ID: 319643
Sample Name: DOC.exe
Cookbook: default.jbs
Time: 14:12:30
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

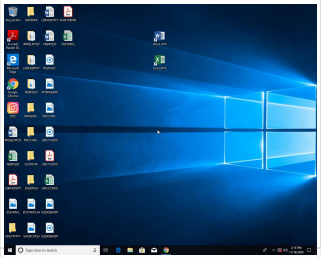
Analysis Report DOC.exe

Overview

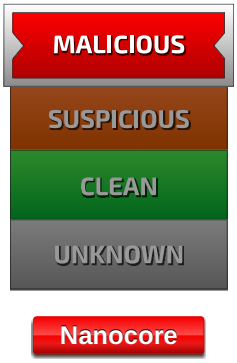
General Information

Sample Name:	DOC.exe
Analysis ID:	319643
MD5:	6ad10f04afb24c9..
SHA1:	561fed791a4a4a1.
SHA256:	c8d2f56a87705f1..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

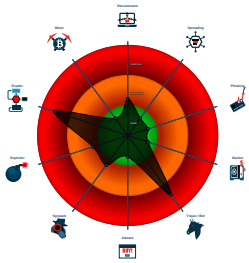


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- DOC.exe (PID: 6600 cmdline: 'C:\Users\user\Desktop\DOC.exe' MD5: 6AD10F04AFB24C96187B76129225C00C)
  - schtasks.exe (PID: 6696 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CZOIAvjovs' /XML 'C:\Users\user\AppData\Local\Temp\tmp3870.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DOC.exe (PID: 6752 cmdline: {path} MD5: 6AD10F04AFB24C96187B76129225C00C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.253582659.0000000002FFC000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.254195888.0000000003FBD000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xfbbfd:$x1: NanoCore.ClientPluginHost • 0xfbc3a:$x2: IClientNetworkHost • 0xff76d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.254195888.0000000003FBD000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.254195888.0000000003FBD000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfb965:$a: NanoCore • 0xfb975:$a: NanoCore • 0xfbba9:$a: NanoCore • 0xfbbbd:$a: NanoCore • 0xfbbfd:$a: NanoCore • 0xfb9c4:$b: ClientPlugin • 0xfbbc6:$b: ClientPlugin • 0xfbc06:$b: ClientPlugin • 0xfbaeb:$c: ProjectData • 0xfc4f2:$d: DESCrypto • 0x103ebe:$e: KeepAlive • 0x101eac:$g: LogClientMessage • 0xfe0a7:$i: get_Connected • 0xfc828:$j: #=q • 0xfc858:$j: #=q • 0xfc874:$j: #=q • 0xfc8a4:$j: #=q • 0xfc8c0:$j: #=q • 0xfc8dc:$j: #=q • 0xfc90c:$j: #=q • 0xfc928:$j: #=q
00000000.00000002.255252413.0000000004173000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x250b1d:$x1: NanoCore.ClientPluginHost • 0x250b5a:$x2: IClientNetworkHost • 0x25468d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 8 entries				

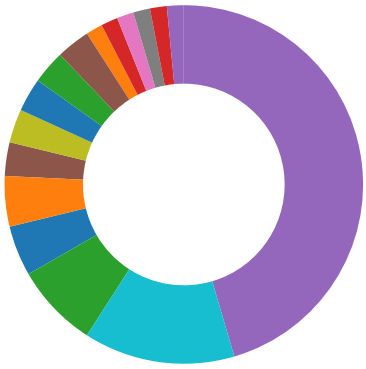
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

