ID: 828467
Sample Name:
SC_TR11670000.exe
Cookbook: default.jbs
Time: 08:55:19
Date: 17/03/2023
Version: 37.0.0 Beryl

Table of Contents

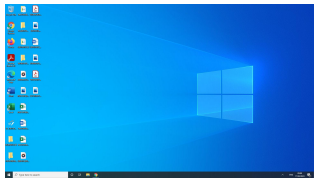
Windows Analysis Report

SC_TR11670000.exe

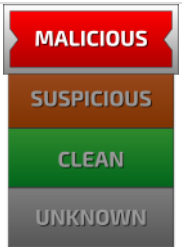
Overview

General Information

Sample Name:	SC_TR11670000.exe
Analysis ID:	828467
MD5:	778f9f61191bf8..
SHA1:	20f3e834b7592..
SHA256:	47b5e835d443...
Infos:	



Detection



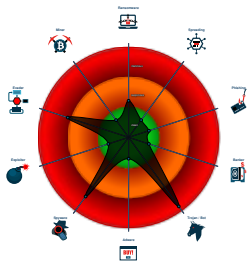
GuLoader, Lokibot

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Lokibot
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to harvest and steal browser in…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- SC_TR11670000.exe (PID: 2852 cmdline: C:\Users\user\Desktop\SC_TR11670000.exe MD5: 778F9F61191BF812A829EDFB93F5B442)
  - SC_TR11670000.exe (PID: 6728 cmdline: C:\Users\user\Desktop\SC_TR11670000.exe MD5: 778F9F61191BF812A829EDFB93F5B442)
    - WerFault.exe (PID: 2396 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6728 -s 212 MD5: 40A149513D721F096DDF50C04DA2F01F)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Loki Password Stealer (PWS), LokiBot	"Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets." - PhishMeLoki-Bot employs function hashing to obfuscate the libraries utilized. While not all functions are hashed, a vast majority of them are.Loki-Bot accepts a single argument/switch of -u that simply delays execution (sleeps) for 10 seconds. This is used when Loki-Bot is upgrading itself.The Mutex generated is the result of MD5 hashing the Machine GUID and trimming to 24-characters. For example: B7E1C2CC98066B250DDB2123.Loki-Bot creates a hidden folder within the %APPDATA% directory whose name is supplied by the 8th thru 13th characters of the Mutex. For example: %APPDATA%\ C98066\.There can be four files within the hidden %APPDATA% directory at any given time: .exe, .lck, .hdb and .kdb. They will be named after characters 13 thru 18 of the Mutex. For example: 6B250D. Below is the explanation of their purpose:FILE EXTENSIONFILE DESCRIPTION.exeA copy of the malware that will execute every time the user account is logged into.lckA lock file created when either decrypting Windows Credentials or Keylogging to prevent resource conflicts.hdbA database of hashes for data that has already been exfiltrated to the C2 server.kdbA database of keylogger data that has yet to be sent to the C2 serverIf the user is privileged, Loki-Bot sets up persistence within the registry under HKEY_LOCAL_MACHINE. If not, it sets up persistence under HKEY_CURRENT_USER.The first packet transmitted by Loki-Bot contains application data.The second packet transmitted by Loki-Bot contains decrypted Windows credentials.The third packet transmitted by Loki-Bot is the malware requesting C2 commands from the C2 server. By default, Loki-Bot will send this request out every 10 minutes after the initial packet it sent.Communications to the C2 server from the compromised host contain information about the user and system including the username, hostname, domain, screen resolution, privilege level, system architecture, and Operating System.The first WORD of the HTTP Payload represents the Loki-Bot version.The second WORD of the HTTP Payload is the Payload Type. Below is the table of identified payload types:BYTEPAYLOAD TYPE0x26Stolen Cryptocurrency Wallet0x27Stolen Application Data0x28Get C2 Commands from C2 Server0x29Stolen File0x2APOS (Point of Sale?)0x2BKeylogger Data0x2CScreenshotThe 11th byte of the HTTP Payload begins the Binary ID. This might be useful in tracking campaigns or specific threat actors. This value value is typically ckav.ru. If you come across a Binary ID that is different from this, take note!Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption.The Content-Key HTTP Header value is the result of hashing the HTTP Header values that precede it. This is likely used as a protection against researchers who wish to poke and prod at Loki-Bots C2 infrastructure.Loki-Bot can accept the following instructions from the C2 Server:BYTEINSTRUCTION DESCRIPTION0x00Download EXE & Execute0x01Download DLL & Load #10x02Download DLL & Load #20x08Delete HDB File0x09Start Keylogger0x0AMine & Steal Data0x0EExit Loki-Bot0x0FUpgrade Loki-Bot0x10Change C2 Polling Frequency0x11Delete Executables & ExitSuricata SignaturesRULE SIDRULE NAME2024311ET TROJAN Loki Bot Cryptocurrency Wallet Exfiltration Detected2024312ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M12024313ET TROJAN Loki Bot Request for C2 Commands Detected M12024314ET TROJAN Loki Bot File Exfiltration Detected2024315ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M12024316ET TROJAN Loki Bot Screenshot Exfiltration Detected2024317ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M22024318ET TROJAN Loki Bot Request for C2 Commands Detected M22024319ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M2	• SWEED • The Gorgon Group • Cobalt	http://blog.reversing.xyz/reversing/2021/06/08/lokibot.htmlhttp://reversing.fun/posts/2021/06/08/lokibot.htmlhttp://reversing.fun/reversing/2021/06/08/lokibot.htmlhttp://www.malware-traffic-analysis.net/2017/06/12/index.htmlhttps://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws

