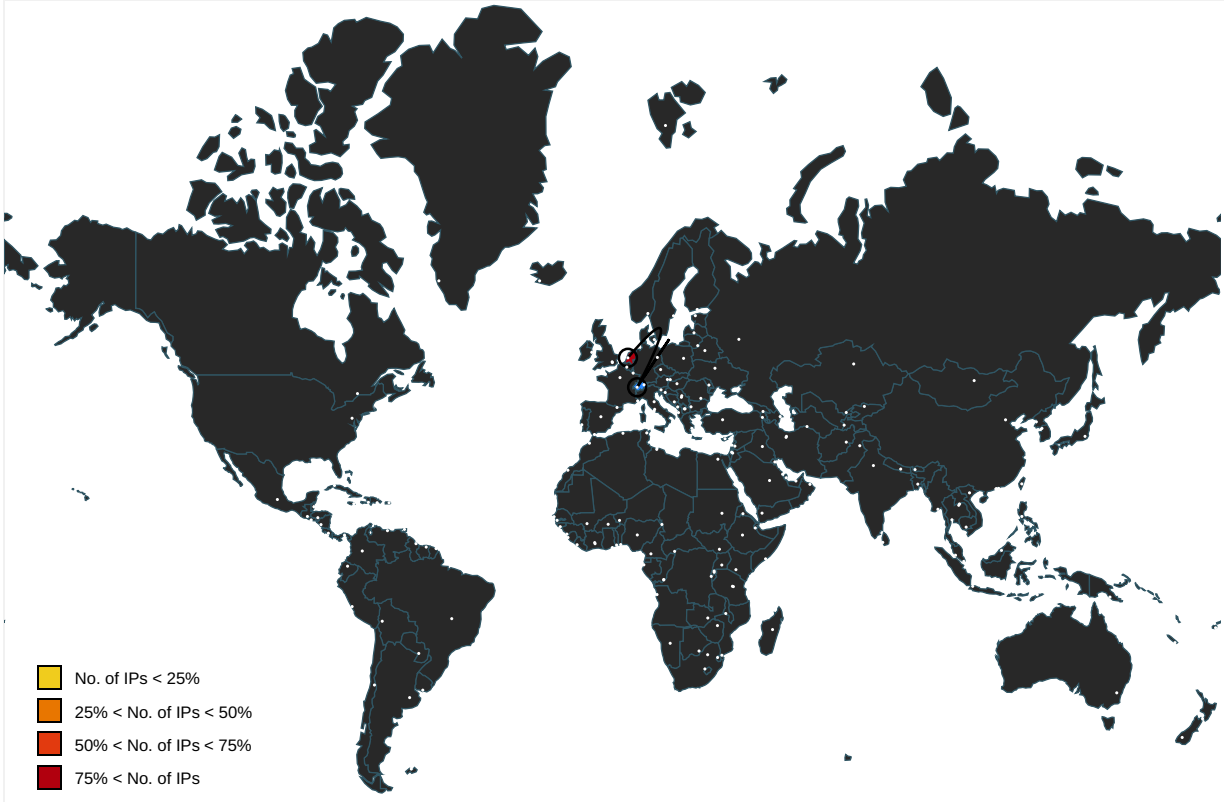
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coma	checklist pdf.exe, 00000000.00000003.236008822.0000000004E63000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/X	checklist pdf.exe, 00000000.00000003.236517335.0000000004E5C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	checklist pdf.exe, 00000000.00000003.236517335.0000000004E5C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/P	checklist pdf.exe, 00000000.00000003.236369930.0000000004E56000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/J	checklist pdf.exe, 00000000.00000003.236619084.0000000004E57000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://coinmarketcap.com/api/	checklist pdf.exe	false		high
http://www.jiyu-kobo.co.jp/Y0/E	checklist pdf.exe, 00000000.00000003.236517335.0000000004E5C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/H	checklist pdf.exe, 00000000.00000003.236448569.0000000004E5D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/E	checklist pdf.exe, 00000000.00000003.236619084.0000000004E57000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0s	checklist pdf.exe, 00000000.00000003.236517335.0000000004E5C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://https://api.coinmarketcap.com/v1/ticker/	checklist pdf.exe	false		high
http://www.goodfont.co.kr	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnM1	checklist pdf.exe, 00000000.00000003.235767459.0000000004E5F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	checklist pdf.exe, 00000000.00000003.236517335.0000000004E5C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/v	checklist pdf.exe, 00000000.00000003.236517335.0000000004E5C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	checklist pdf.exe, 00000000.00000003.246990634.0000000004E50000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	checklist pdf.exe, 00000000.00000003.235767459.0000000004E5F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/v	checklist pdf.exe, 00000000.00000003.236448569.0000000004E5D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cna	checklist pdf.exe, 00000000.00000003.235981732.0000000004E64000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnb-n	checklist pdf.exe, 00000000.00000003.235869978.0000000004E63000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.come.comE	checklist pdf.exe, 00000000.00000003.246990634.0000000004E50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	checklist pdf.exe, 00000000.00000003.236732753.0000000004E5D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0	checklist pdf.exe, 00000000.00000003.236732753.0000000004E5D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false		high
http://www.fonts.com	checklist pdf.exe, 00000000.00000002.247712407.0000000000D27000.00000004.00000040.sdmp	false		high
http://www.founder.com.c&	checklist pdf.exe, 00000000.00000003.235767459.0000000004E5F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sandoll.co.kr	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	checklist pdf.exe, 00000000.00000002.251725059.0000000004F40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.129	unknown	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323809
Start date:	27.11.2020
Start time:	15:23:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	checklist 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:	22
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.spyw.evad.winEXE@6/4@23/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.79.90.110, 52.147.198.201, 13.88.21.125, 51.104.144.132, 20.54.26.129, 205.185.216.10, 205.185.216.42, 51.103.5.186, 52.142.114.176, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:24:53	API Interceptor	1035x Sleep call for process: checklist pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	PEDIDO-6764,pdf.exe	Get hash	malicious	Browse	• 194.5.98.14
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 194.5.98.78
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 194.5.97.9
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 194.5.97.9
	19112020778IMG78487784.exe	Get hash	malicious	Browse	• 194.5.97.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentConformation.exe	Get hash	malicious	Browse	• 194.5.97.202
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 194.5.98.122
	IMAGE-18112020.exe	Get hash	malicious	Browse	• 194.5.97.17
	Covid-19 relief.exe	Get hash	malicious	Browse	• 194.5.97.21
	tax-relief.exe	Get hash	malicious	Browse	• 194.5.97.166
	Ref-BID PRICE.exe	Get hash	malicious	Browse	• 194.5.98.252
	1ttmgYD97B.exe	Get hash	malicious	Browse	• 194.5.99.163
	2mtUEXin7W.exe	Get hash	malicious	Browse	• 194.5.99.163
	wk59hOo880.exe	Get hash	malicious	Browse	• 194.5.99.163
	BCVaSYrgmG.exe	Get hash	malicious	Browse	• 194.5.99.163
	30203490666.exe	Get hash	malicious	Browse	• 194.5.98.199
	InSppuoN2s.exe	Get hash	malicious	Browse	• 194.5.98.196
	Av01vC7kS1.exe	Get hash	malicious	Browse	• 194.5.97.155
	yb1rlaFJuO.exe	Get hash	malicious	Browse	• 194.5.99.163
	1MwYrZqjEy.exe	Get hash	malicious	Browse	• 194.5.99.163