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

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

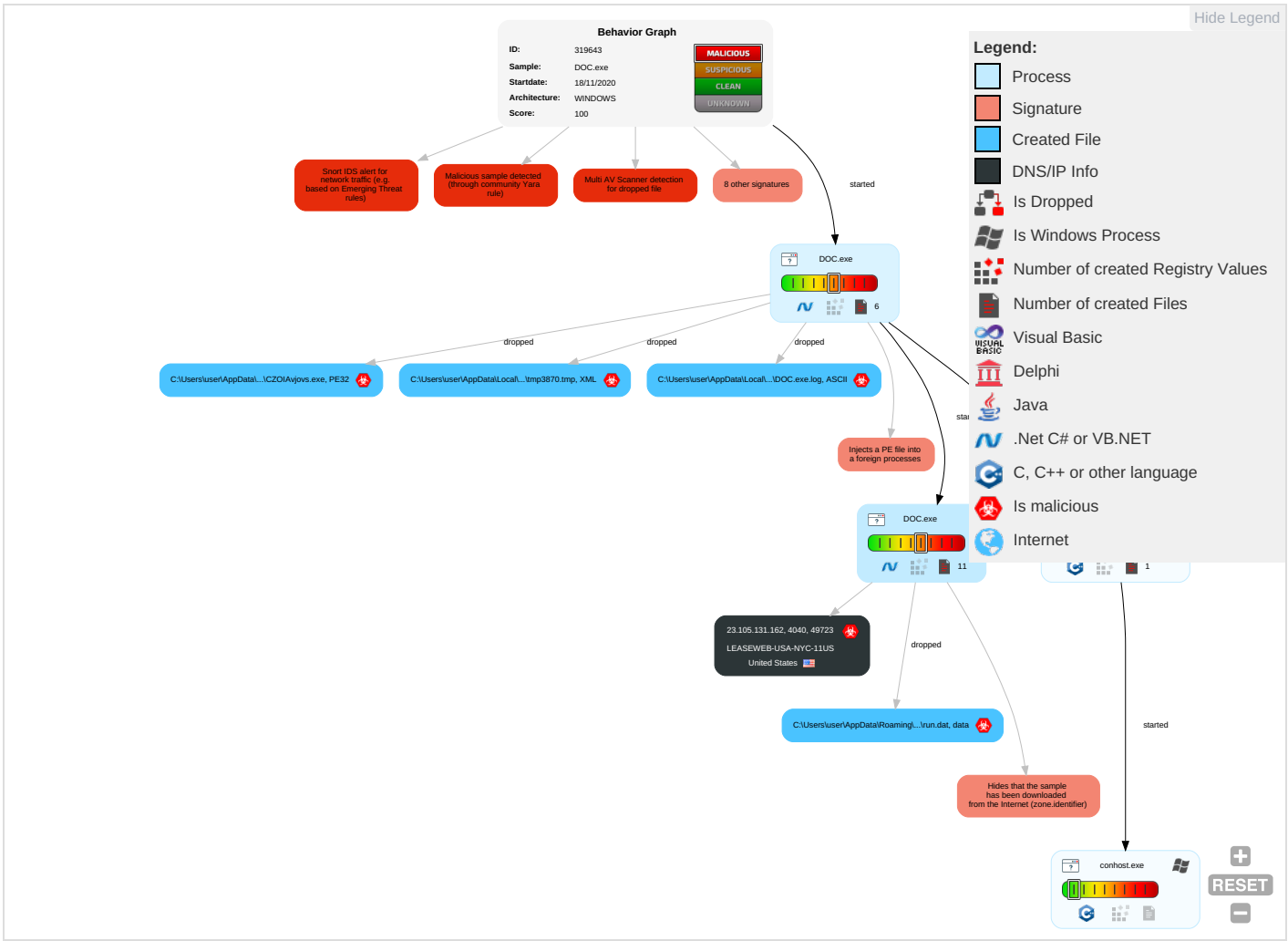
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
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	Jamn Denia Servi
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	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

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
DOC.exe	19%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CZOIAvjovs.exe	19%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Webd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/0	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.jiyu-kobo.co.jp/9	0%	Avira URL Cloud	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.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.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://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://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/f	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	Avira URL Cloud	safe	
http://www.fontbureau.com0	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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.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.jiyu-kobo.co.jp/Regux	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.como.Z	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comeuG	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/J	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/A	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiefx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicdS	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/Conn	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.carterandcone.comizey	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.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.sajatypeworks.comte?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/anie	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0so	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