Malware Configuration

No configs have been found

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\Krugerite.Fri	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.23294314112.00000000028DD000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000004.00000002.24273911659.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000001.00000002.24272353899.0000000003330000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000001.00000002.24272353899.0000000003E2A000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: SC_TR11670000.exe PID: 2852	JoeSecurity_GuLoader_3	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.11.20 - Destination IP: 171.22.30.147

Timestamp:	192.168.11.20171.22.30.14749842802024317 03/17/23-08:58:50.216236
SID:	2024317
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Checkin - Source IP: 192.168.11.20 - Destination IP: 171.22.30.147

Timestamp:	192.168.11.20171.22.30.14749842802025381 03/17/23-08:58:50.216236
SID:	2025381
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.11.20 - Destination IP: 171.22.30.147

Timestamp:	192.168.11.20171.22.30.14749842802021641 03/17/23-08:58:50.216236
SID:	2021641
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN LokiBot Checkin M2 - Source IP: 192.168.11.20 - Destination IP: 171.22.30.147

Timestamp:	192.168.11.20171.22.30.14749842802825766 03/17/23-08:58:50.216236
SID:	2825766
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.11.20 - Destination IP: 171.22.30.147

Timestamp:	192.168.11.20171.22.30.14749842802024312 03/17/23-08:58:50.216236

SID:	2024312
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Networking

Snort IDS alert for network traffic

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

