ID: 882700
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:13:55
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

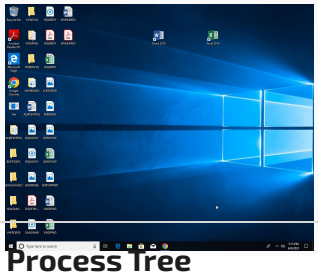
Windows Analysis Report

file.exe

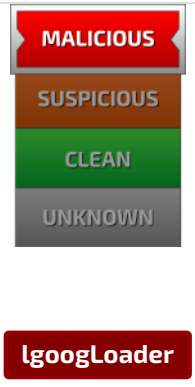
Overview

General Information

Sample Name:	file.exe
Analysis ID:	882700
MD5:	daf761fb9aaa3…
SHA1:	47fd2695b6da2..
SHA256:	18d4850a1081…
Tags:	NET exe LgoogLoader MSIL x64
Infos:	



Detection



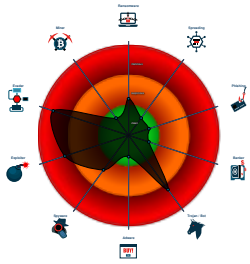
lgoogLoader

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

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Yara detected lgoogLoader
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Writes to foreign memory regions
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Sample is not signed and drops a de…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6988 cmdline: C:\Users\user\Desktop\file.exe MD5: DAF761FB9AAA34A9C2120003694D88A3)
  - ComSvcConfig.exe (PID: 4572 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ComSvcConfig.exe MD5: 2778AE0EB674B74FF8028BF4E51F1DF5)
  - jsc.exe (PID: 3068 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\jsc.exe MD5: 2B40A449D6034F41771A460DADD53A60)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
LgoogLoader	LgoogLoader is an installer that drops three files: a batch file, an AutoIt interpreter, and an AutoIt script. After downloading, it executes the batch file.	No Attribution	http://https://blog.polyswarm.io/null mixer-drops-multiple-malware-families	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.lgoogloader

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\?????.sys	PUA_VULN_Driver_Sysinternalswwwsysinternalscom_procexpsys_ProcessExplorer_HoEP	Detects vulnerable driver mentioned in LOLDrivers project using VersionInfo values from the PE header - 97e3a44ec4ae58c8cc38eefc613e950e.bin	Florian Roth	• 0x6765:$: 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 50 00 72 00 6F 00 63 00 65 00 73 00 73 00 20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 ... • 0x66fd:$: 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 53 00 79 00 73 00 69 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 73 00 20 00 2D 00 20 00 77 00 77 00 77 00 2E ... • 0x67b1:$: 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 31 00 36 00 2E 00 34 00 33 • 0x6911:$: 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 31 00 36 00 2E 00 34 00 33 • 0x67dd:$: 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 70 00 72 00 6F 00 63 00 65 00 78 00 70 00 2E 00 73 00 79 00 73 • 0x68cd:$: 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 50 00 72 00 6F 00 63 00 65 00 73 00 73 00 20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 • 0x688d:$: 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 70 00 72 00 6F 00 63 00 65 00 78 00 70 00 2E 00 53 00 79 00 73 • 0x6815:$: 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 4D 00 61 00 72 ...

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.492960569.0000000000E30000.00000040.00001000.00020000.00000000.sdmp	SUSP_XORed_MSDOS_Stub_Message	Detects suspicious XORed MSDOS stub message	Florian Roth (Nextron Systems)	• 0xade:$xo1: \x9E\xA2\xA3\xB9\xEA\xBA\xB8\xA5\xAD\xB8\xAB\xA7\xEA\xA9\xAB\xA4\xA4\xA5\xBE\xEA\xA8\xAF\xEA\xB8\xBF\xA4\xEA\xA3\xA4\xEA\x8E\x85\x99\xEA\xA7\xA5\xAE\xAF • 0x6546:$xo1: \x9E\xA2\xA3\xB9\xEA\xBA\xB8\xA5\xAD\xB8\xAB\xA7\xEA\xA9\xAB\xA4\xA4\xA5\xBE\xEA\xA8\xAF\xEA\xB8\xBF\xA4\xEA\xA3\xA4\xEA\x8E\x85\x99\xEA\xA7\xA5\xAE\xAF
00000002.00000002.492960569.0000000000E30000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_IGoogLoader	Yara detected IgoogLoader	Joe Security	
00000000.00000002.493841709.000001F6C76CC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
Process Memory Space: file.exe PID: 6988	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: file.exe PID: 6988	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.1f6c773a2a8.2.raw.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
0.2.file.exe.1f6c773a2a8.2.raw.unpack	INDICATOR_SUSPICIOUS_DisableWinDefender	Detects executables containing artifcats associated with disabling Widnows Defender	ditekSHen	• 0x9d0d:$e1: Microsoft\Windows Defender\Exclusions\Paths • 0x9d3c:$e2: Add-MpPreference -ExclusionPath
0.2.file.exe.1f6c773a2a8.2.raw.unpack	INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM	Detects executables embedding command execution via IExecuteCommandCOM object	ditekSHen	• 0x9cdd:$r1: Classes\Folder\shell\open\command • 0x912c:$k1: DelegateExecute