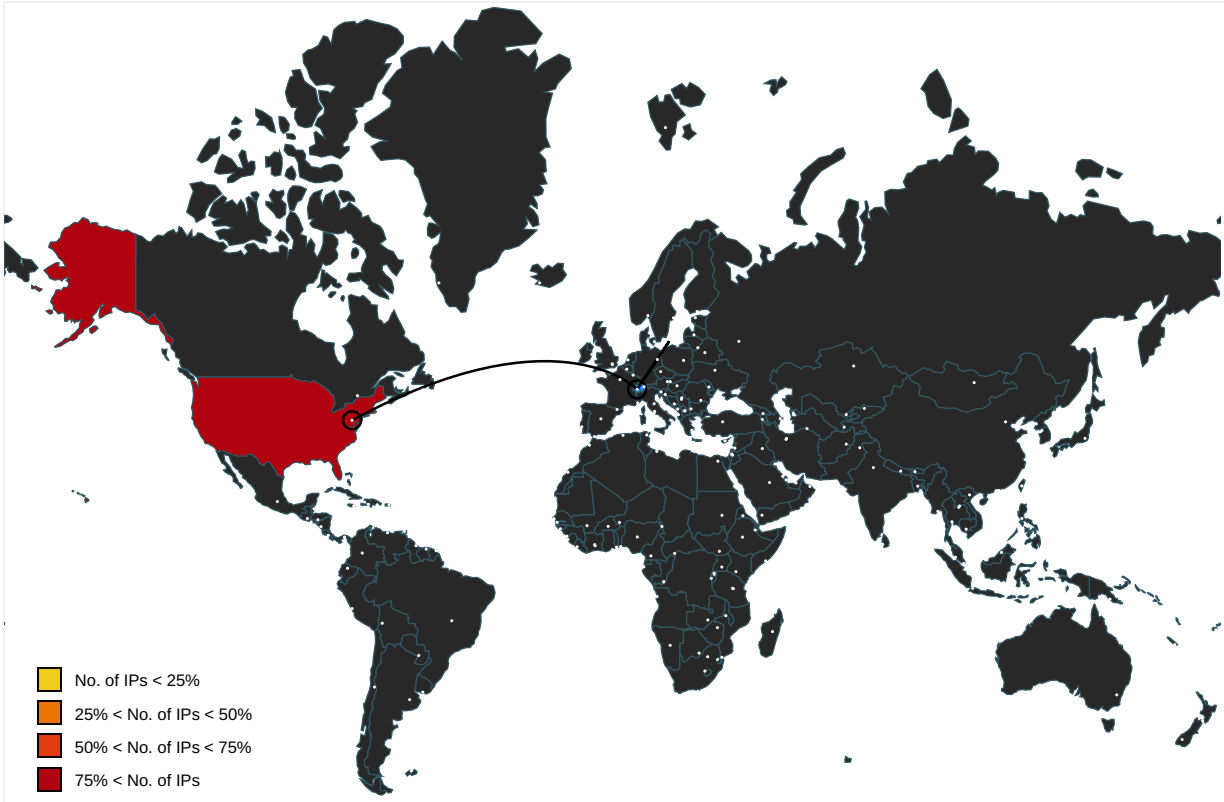
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnue	DOC.exe, 00000000.00000003.242216750.000000000542C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Webd	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/0	DOC.exe, 00000000.00000003.242988653.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	DOC.exe, 00000000.00000003.242614903.000000000541A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/9	DOC.exe, 00000000.00000003.242988653.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/f	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom	DOC.exe, 00000000.00000003.244365755.000000000542B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/0	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com0	DOC.exe, 00000000.00000003.244365755.000000000542B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	DOC.exe, 00000000.00000003.243289341.0000000005426000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Regux	DOC.exe, 00000000.00000003.243289341.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.Z	DOC.exe, 00000000.00000003.242274345.000000000542D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp, DOC.exe, 00000000.00000003.242124625.00000000541D000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	DOC.exe, 00000000.00000003.244700687.000000000542A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	DOC.exe, 00000000.00000003.244081653.0000000005426000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/f	DOC.exe, 00000000.00000003.244365755.000000000542B000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comeuG	DOC.exe, 00000000.00000003.240828716.000000000542B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/J	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/A	DOC.exe, 00000000.00000003.244700687.000000000542A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsiefx	DOC.exe, 00000000.00000003.244365755.000000000542B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comlicdS	DOC.exe, 00000000.00000003.244365755.000000000542B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Conn	DOC.exe, 00000000.00000003.242988653.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTFJ	DOC.exe, 00000000.00000003.244365755.000000000542B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	DOC.exe, 00000000.00000003.241955458.000000000542D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comizey	DOC.exe, 00000000.00000003.242614903.000000000541A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.comte?	DOC.exe, 00000000.00000003.240828716.000000000542B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/anie	DOC.exe, 00000000.00000003.242822237.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0so	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp, DOC.exe, 00000000.00000003.242988653.00000000005426000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DOC.exe, 00000000.00000002.257492311.0000000005622000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comgrita9	DOC.exe, 00000000.00000002.257330031.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/h	DOC.exe, 00000000.00000003.243551878.0000000005426000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comFm.	DOC.exe, 00000000.00000002.257330031.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/f	DOC.exe, 00000000.00000003.242988653.0000000005426000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgretaJ	DOC.exe, 00000000.00000003.245481149.000000000542A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319643
Start date:	18.11.2020