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\checklist pdf.exe.log	
Process:	C:\Users\user\Desktop\checklist pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	777
Entropy (8bit):	5.26742276088186
Encrypted:	false
SSDEEP:	24:MLF20NaL329hJ5g522rW26K95rKoO2I3rOz2T:MwLLG9h3go2rx6oxkr+2T
MD5:	2B6C737933EA1F082E0AA5CF21FE4B27
SHA1:	AB8133CDDD6361EC01FC5C6F2434A0666C764A62
SHA-256:	3D9DC8F0D25AFD18708145A78CF868393C4FD99989D02E090080C93A680680F9
SHA-512:	72E6087A511A26BD1811F74468D2D72A84818C0A8BB2F8CB72FFAD5FA8440E176F2238311DD9644F3CA3007E11DAB71B8CB62323400F25A7D61FBAB7CF329968
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Web\d05d469d89b319a068f2123e7e6f8621\System.Web.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpECD4.tmp	
Process:	C:\Users\user\Desktop\checklist pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	5.17327511273268
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3Q
MD5:	95DB87F25A16CF410E85B362AF9E8C54
SHA1:	0E2E257BFE1735C46F12884B7F525DE75C528617
SHA-256:	49635271511342 93B0D4E677DB01EAE3CB0FD852A47FA6D98C92F9AE8AEE13D6
SHA-512:	100AD6AAE6DD06783F8CFFB5378BA3FCCBE6BDB2767ABFF156F72A79F67073CCFB614EAE1D693E6057A6F32231C4F39A16EF059BA6DA31B3A7B964295AD883F7
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmpECD4.tmp	
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\run.dat	
Process:	C:\Users\user\Desktop\checklist pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:4N29t:4Nat
MD5:	1E849DE2B5A6913898333D1F94BCE8B7
SHA1:	217ED3764189A0E975CAEDC45368F292AF096215
SHA-256:	735F07332B146A283995E832359A13973DB93A3DB051E65AE1FCAA980F96F1B8
SHA-512:	D2196DA8B1C79B182A949E23519DEE669DE2A33B98126807D5AD08B61CEFDE55A0C5951A6BD89546E41C86D59D8B08F7CC8B5088B29254DE0D43087FC57025
Malicious:	**true**
Reputation:	low
Preview:	DS..+..H