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Exploits

Yara detected UAC Bypass using CMSTP

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected IgoogLoader

Persistence and Installation Behavior

Sample is not signed and drops a device driver

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

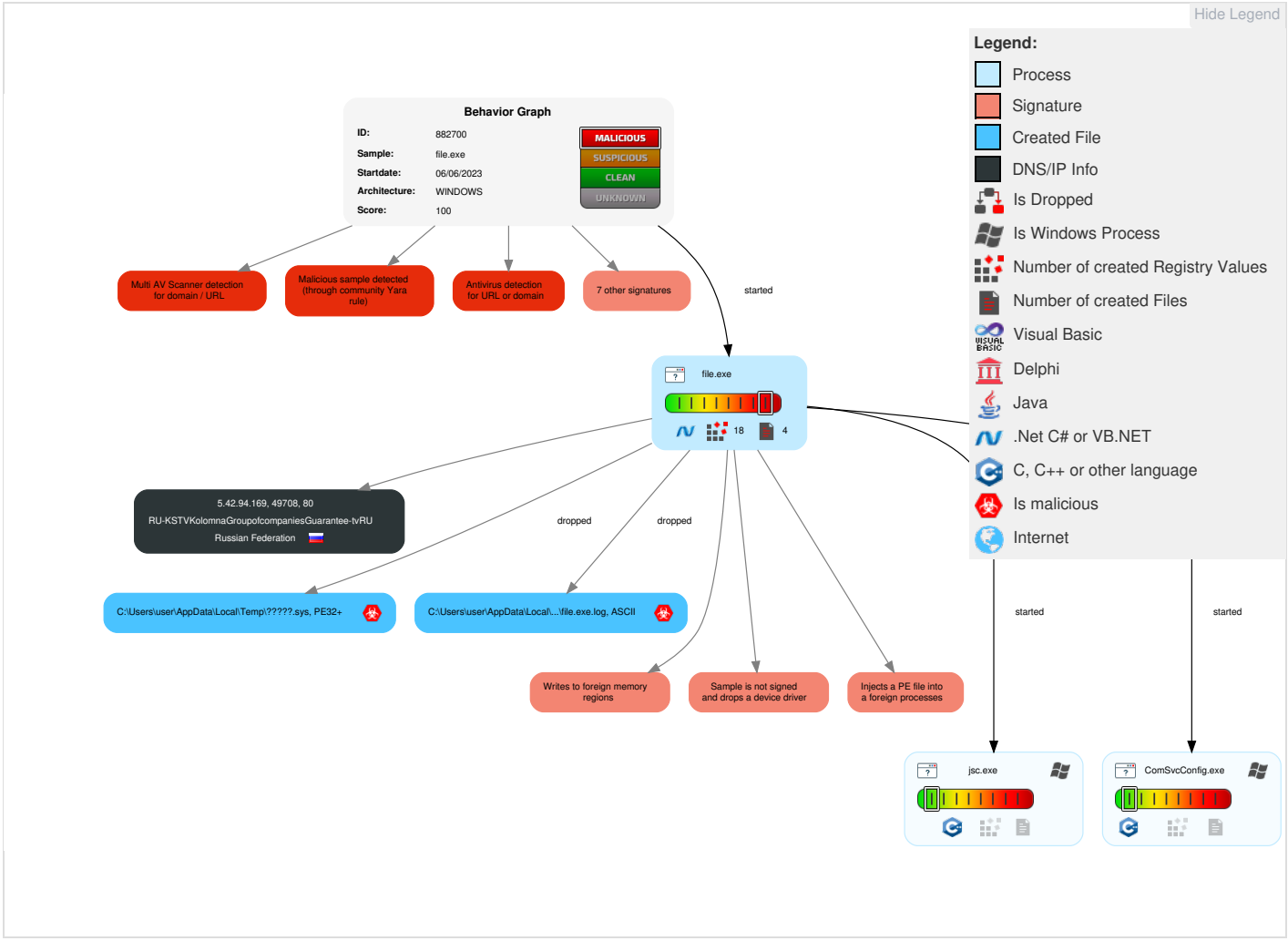
Injects a PE file into a foreign processes