Start time:	14:12:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DOC.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:	24
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@6/7@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.3% (good quality ratio 8.7%) • Quality average: 38.1% • Quality standard deviation: 36.2%
HCA Information:	• Successful, ratio: 79% • 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, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:13:27	API Interceptor	1016x Sleep call for process: DOC.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	Shipping_Details.exe	Get hash	malicious	Browse	• 23.105.131.165
	2AyWKsCvVF.exe	Get hash	malicious	Browse	• 192.253.246.143
	tn9jVPvlMSqAUX5.exe	Get hash	malicious	Browse	• 23.105.131.229
	HLiw2LPA8i.rtf	Get hash	malicious	Browse	• 192.253.246.143
	TDToxqrclL.exe	Get hash	malicious	Browse	• 23.105.131.177
	Ziiq5tI3CT.exe	Get hash	malicious	Browse	• 23.105.131.239
	f3wo2FuLN6.exe	Get hash	malicious	Browse	• 192.253.246.143
	ORDER INQUIRY.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Purchase Order 4500033557.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	SecuriteInfo.com.Trojan.DownLoader35.34609.25775.exe	Get hash	malicious	Browse	• 192.253.246.138
	Proof_of_payment.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	invoice tax.xlsm	Get hash	malicious	Browse	• 23.105.131.217
	SHIPPING DOCUMENTS.pdf.exe	Get hash	malicious	Browse	• 23.105.131.177
	Payment_Order_20201111.xlsx	Get hash	malicious	Browse	• 192.253.246.138
	TLpMnhJmg7.exe	Get hash	malicious	Browse	• 192.253.246.143
	HDyADDoI3I.exe	Get hash	malicious	Browse	• 192.253.246.143
	11.exe	Get hash	malicious	Browse	• 173.234.155.145
	53C29QAJnd.exe	Get hash	malicious	Browse	• 173.234.155.145
	OMQZvmAmCj.exe	Get hash	malicious	Browse	• 173.234.155.145
	gH4o5FCHAE.exe	Get hash	malicious	Browse	• 173.234.155.145

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DOC.exe.log

Process:	C:\Users\user\Desktop\DOC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	5.271473536084351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2u7x5I6Hi0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2I3rOz2T
MD5:	C3EC08CD6BEA8576070D5A52B4B6D7D0
SHA1:	40B95253F98B3CC5953100C0E71DAC7915094A5A
SHA-256:	28B314C3E5651414FD36B2A65B644A2A55F007A34A536BE17514E12CEE5A091B
SHA-512:	5B0E6398A092F08240DC6765425E16DB52F32542FF7250E87403C407E54B3660EF93E0EAD17BA2CEF6B666951ACF66FA0EAD61FB52E80867DDD398E8258DED2
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DOC.exe.log	
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.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\tmp3870.tmp	
Process:	C:\Users\user\Desktop\DOC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1659
Entropy (8bit):	5.176378890983135
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBAqPMtn:cbhH7MlNQ8/rydbz9I3YODOLNdq32
MD5:	8D3271AEF7B24B0FBA2824A6FDCB3175
SHA1:	BB1BE4542A6924BB767F5E2929ED3724E31F566B
SHA-256:	481AD806BE0C55F5D357C2196FA5C451CC9529106116DA6D070BD5BCE626B072
SHA-512:	45A249B869B041FBCA277F07722997D600028546953F80643137980FDDB268FFAC44E1AD65BB2FA07F6C32C2B7B4C9003DDD6FF701C4196158258C87337CD3E0
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>.. <StartWhenAv