Stealing of Sensitive Information

Yara detected Lokibot

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

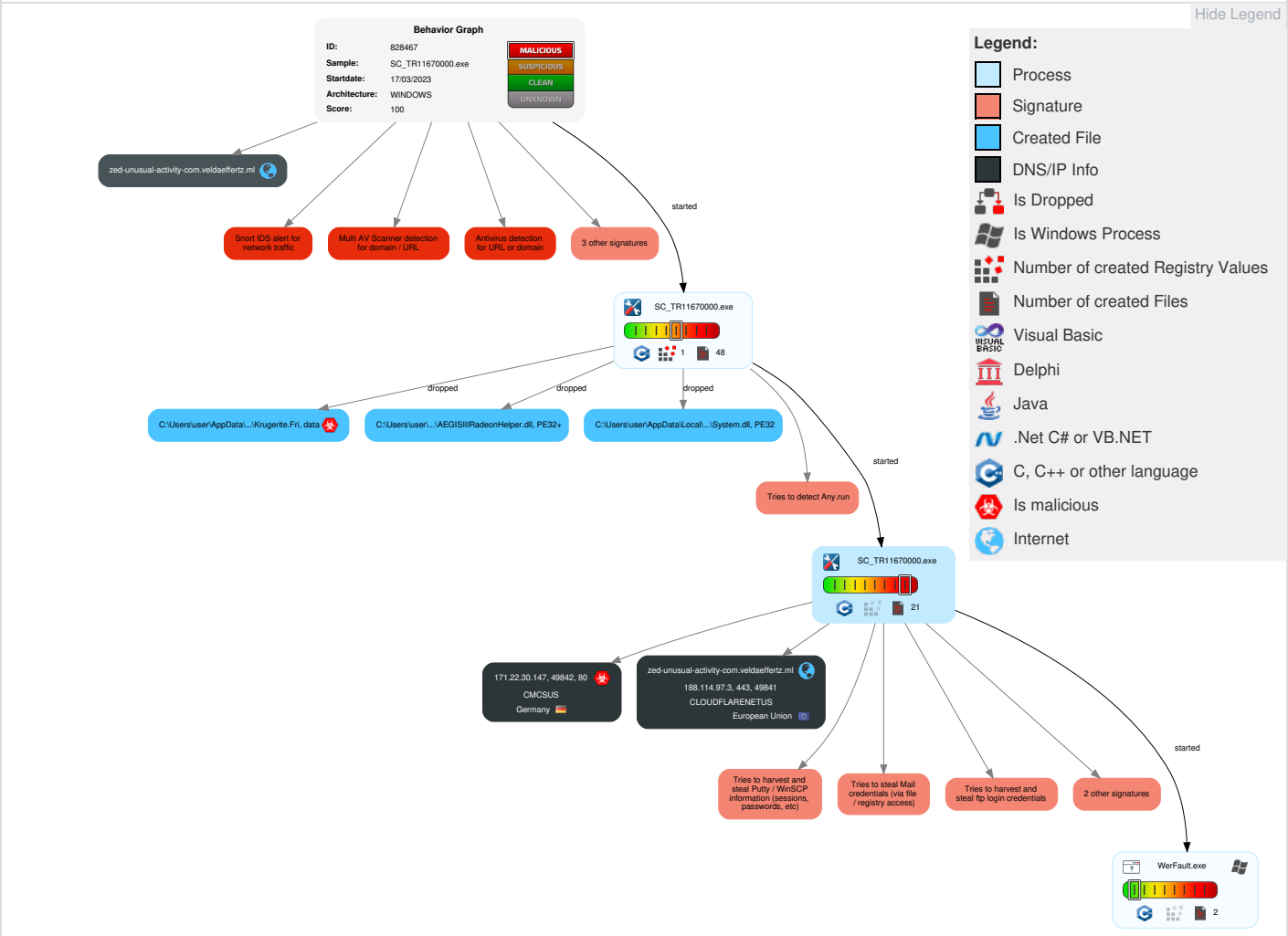
Yara detected Lokibot

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	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 Masquerading	2 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	5 System Information Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System 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	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

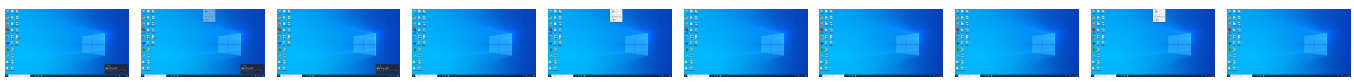
Behavior Graph

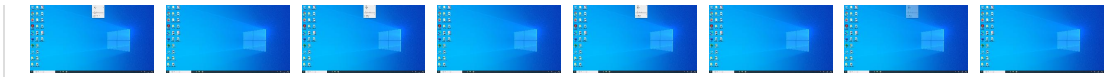


Screenshots

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
SC_TR11670000.exe	48%	Virustotal		Browse
SC_TR11670000.exe	51%	ReversingLabs	Win32.Trojan.Kryni s	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nss6D2B.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\AEGISIIIRadeo nHelper.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.SC_TR11670000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.12 23491		Download File
1.2.SC_TR11670000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.12 23491		Download File
1.0.SC_TR11670000.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.12 23491		Download File

Domains

Source	Detection	Scanner	Label	Link
zed-unusual-activity-com.veldaeffertz.ml	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://171.22.30.147/flowe/five/fre.php	100%	Avira URL Cloud	malware	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://https://zed-unusual-activity-com.veldaeffertz.ml/CodkZc57.sea	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zed-unusual-activity-com.veldaeffertz.ml	188.114.97.3	true	false	• 7%, Virustotal, Browse	unknown