C:\Users\user\AppData\Roaming\PUalpOJlfJW.exe	
Process:	C:\Users\user\Desktop\checklist pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	574464
Entropy (8bit):	7.516903184797801
Encrypted:	false
SSDEEP:	12288:3rrzEvkQwHE8Xk4ERhrRarQPY4Rt8LFNo:nY89k8LEfdarQP58
MD5:	33FB3C28DF0F678C7C6EF72E7E748CB1
SHA1:	AB7FBFDAF59BF4D6C79BB7ACF2B59DAD316675F9
SHA-256:	5295F63F8452D5AC0FC3577CB720949DB21EFE807059E0A74CADD4D9BBBC941F
SHA-512:	23950E6FCDAA53C881C6B140A48B1A78741798E12FED6CFF87502059097B34CE808B93A9C4FE6C2D34A2179A54ACB12AF7FBA4AC80F68A6FD646E783B4F25E2B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0..~...D..... .....@.. ....@..... .....O.....A..... ....H.....text....}... ...~..... ..`.rsrc....A.....B.....@..@.relo c.....@..B.....H.....H.....H...H}.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*....0..)... .....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*..s....}.....~....}.....(.....(.....*.0.....(.....(.....*.....0..4.....r...p(.....s....}.....{.....(....}... .*...{....(....&*..0.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.516903184797801
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	checklist pdf.exe
File size:	574464
MD5:	33fb3c28df0f678c7c6ef72e7e748cb1
SHA1:	ab7fbfdaf59bf4d6c79bb7acf2b59dad316675f9

General

SHA256:	5295f63f8452d5ac0fc3577cb720949db21efe807059e0a74cadd4d9bbbc941f
SHA512:	23950e6fcdaa53c881c6b140a48b1a78741798e12fed6cff87502059097b34ce808b93a9c4fe6c2d34a2179a54acb12af7fba4ac80f68a6fd646e783b4f25e2b
SSDEEP:	12288:3rrzEvkQwHE8Xk4ERhrRarQPY4Rt8LFNo:nY89k8LEfdarQP58
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0..~...D..... .....@.. ....@.....

File Icon

Icon Hash:	f8c492aaaa92dcfe

Static PE Info

General

Entrypoint:	0x489ce2
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:	0x5FBFA986 [Thu Nov 26 13:11:34 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, 00h
adc byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
or byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add eax, 04000000h
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [edx], al
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [ecx], cl
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x89c90	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x41e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x90000	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	0x87d18	0x87e00	False	0.758976828427	data	7.54197829505	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x41e8	0x4200	False	0.506569602273	data	5.46524750156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x90000	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	0x8a190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x8a5f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0x8b6a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3771611807, next used block 3167566498		
RT_GROUP_ICON	0x8dc48	0x30	data		
RT_VERSION	0x8dc78	0x384	data		
RT_MANIFEST	0x8dffc	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 2018
Assembly Version	0.9.0.0