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
1 Valid Accounts	1 3 Native API	1 Valid Accounts	1 Valid Accounts	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	2 Windows Service	1 Exploitation for Privilege Escalation	1 Valid Accounts	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	2 LSASS Driver	1 1 Access Token Manipulation	1 Disable or Modify Tools	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	2 Windows Service	2 1 Virtualization/Sandbox Evasion	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	2 1 1 Process Injection	1 1 Access Token Manipulation	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	2 LSASS Driver	2 1 1 Process Injection	Cached Domain Credentials	3 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Deobfuscate/Decode Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

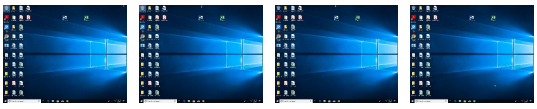
Behavior Graph



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
file.exe	46%	ReversingLabs	Win64.Trojan.Pwsx	
file.exe	56%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\?????.sys	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sysinternals.comopen/?ICONSHELLRUNASAboutUsage/raw/netonlyRunAsInvoker__COMPAT_LAYERcmd	0%	URL Reputation	safe	
http://https://www.sysinternals.com0	0%	URL Reputation	safe	
http://5.42.94.169	0%	Avira URL Cloud	safe	
http://5.42.94.169/customer/368	100%	Avira URL Cloud	malware	
http://5.42.94.169	8%	Virustotal		Browse
http://5.42.94.169/customer/368	9%	Virustotal		Browse
http://109.206.241.33/files/Hadi.config.CfgEncFileMZ	0%	Virustotal		Browse
http://109.206.241.33/files/Hadi.config.CfgEncFileMZ	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

