ID: 800680
Sample Name:
RogueChecker.exe
Cookbook: default.jbs
Time: 18:03:43
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

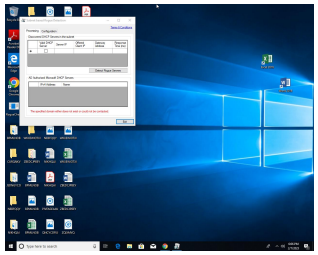
Windows Analysis Report

RogueChecker.exe

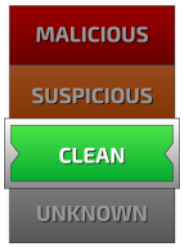
Overview

General Information

Sample Name:	RogueChecker.exe
Analysis ID:	800680
MD5:	7b0c95a1d60d…
SHA1:	502ed0d549aa…
SHA256:	96a19d810a0c…
Infos:	



Detection

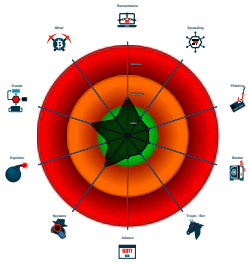


Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Uses 32bit PE files
- Queries the volume information (nam…
- Sample file is different than original …
- Detected potential crypto function
- Potential time zone aware malware
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- RogueChecker.exe (PID: 5988 cmdline: C:\Users\user\Desktop\RogueChecker.exe MD5: 7B0C95A1D60D8148497730601D29399A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

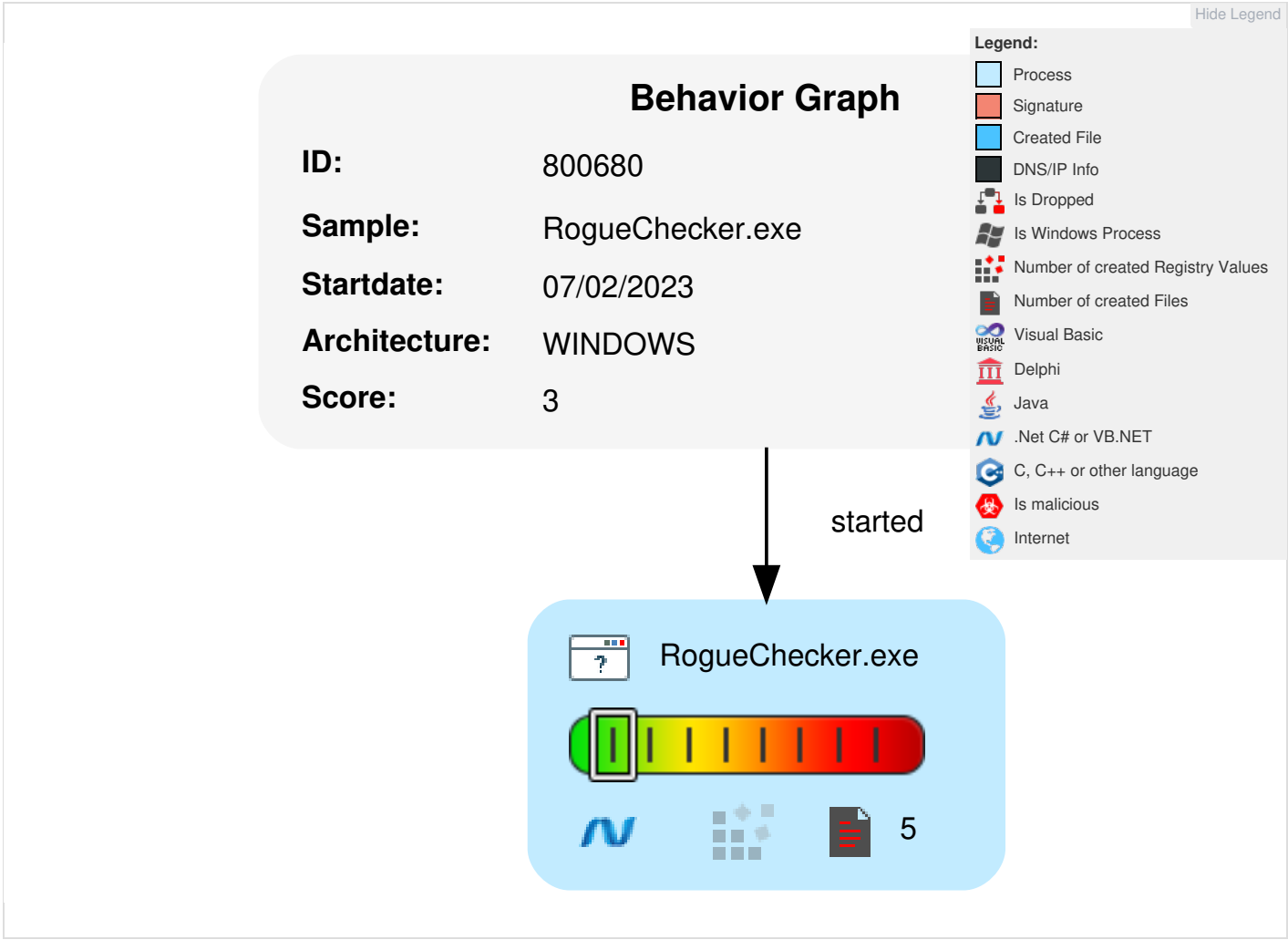
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