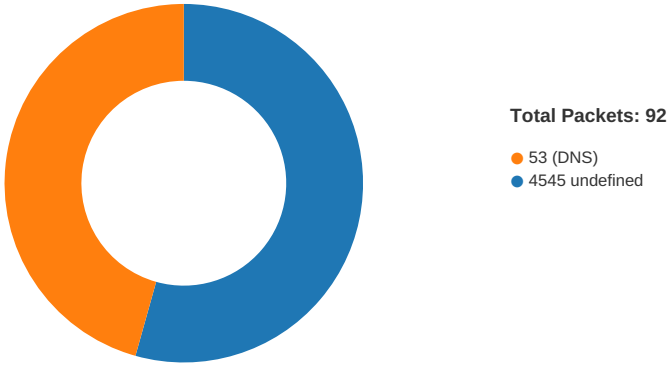
Description	Data
InternalName	z.exe
FileVersion	0.9.0.0
CompanyName	
LegalTrademarks	
Comments	A simple ticker to display various cryptocurrency prices
ProductName	SimpleTicker
ProductVersion	0.9.0.0
FileDescription	SimpleTicker
OriginalFilename	z.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-15:25:11.690596	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:24:58.405519009 CET	49704	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:24:58.650526047 CET	4545	49704	194.5.98.129	192.168.2.5
Nov 27, 2020 15:24:59.198980093 CET	49704	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:24:59.440412998 CET	4545	49704	194.5.98.129	192.168.2.5
Nov 27, 2020 15:24:59.949325085 CET	49704	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:00.360718012 CET	4545	49704	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:04.523170948 CET	49707	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:04.830581903 CET	4545	49707	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:05.340272903 CET	49707	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:05.600172043 CET	4545	49707	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:06.105927944 CET	49707	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:06.360011101 CET	4545	49707	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:11.691922903 CET	49715	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:11.930038929 CET	4545	49715	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:12.434484959 CET	49715	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:12.680125952 CET	4545	49715	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:13.184556961 CET	49715	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:13.430128098 CET	4545	49715	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:17.513664007 CET	49721	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:17.740284920 CET	4545	49721	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:18.247497082 CET	49721	4545	192.168.2.5	194.5.98.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:25:18.530086040 CET	4545	49721	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:19.044388056 CET	49721	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:19.260154009 CET	4545	49721	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:23.338351965 CET	49724	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:23.570322037 CET	4545	49724	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:24.076122046 CET	49724	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:24.390094995 CET	4545	49724	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:24.904268026 CET	49724	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:25.150145054 CET	4545	49724	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:29.242217064 CET	49726	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:29.480413914 CET	4545	49726	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:29.982908964 CET	49726	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:30.340281963 CET	4545	49726	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:30.842274904 CET	49726	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:31.100343943 CET	4545	49726	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:35.466732025 CET	49728	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:35.680409908 CET	4545	49728	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:36.186460972 CET	49728	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:36.480526924 CET	4545	49728	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:37.014648914 CET	49728	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:37.450448036 CET	4545	49728	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:41.634223938 CET	49732	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:41.970936060 CET	4545	49732	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:42.483820915 CET	49732	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:42.861203909 CET	4545	49732	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:43.374552011 CET	49732	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:43.630310059 CET	4545	49732	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:47.873739958 CET	49739	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:48.110625982 CET	4545	49739	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:48.624947071 CET	49739	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:48.910851955 CET	4545	49739	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:49.421907902 CET	49739	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:49.640892029 CET	4545	49739	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:53.760840893 CET	49740	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:54.130446911 CET	4545	49740	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:54.641273022 CET	49740	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:54.910104036 CET	4545	49740	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:55.413660049 CET	49740	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:25:55.850143909 CET	4545	49740	194.5.98.129	192.168.2.5
Nov 27, 2020 15:25:59.935532093 CET	49741	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:00.180088997 CET	4545	49741	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:00.688467979 CET	49741	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:00.929894924 CET	4545	49741	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:01.438709021 CET	49741	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:01.680001020 CET	4545	49741	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:05.762311935 CET	49742	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:06.040018082 CET	4545	49742	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:06.548357964 CET	49742	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:06.820146084 CET	4545	49742	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:07.329704046 CET	49742	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:07.550179958 CET	4545	49742	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:11.683203936 CET	49743	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:11.940596104 CET	4545	49743	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:12.455055952 CET	49743	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:12.710442066 CET	4545	49743	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:13.220777035 CET	49743	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:13.450519085 CET	4545	49743	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:17.524827003 CET	49745	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:17.770490885 CET	4545	49745	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:18.283685923 CET	49745	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:18.510463953 CET	4545	49745	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:19.018301964 CET	49745	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:19.270576954 CET	4545	49745	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:23.548501015 CET	49746	4545	192.168.2.5	194.5.98.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:26:23.780339003 CET	4545	49746	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:24.284320116 CET	49746	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:24.530333042 CET	4545	49746	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:25.034338951 CET	49746	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:25.290507078 CET	4545	49746	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:29.365698099 CET	49747	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:29.640475035 CET	4545	49747	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:30.144191027 CET	49747	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:30.390332937 CET	4545	49747	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:30.909728050 CET	49747	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:31.150455952 CET	4545	49747	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:35.243457079 CET	49748	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:35.470355034 CET	4545	49748	194.5.98.129	192.168.2.5
Nov 27, 2020 15:26:35.972807884 CET	49748	4545	192.168.2.5	194.5.98.129