C:\Users\user\AppData\Roaming\CZOIAvjovs.exe	
Process:	C:\Users\user\Desktop\DOC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1119744
Entropy (8bit):	7.3796673297276865
Encrypted:	false
SSDEEP:	12288:ZivDqJF9EWc+ylc3UognpsVjxonj4GdnfKM3yvt8LFOcc6WkFRJtsbUpmmEvx74F:cuJFHJipkj+nkGdnf73y18bWkbzswH
MD5:	6AD10F04AFB24C96187B76129225C00C
SHA1:	561FED791A4A4A10EC9889E3E30F0C4E0DB80FD0
SHA-256:	C8D2F56A87705F11451E14E6ED7FE90A5B995B3E7F668811FB2F43A8F4325579
SHA-512:	622A5C80012D121D765DC57436F06B321379AED457DB210ECAF68ABFD2E6462F2A20FF16ABE948014C6E3B060D4A62E087A3BF0AB6E7A83CE76C34B21667830
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0.....D.....^.... .....@.. ..... .@.....W.....A.....`..... ..... ..H.....text...d.... ..... ..`.rsrc....A.....B.....@..@.relo c.....`.....@..B.....@.....H..... 6..... .....S.DMy.4.Y....g5'.....jT.....=...!rXF.T.yI..XB..6P.EQ..;..e....m...:.....gy..SP.g. [...C....#.6.....F..u,....Zk6...X.....sm.Y>.H.L...S..5.O..a>.-.<w.....w.#.....:.=.w.@.X....Vi..e5...'e....Pl7G....i.....p1lE...]..R....K..f..UqO...^..X3..n.t.....%.v..\.b.-.....Xp..@.Hn...Lq... *..;."K.....#Q.H1...M.W.....>...i.\.#.._y...a.....l..6...AO.*G...\S.3m..J...<Hp.f.....W

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\DOC.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\DOC.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:mqh:mC
MD5:	FCDEA6ED59DF2E5154B0CF3F084BF8DF
SHA1:	B8C1743A845038E38892E7CA8240FC2C68EF443E
SHA-256:	07D3164F04628B1D3D1819E04C0C0AE83FD6DC72199976349A0956152091C478
SHA-512:	FEB7ABF35FD28E282C7E76C1A68338A0DE2C8D8B9B13A771A16EDD6C1D1E811F14602A26C1D50624F6030AA9241E472E12B618386A6ADD90DB48930671D2442
Malicious:	**true**
Reputation:	low
Preview:	.../...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\DOC.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.3796673297276865

General

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:	DOC.exe
File size:	1119744
MD5:	6ad10f04afb24c96187b76129225c00c
SHA1:	561fed791a4a4a10ec9889e3e30f0c4e0db80fd0
SHA256:	c8d2f56a87705f11451e14e6ed7fe90a5b995b3e7f668811fb2f43a8f4325579
SHA512:	622a5c80012d121d765dc57436f06b321379aed457db210ecaf68abfd2e6462f2a20ff16abe948014c6e3b060d4a62e087a3bf0ab6e7a83ce76c34b216678302
SSDEEP:	12288:ZivDqJF9EWc+ylc3UognpsVjxonj4GdnfKM3yvt8LFOcc6WkFRJtsbUpmmEvx74F:cuJFHJipkj+nkGdnf73y18bWkbzswH
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:	0x50ee5e
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:	0x5FB4A4C5 [Wed Nov 18 04:36:21 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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	0x10ee04	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x110000	0x41a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x116000	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	0x10ce64	0x10d000	False	0.694431234026	data	7.38686348526	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x110000	0x41a8	0x4200	False	0.503432765152	data	5.45039345339	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x116000	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	0x110190	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1105f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0x1116a0	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	0x113c48	0x30	data		
RT_VERSION	0x113c78	0x344	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x113fbc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	d.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Clinic Management System
ProductVersion	1.0.0.0
FileDescription	Clinic Management System
OriginalFilename	d.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/18/20-14:13:34.045618	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	4040	192.168.2.7	23.105.131.162

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 14:13:33.600183010 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:34.005378008 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:34.005552053 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:34.045618057 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:34.496907949 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:34.525669098 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:34.974037886 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:35.205224037 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:35.245909929 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:35.658174992 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:35.685698986 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.186507940 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.497425079 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.499332905 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.499439001 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.508373976 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.508555889 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.508594036 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.508697033 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.508867025 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.508979082 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.515528917 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.518650055 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.518789053 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.518896103 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.519356012 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.520392895 CET	49723	4040	192.168.2.7	23.105.131.162