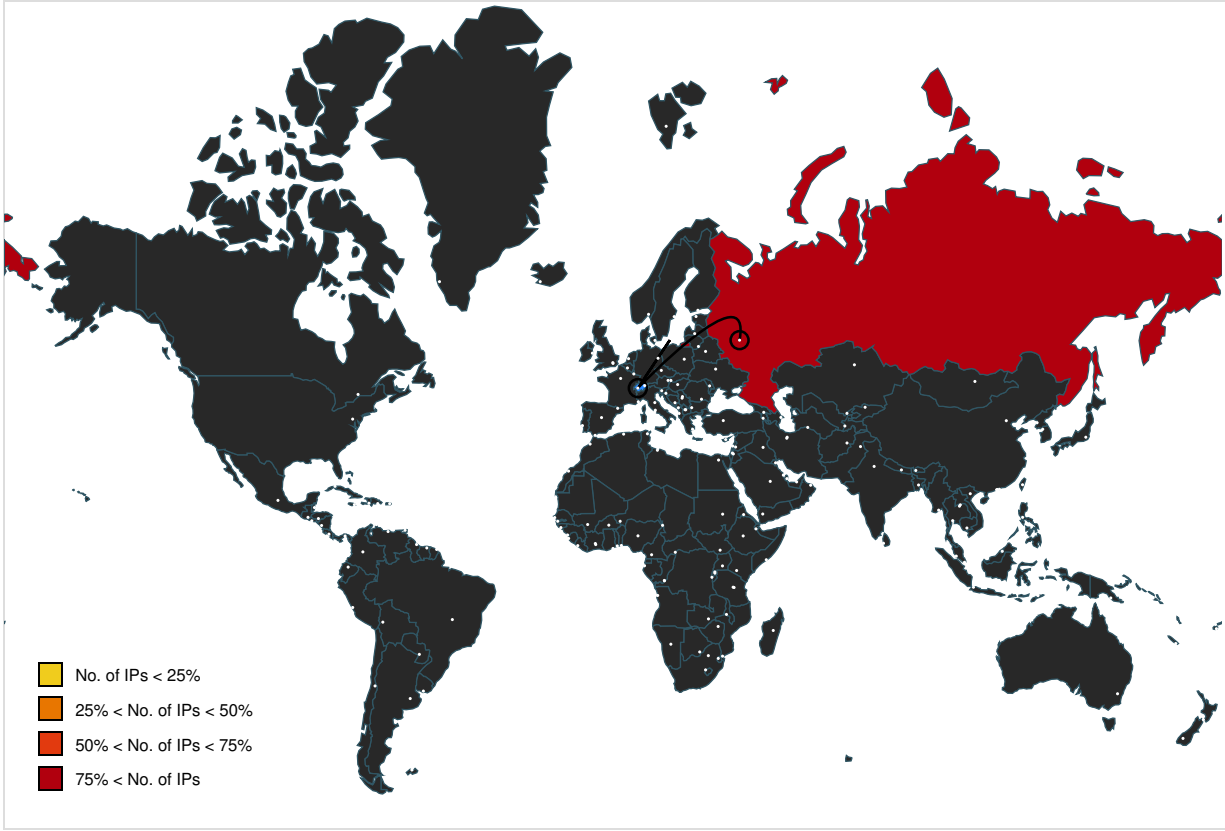
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://5.42.94.169/customer/368	true	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sysinternals.com	jsc.exe	false		high
http://www.sysinternals.comopen/?ICONSHELLRUNASAboutUsage/raw/netonlyRunAsInvoker__COMPAT_LAYERcmd	file.exe, 00000000.00000002.495389743.000001F6D7691000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.493841709.000001F6C77A3000.00000004.00000800.00020000.00000000.sdmp, jsc.exe, 00000002.00000002.492840110.000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://109.206.241.33/files/Hadi.config.CfgEncFileMZ	jsc.exe, 00000002.00000002.492997621.0000000E50000.00000040.00001000.00020000.00000000.sdmp, jsc.exe, 00000002.00000002.493023944.0000000000E66000.00000040.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://5.42.94.169	file.exe, 00000000.00000002.493841709.000001F6C7685000.00000004.00000800.00020000.00000000.sdmp	false	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	file.exe, 00000000.00000002.493841709.000001F6C7685000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.sysinternals.com0	file.exe, 00000000.00000002.493841709.000001F6C76CC000.00000004.00000800.00020000.00000000.sdmp, ?????.sys.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.42.94.169	unknown	Russian Federation		39493	RU-KSTVKolomnaGroupofcompaniesGuarantee-tvRU	false

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882700
Start date and time:	2023-06-06 17:13:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 0s
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:	3
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:	file.exe
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@5/2@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 28.5% (good quality ratio 26.2%) • Quality average: 72.8% • Quality standard deviation: 31.3%

HCA Information:	• Successful, ratio: 76% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
17:14:52	API Interceptor	62x Sleep call for process: file.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1595
Entropy (8bit):	5.378294470225564
Encrypted:	false
SSDEEP:	48:MxHKn1qHGiD0HKeGiYHKGD8AoiHd+vxpNStHTG1hAHKKPz:iqnwmI0qerYqGgAoi0ZPStzG1eqKPz
MD5:	3D4F5C31B249A99B5AC79BB49D9894F3
SHA1:	C7F66B88EB5A896E235CB6C37CC752C225119173
SHA-256:	472C344E0D0AB687ED38440FCE12C0E010957CF27C4514710C0683F15DC0DEC5
SHA-512:	CF6805ACC8DAEBFB21DC467BF533D6D68BC9EF5BED519D1DF0833BFB5E982E54828702A672EBD971EFE4FC7B828818B8DB57FAC70B673AA5A884B5AB9130CA1E
Malicious:	**true**

Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..2,"System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neut