Nov 27, 2020 15:26:36.260142088 CET	4545	49748	194.5.98.129	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:24:58.357662916 CET	61733	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:24:58.395020962 CET	53	61733	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:04.484256983 CET	65447	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:04.521737099 CET	53	65447	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:04.652782917 CET	52441	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:04.689975977 CET	53	52441	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:07.007154942 CET	62176	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:07.034149885 CET	53	62176	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:07.683125973 CET	59596	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:07.710150957 CET	53	59596	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:08.400015116 CET	65296	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:08.427098989 CET	53	65296	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:09.183744907 CET	63183	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:09.210896969 CET	53	63183	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:09.435415030 CET	60151	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:09.462397099 CET	53	60151	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:10.421276093 CET	56969	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:11.434983015 CET	56969	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:11.690089941 CET	53	56969	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:11.690448046 CET	53	56969	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:13.532213926 CET	55161	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:13.559271097 CET	53	55161	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:14.374159098 CET	54757	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:14.409761906 CET	53	54757	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:15.570341110 CET	49992	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:15.605603933 CET	53	49992	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:16.248915911 CET	60075	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:16.284332991 CET	53	60075	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:16.923398972 CET	55016	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:16.950576067 CET	53	55016	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:17.476521969 CET	64345	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:17.512070894 CET	53	64345	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:18.021945953 CET	57128	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:18.049098015 CET	53	57128	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:18.697639942 CET	54791	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:18.724796057 CET	53	54791	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:23.300571918 CET	50463	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:23.335999966 CET	53	50463	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:28.457411051 CET	50394	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:28.495412111 CET	53	50394	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:29.204447031 CET	58530	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:29.239996910 CET	53	58530	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:34.645425081 CET	53813	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:34.672533989 CET	53	53813	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:35.410989046 CET	63732	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:25:35.446361065 CET	53	63732	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:35.597779989 CET	57344	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:35.635382891 CET	53	57344	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:39.218868971 CET	54450	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:39.245986938 CET	53	54450	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:41.597326040 CET	59261	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:41.633171082 CET	53	59261	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:42.022618055 CET	57151	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:42.058497906 CET	53	57151	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:44.055949926 CET	59413	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:44.098527908 CET	53	59413	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:47.834994078 CET	60516	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:47.870517969 CET	53	60516	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:53.724030972 CET	51649	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:53.759481907 CET	53	51649	8.8.8.8	192.168.2.5
Nov 27, 2020 15:25:59.898118019 CET	65086	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:25:59.933912992 CET	53	65086	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:05.723683119 CET	56432	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:05.760940075 CET	53	56432	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:11.645477057 CET	52929	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:11.680973053 CET	53	52929	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:13.623311996 CET	64317	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:13.650369883 CET	53	64317	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:17.485431910 CET	61004	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:17.523525953 CET	53	61004	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:23.511261940 CET	56895	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:23.547116995 CET	53	56895	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:29.328500032 CET	62372	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:29.364310980 CET	53	62372	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:35.203321934 CET	61515	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:35.240972042 CET	53	61515	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:41.366586924 CET	56675	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:41.402296066 CET	53	56675	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:47.209471941 CET	57172	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:47.247246981 CET	53	57172	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:53.024509907 CET	55267	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:53.060303926 CET	53	55267	8.8.8.8	192.168.2.5
Nov 27, 2020 15:26:58.915927887 CET	50969	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:26:58.951435089 CET	53	50969	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 27, 2020 15:25:11.690596104 CET	192.168.2.5	8.8.8.8	d006	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:24:58.357662916 CET	192.168.2.5	8.8.8.8	0x9472	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:04.484256983 CET	192.168.2.5	8.8.8.8	0x924b	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:10.421276093 CET	192.168.2.5	8.8.8.8	0x7629	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:11.434983015 CET	192.168.2.5	8.8.8.8	0x7629	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:17.476521969 CET	192.168.2.5	8.8.8.8	0xdfc9	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:23.300571918 CET	192.168.2.5	8.8.8.8	0x1b29	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:29.204447031 CET	192.168.2.5	8.8.8.8	0xd8b3	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:35.410989046 CET	192.168.2.5	8.8.8.8	0xd6fd	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:41.597326040 CET	192.168.2.5	8.8.8.8	0xfdbf	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:25:42.022618055 CET	192.168.2.5	8.8.8.8	0xb27d	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:47.834994078 CET	192.168.2.5	8.8.8.8	0x24fb	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:53.724030972 CET	192.168.2.5	8.8.8.8	0x7ee6	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:59.898118019 CET	192.168.2.5	8.8.8.8	0xfb54	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:05.723683119 CET	192.168.2.5	8.8.8.8	0x449d	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:11.645477057 CET	192.168.2.5	8.8.8.8	0x50f4	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:17.485431910 CET	192.168.2.5	8.8.8.8	0xe529	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:23.511261940 CET	192.168.2.5	8.8.8.8	0x6157	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:29.328500032 CET	192.168.2.5	8.8.8.8	0xd8e4	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:35.203321934 CET	192.168.2.5	8.8.8.8	0x1267	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:41.366586924 CET	192.168.2.5	8.8.8.8	0xcea5	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:47.209471941 CET	192.168.2.5	8.8.8.8	0xcb42	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:53.024509907 CET	192.168.2.5	8.8.8.8	0x728a	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:58.915927887 CET	192.168.2.5	8.8.8.8	0x7233	Standard query (0)	kingman1.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