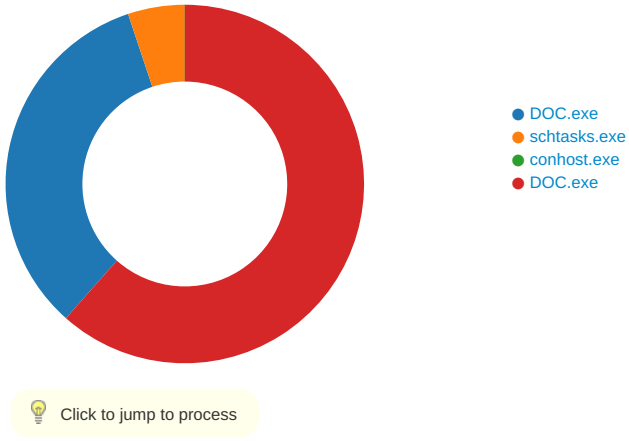
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 14:13:36.922518015 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.924273014 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.924427032 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.925810099 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.927284956 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.927381039 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.941277981 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.950264931 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.950380087 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.952456951 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.952718019 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.952824116 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.956509113 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.969232082 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.969285011 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.969333887 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.969424963 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.969526052 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.969541073 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.975753069 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.978308916 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.978502035 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.980390072 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.980462074 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.980479956 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.982404947 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.982477903 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:36.985758066 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.988337040 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:36.988409996 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.379363060 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.381352901 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.381527901 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.383512020 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.392493010 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.392658949 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.392733097 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.396400928 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.396483898 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.398395061 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.402513027 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.402565002 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.402647972 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.411446095 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.411521912 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.411577940 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.411645889 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.411701918 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.415158033 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.418374062 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.418505907 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.421237946 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.439531088 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.439574957 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.439678907 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.439692020 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.439747095 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.439862013 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.439968109 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.440030098 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.440036058 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.442368984 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.442516088 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.452541113 CET	4040	49723	23.105.131.162	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 14:13:37.456428051 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.456577063 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.458225965 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.462277889 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.462379932 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.468354940 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.468463898 CET	4040	49723	23.105.131.162	192.168.2.7
Nov 18, 2020 14:13:37.468532085 CET	49723	4040	192.168.2.7	23.105.131.162
Nov 18, 2020 14:13:37.475269079 CET	4040	49723	23.105.131.162	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DOC.exe PID: 6600 Parent PID: 5724

General

Start time:	14:13:24
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\DOC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOC.exe'
Imagebase:	0x890000
File size:	1119744 bytes
MD5 hash:	6AD10F04AFB24C96187B76129225C00C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.253582659.0000000002FFC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.254195888.0000000003FBD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254195888.0000000003FBD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254195888.0000000003FBD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.255252413.0000000004173000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.255252413.0000000004173000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.255252413.0000000004173000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\CZOIAvjovs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5BD0403	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3870.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	129B2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DOC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3870.tmp	success or wait	1	5BD112A	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\CZOIAvjovs.exe	unknown	1119744	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 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 c5 a4 b4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 d0 10 00 00 44 00 00 00 00 00 00 5e ee 10 00 00 20 00 00 00 00 11 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 80 11 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	5BD068B	WriteFile
C:\Users\user\AppData\Local\Temp\tmp3870.tmp	unknown	1659	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 66 72 6f 6e 74 64 65 73 6b 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	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registrati	success or wait	1	5BD068B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DOC.exe.log	unknown	641	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\Desktop\DOC.exe	unknown	1119744	success or wait	1	5BD068B	ReadFile

Analysis Process: schtasks.exe PID: 6696 Parent PID: 6600

General

Start time:	14:13:29
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CZOIAvjovs' /XML 'C:\Users\user\AppData\Local\Temp\tmp3870.tmp'
Imagebase:	0xf00000
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\tmp3870.tmp	unknown	2	success or wait	1	F0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3870.tmp	unknown	1660	success or wait	1	F0ABD9	ReadFile

Analysis Process: conhost.exe PID: 6704 Parent PID: 6696

General

Start time:	14:13:29
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: DOC.exe PID: 6752 Parent PID: 6600

General

Start time:	14:13:30
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\DOC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaf0000
File size:	1119744 bytes
MD5 hash:	6AD10F04AFB24C96187B76129225C00C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000003.00000003.270319895.000000000477B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	56307A1	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	563089B	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	56307A1	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	56307A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	563089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	563089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	563089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DOC.exe:Zone.Identifier	success or wait	1	5630B41	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	be 1c 14 2f 0f 8c d8 48	.../...H	success or wait	1	5630A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	5630A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426840	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^.._.........B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	5630A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 85 16 f4 a5 20 38 a2 6a 80 a4 a3 f3 7c 88 26 58 b6 ca 65 a6 46 b8 2a 80	9iH....}Z..4..f..... 8.j....|. &X..e.F.*.	success or wait	1	5630A53	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\Desktop\DOC.exe	unknown	4096	success or wait	1	7253BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DOC.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5630A53	ReadFile

Disassembly

Code Analysis