C:\Users\user\AppData\Local\Temp\?????.sys

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (DLL) (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36208
Entropy (8bit):	6.284053631838433
Encrypted:	false
SSDEEP:	768:tKCM0IWRhm8LiES4cT4iZ923OMqUD6Q4KICJw4:t7/Vhzb3pL4GJw4
MD5:	97E3A44EC4AE58C8CC38EEFC613E950E
SHA1:	BC47E15537FA7C32DFEFD23168D7E1741F8477ED
SHA-256:	440883CD9D6A76DB5E53517D0EC7FE13D5A50D2F6A7F91ECFC863BC3490E4F5C
SHA-512:	8EF7FC489B6FFED9EC14746E526AE87F44C39D5EAFFF0D4C3BFA0B3F0D28450F76D1066F446C766F4C9A20842A7F084FE4A9F94659D5487EA88959FCCB2A96EB
Malicious:	**true**
Yara Hits:	• Rule: PUA_VULN_Driver_Sysinternalswwwsysinternalscom_procexpsys_ProcessExplorer_HoEP, Description: Detects vulnerable driver mentioned in LOLDrivers project using VersionInfo values from the PE header - 97e3a44ec4ae58c8cc38eefc613e950e.bin, Source: C:\Users\user\AppData\Local\Temp\?????.sys, Author: Florian Roth
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3...w.{.w.{.w.{.~...p.{.w.z.H.{.~...t.{.~...t.{.~...t.{."...v.{."..v.{.".y.v.{.Richw.{.....PE..d...l..a....." .....L.....X.....x...(.....`.....l..p!.....0....l..T.....@.....text....%.....&..... ..h.rdata.....@.....*.....@..H.data.....P.....:.....@....pdata.....`.....<.....@..HPAGE.....p.....@.....`INIT.....\..... ..b.rsrc.....f.....@..B.reloc..0.....j.....@..B.....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.697202938635302
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	30720
MD5:	daf761fb9aaa34a9c2120003694d88a3
SHA1:	47fd2695b6da26f6444799d442662b982d70f783
SHA256:	18d4850a10812f3b4d8631939d469b41c1d344a7fa9205acc31b265d0600291b
SHA512:	1ddf3c0b4dcbb4103d24b6a5bb3308dff706c9d9277d411be3f9356e9040e67b04c0c02c9c927ba60c5723a50d746287de34cff5545003a0aed3596ec13fd7b2
SSDEEP:	768:uwVMApolbUGPPMdwdunhdH15FIU/ogyejq:bVLoljn8nhj5FF1jq
TLSH:	68D20800A3F98767EAFB4BF64871124447BA7ABB7936E75D0DC460DB1A637404A01BA3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...Lx}d....."...0.Uk..... ....@.....`.....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General	
Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x647D784C [Mon Jun 5 05:53:16 2023 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:	

Entrypoint Preview
Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x8f4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x8ad8	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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	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	0x6b55	0x6c00	False	0.5057146990740741	data	5.791232238044552	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x8f4	0xa00	False	0.2921875	data	4.376579543169947	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources					
Name	**RVA**	**Size**	**Type**	**Language**	**Country**
RT_VERSION	0xa0b8	0x328	data		

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa3e0	0x328	data	English	United States
RT_MANIFEST	0xa708	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:14:51.786187887 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.835110903 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.835464001 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.860167980 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.911331892 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911371946 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911385059 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911403894 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911417961 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911432028 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911446095 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911465883 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911478996 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911498070 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.911545992 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.911638021 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.960335970 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960397005 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960416079 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960436106 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960455894 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960474014 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960494041 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960513115 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960531950 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960550070 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960567951 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960586071 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960602999 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960619926 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960633993 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.960639000 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960656881 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960675001 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960676908 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.960692883 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960701942 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.960711002 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960728884 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:51.960736990 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:51.960772038 CEST	49708	80	192.168.2.6	5.42.94.169