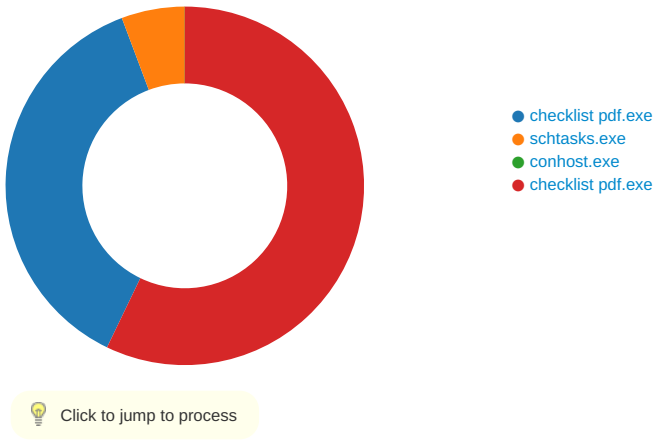
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:24:58.395020962 CET	8.8.8.8	192.168.2.5	0x9472	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:04.521737099 CET	8.8.8.8	192.168.2.5	0x924b	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:11.690089941 CET	8.8.8.8	192.168.2.5	0x7629	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:11.690448046 CET	8.8.8.8	192.168.2.5	0x7629	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:17.512070894 CET	8.8.8.8	192.168.2.5	0xdfc9	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:23.335999966 CET	8.8.8.8	192.168.2.5	0x1b29	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:29.239996910 CET	8.8.8.8	192.168.2.5	0xd8b3	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:35.446361065 CET	8.8.8.8	192.168.2.5	0xd6fd	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:41.633171082 CET	8.8.8.8	192.168.2.5	0xfdbf	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:42.058497906 CET	8.8.8.8	192.168.2.5	0xb27d	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:25:47.870517969 CET	8.8.8.8	192.168.2.5	0x24fb	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:53.759481907 CET	8.8.8.8	192.168.2.5	0x7ee6	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:25:59.933912992 CET	8.8.8.8	192.168.2.5	0xfb54	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:05.760940075 CET	8.8.8.8	192.168.2.5	0x449d	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:26:11.680973053 CET	8.8.8.8	192.168.2.5	0x50f4	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:17.523525953 CET	8.8.8.8	192.168.2.5	0xe529	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:23.547116995 CET	8.8.8.8	192.168.2.5	0x6157	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:29.364310980 CET	8.8.8.8	192.168.2.5	0xd8e4	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:35.240972042 CET	8.8.8.8	192.168.2.5	0x1267	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:41.402296066 CET	8.8.8.8	192.168.2.5	0xcea5	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:47.247246981 CET	8.8.8.8	192.168.2.5	0xcb42	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:53.060303926 CET	8.8.8.8	192.168.2.5	0x728a	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)
Nov 27, 2020 15:26:58.951435089 CET	8.8.8.8	192.168.2.5	0x7233	No error (0)	kingman1.ddns.net		194.5.98.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: checklist pdf.exe PID: 4728 Parent PID: 5612