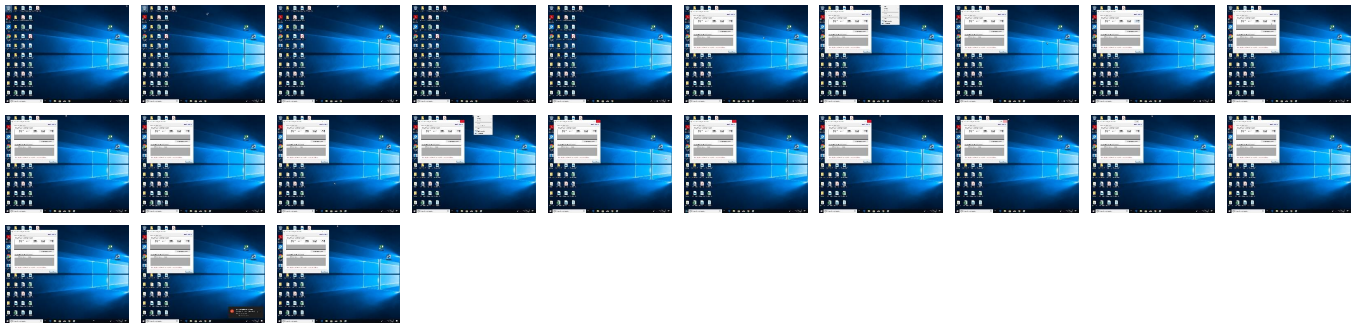
Behavior Graph



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
RogueChecker.exe	0%	ReversingLabs		
RogueChecker.exe	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.urwpp.dee.ht	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sajatypeworks.comX	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sakkal.comS	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comF	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sajatypeworks.comW	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://en.w0	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comc	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comi	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000002.572385337.000000001BE40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comS	RogueChecker.exe, 00000000.00000003.314562722.000000001BE54000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.dee.ht	RogueChecker.exe, 00000000.00000003.316192055.000000001BE5B000.00000004.00000020.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000003.316379528.000000001BE5B000.00000004.00000020.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000003.316428904.000000001BE5B000.00000004.00000020.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000003.316114398.000000001BE5B000.00000004.00000020.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000003.316264076.000000001BE5B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000002.572385337.000000001BE40000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comF	RogueChecker.exe, 00000000.00000003.311423599.000000001BE52000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlra	RogueChecker.exe, 00000000.00000003.317378745.000000001BE79000.00000004.00000020.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000003.317322877.000000001BE79000.00000004.00000020.00020000.00000000.sdmp	false		high
http://en.w	RogueChecker.exe, 00000000.00000003.313867561.000000001BE51000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp, RogueChecker.exe, 00000000.00000003.317322877.000000001BE79000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	RogueChecker.exe, 00000000.00000003.317842792.000000001BE79000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comX	RogueChecker.exe, 00000000.00000003.311423599.000000001BE52000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comW	RogueChecker.exe, 00000000.00000003.311423599.000000001BE52000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	RogueChecker.exe, 00000000.00000002.572603013.000000001D052000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.w0	RogueChecker.exe, 00000000.00000003.3109 37935.000000001BE42000.00000004.00000020 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	RogueChecker.exe, 00000000.00000003.3145 62722.000000001BE54000.00000004.00000020 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comd	RogueChecker.exe, 00000000.00000003.3114 23599.000000001BE52000.00000004.00000020 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comc	RogueChecker.exe, 00000000.00000003.3114 23599.000000001BE52000.00000004.00000020 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	RogueChecker.exe, 00000000.00000003.3183 69985.000000001BE7B000.00000004.00000020 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	RogueChecker.exe, 00000000.00000002.5726 03013.000000001D052000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comi	RogueChecker.exe, 00000000.00000003.3114 23599.000000001BE52000.00000004.00000020 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800680
Start date and time:	2023-02-07 18:03:43 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	7
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

Sample file name:	RogueChecker.exe
Detection:	CLEAN
Classification:	clean3.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target RogueChecker.exe, PID 5988 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.944234855292515
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:	RogueChecker.exe
File size:	88064
MD5:	7b0c95a1d60d8148497730601d29399a
SHA1:	502ed0d549aacb8ff7442e47a3afa8bee3e9117d
SHA256:	96a19d810a0c76c97a06fe2d3860b6bf6d0cb6aaecf81a913cc69c583be5a85c
SHA512:	501826fa2ce317032ccff911111becf76ab92e1007aa24ce352aefc08d4e34bdcc5e98bd9fb724966085b593828d14a7b2908ffa9cd60844f2b0513561ccff93
SSDEEP:	1536:uYhFCiRUSCdNPBRpSzQDpeMaQQQduXLL+76HDXr5z6S5j2:ucFCiRUSCd5B6zQtwQQQduXH+76HTr5w
TLSH:	4483F8143288571BC2A712F8EB12B0442737F91959E1D5D83DEBD2BE25FBB88D312663
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&}MJ.....N.....nm... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x416d6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH
Time Stamp:	0x4A4D7D26 [Fri Jul 3 03:38:14 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16d20	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x5a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x16c8c	0x1c	.text
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	0x14d74	0x14e00	False	0.36578405688622756	data	5.993089999094043	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x5a8	0x600	False	0.41015625	data	4.07178673962085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1a000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x180a0	0x318	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x183b8	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: RogueChecker.exe PID: **5988**, Parent PID: **3324**

General

Target ID:	0
Start time:	18:04:40
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\RogueChecker.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RogueChecker.exe
Imagebase:	0xa20000
File size:	88064 bytes
MD5 hash:	7B0C95A1D60D8148497730601D29399A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	7FFA05508527	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	7FFA05508527	unknown
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	7FFA05508527	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA05508527	unknown
C:\Users\user\Desktop\WellKnownServers.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA056C8147	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA05535C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFA05535C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA05655AF3	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFA05535C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	7FFA05535C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FFA056C8147	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FFA056C8147	ReadFile

Disassembly

No disassembly