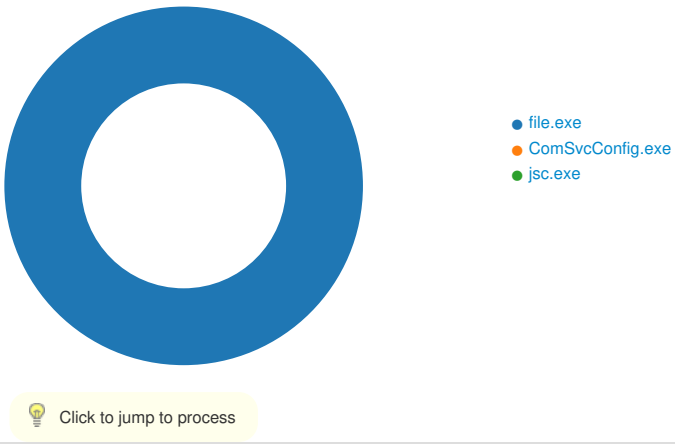
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:14:52.009464979 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009502888 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009522915 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009541035 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009560108 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009574890 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009582043 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009602070 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009619951 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009625912 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009648085 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009649992 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009670973 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009673119 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009691954 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009711027 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009721994 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009732962 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009752989 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009766102 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009774923 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009789944 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009798050 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009819984 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009838104 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009859085 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009860039 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009879112 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009897947 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009902954 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009924889 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009946108 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009948969 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009964943 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.009972095 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.009987116 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010001898 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010008097 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010026932 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010050058 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010062933 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010071039 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010092974 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010097980 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010113955 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010133028 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010142088 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010154963 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010174990 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010181904 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010196924 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010215998 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010221958 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010241985 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010260105 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010277033 CEST	49708	80	192.168.2.6	5.42.94.169
Jun 6, 2023 17:14:52.010282993 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010303020 CEST	80	49708	5.42.94.169	192.168.2.6
Jun 6, 2023 17:14:52.010312080 CEST	49708	80	192.168.2.6	5.42.94.169

HTTP Request Dependency Graph

- 5.42.94.169

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **6988**, Parent PID: **3452**

General

Target ID:	0
Start time:	17:14:48
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x1f6c58b0000
File size:	30720 bytes
MD5 hash:	DAF761FB9AAA34A9C2120003694D88A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.493841709.000001F6C76CC000.00000004.00000800.00020000.00000000.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	7FFCFC74F1E9	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	7FFCFC74F1E9	unknown
C:\Users\user\AppData\Local\Temp\?????.sys	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFB476FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFCFCBB86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\?????.sys	0	36208	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 33 fd 15 fd 77 fd 7b fd 77 fd 7b fd 77 fd 7b fd 7e fd fd fd 70 fd 7b fd 77 fd 7a fd 48 fd 7b fd 7e fd fd fd 74 fd 7b fd 7e fd fd fd 74 fd 7b fd 7e fd fd fd 74 fd 7b fd 22 fd 7f fd 76 fd 7b fd 22 04 fd 76 fd 7b fd 22 fd 79 fd 76 fd 7b fd 52 69 63 68 77 fd 7b fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 6c 18 1b 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0e 1d 00 4c 00	MZ@!L!This program cannot be run in DOS mode.$3w{w{w{~p{wzH{~t{~t{~t{"v{"v{"yv{Richw{PEdla" L	success or wait	1	7FFCFB47B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\file.exe.log	0	1595	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Drawing, Version=4.	success or wait	1	7FFCFCBB8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFC61B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFCFC61B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFC622625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFC61B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFCFC61B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFCFC6F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFCFB47B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFCFB47B526	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TaskKill	success or wait	1	7FFCFB47E75B	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TaskKill	Type	dword	0	success or wait	1	7FFCFBB5A911	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TaskKill	ErrorControl	dword	0	success or wait	1	7FFCFBB5A911	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TaskKill	Start	dword	0	success or wait	1	7FFCFBB5A911	RegSetValueExW
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TaskKill	ImagePath	unicode	\??\C:\Users\user\AppData\Local\Temp\.8ACA.sys	success or wait	1	7FFCFB4803AD	RegSetValueExW

Analysis Process: ComSvcConfig.exe PID: **4572**, Parent PID: **6988**

General

Target ID:	1
Start time:	17:14:59
Start date:	06/06/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ComSvcConfig.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ComSvcConfig.exe
Imagebase:	0x13570130000
File size:	173672 bytes
MD5 hash:	2778AE0EB674B74FF8028BF4E51F1DF5
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: jsc.exe PID: **3068**, Parent PID: **6988**

General	
Target ID:	2
Start time:	17:14:59
Start date:	06/06/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\jsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\jsc.exe
Imagebase:	0x8b0000
File size:	46688 bytes
MD5 hash:	2B40A449D6034F41771A460DADD53A60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 00000002.00000002.492960569.0000000000E30000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_IGoogLoader, Description: Yara detected IgoogLoader, Source: 00000002.00000002.492960569.0000000000E30000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

No disassembly