General

Start time:	15:24:50
Start date:	27/11/2020

Path:	C:\Users\user\Desktop\checklist pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\checklist pdf.exe'
Imagebase:	0x2f0000
File size:	574464 bytes
MD5 hash:	33FB3C28DF0F678C7C6EF72E7E748CB1
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: 00000000.00000002.249652144.00000000039C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.249652144.00000000039C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.249652144.00000000039C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.250632075.0000000003BB3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.250632075.0000000003BB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.250632075.0000000003BB3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.248350217.0000000002A3E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming\PUalpOJIfJW.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A06EB	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpECD4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	66A10F4	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\checklist pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpECD4.tmp	success or wait	1	66A140A	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\PUalpOJIfJW.exe	unknown	574464	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 86 a9 bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 7e 08 00 00 44 00 00 00 00 00 00 e2 9c 08 00 00 20 00 00 00 a0 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....0..~...D........... ....@.. ....@................	success or wait	1	66A0973	WriteFile
C:\Users\user\AppData\Local\Temp\tmpECD4.tmp	unknown	1648	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.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	66A0973	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\checklist pdf.exe.log	unknown	777	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\checklist pdf.exe	unknown	574464	success or wait	1	66A0973	ReadFile

Analysis Process: schtasks.exe PID: 6100 Parent PID: 4728

General

Start time:	15:24:54
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\PUalpOJIfJW' /XML 'C:\Users\user\AppData\Local\Temp\tmpECD4.tmp'
Imagebase:	0xf50000
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\tmpECD4.tmp	unknown	2	success or wait	1	F5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpECD4.tmp	unknown	1649	success or wait	1	F5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6132 Parent PID: 6100

General

Start time:	15:24:55
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: checklist pdf.exe PID: 4648 Parent PID: 4728

General

Start time:	15:24:55
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\checklist pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa00000
File size:	574464 bytes
MD5 hash:	33FB3C28DF0F678C7C6EF72E7E748CB1
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: 00000003.00000002.501688763.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.501688763.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.501688763.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.509908735.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.509908735.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.508000940.0000000004267000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.508000940.0000000004267000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.510380996.00000000059B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.510380996.00000000059B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.510380996.00000000059B0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming\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	52C07A1	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	52C089B	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\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	52C07A1	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	52C07A1	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\checklist pdf.exe:Zone.Identifier	success or wait	1	52C0D41	DeleteFileA

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	44 53 18 a7 2b 93 d8 48	DS..+..H	success or wait	1	52C0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52C0A53	ReadFile
C:\Users\user\Desktop\checklist pdf.exe	unknown	4096	success or wait	1	72C5BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\checklist pdf.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	52C0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52C0A53	ReadFile

Disassembly

Code Analysis