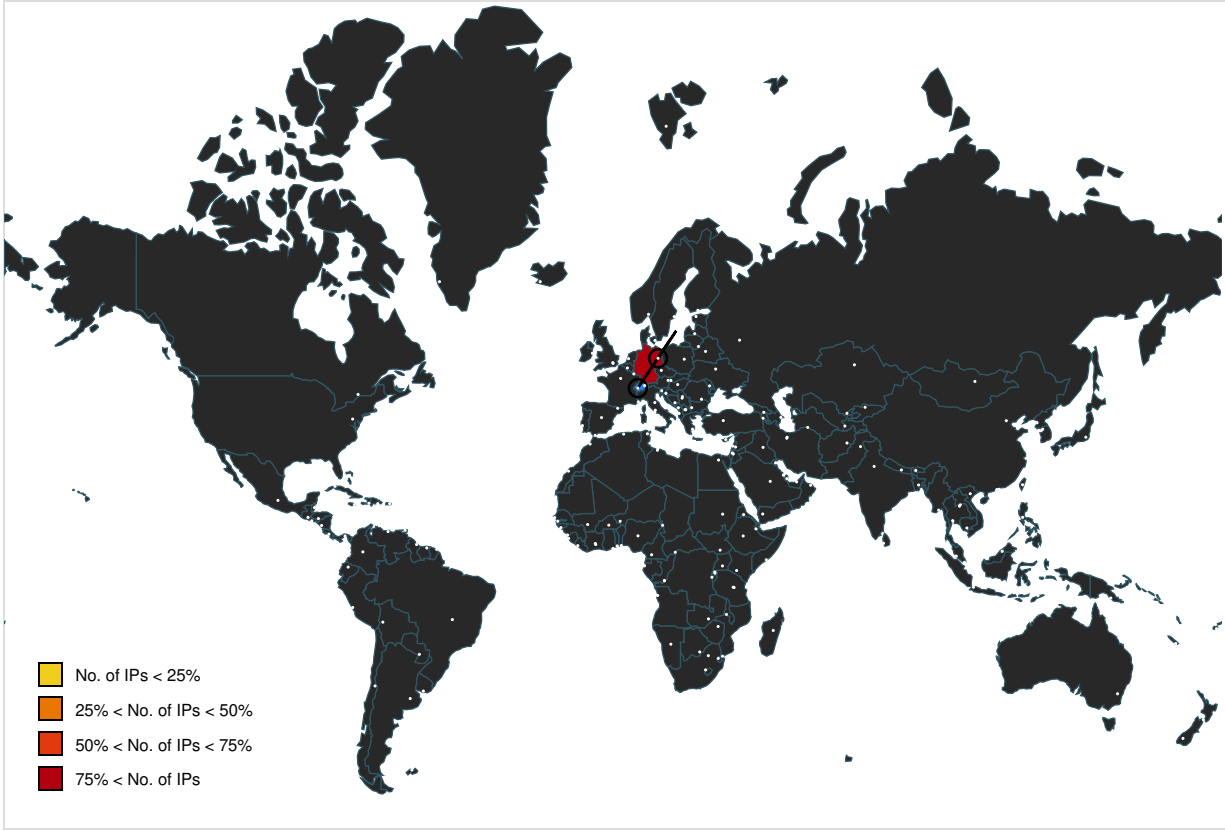
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://171.22.30.147/flowe/five/fre.php	true	• Avira URL Cloud: malware	unknown
http://https://zed-unusual-activity-com.veldaeffertz.ml/CodkZc57.sea	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	SC_TR11670000.exe, 00000004.00000001.24088641658.0000000000649000.00000020.00000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	SC_TR11670000.exe, 00000004.00000001.24088641658.00000000005F2000.00000020.00000001.01000000.00000006.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	SC_TR11670000.exe, 00000004.00000001.24088641658.00000000005F2000.00000020.00000001.01000000.00000006.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	SC_TR11670000.exe, SC_TR11670000.exe, 00000001.00000000.23291984818.0000000000409000.00000008.00000001.01000000.00000003.sdmp, SC_TR11670000.exe, 00000001.00000002.24270690849.0000000000409000.00000004.00000001.01000000.00000003.sdmp, SC_TR11670000.exe, 00000004.00000000.24087597436.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	SC_TR11670000.exe, 00000001.00000000.23291984818.0000000000409000.00000008.00000001.01000000.00000003.sdmp, SC_TR11670000.exe, 00000001.00000002.24270690849.0000000000409000.00000004.00000001.01000000.00000003.sdmp, SC_TR11670000.exe, 00000004.00000000.24087597436.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	SC_TR11670000.exe, 00000004.00000001.24088641658.0000000000626000.00000020.00000001.01000000.00000006.sdmp	false		high
http://www.gopher.ftp://ftp.	SC_TR11670000.exe, 00000004.00000001.24088641658.0000000000649000.00000020.00000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	SC_TR11670000.exe, 00000004.00000001.24088641658.0000000000649000.00000020.00000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
171.22.30.147	unknown	Germany		33657	CMCSUS	true
188.114.97.3	zed-unusual-activity-com.veldaeffertz.ml	European Union		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828467
Start date and time:	2023-03-17 08:55:19 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	8
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:	SC_TR11670000.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/19@1/2
EGA Information:	• Successful, ratio: 50%

HDC Information:	• Successful, ratio: 51.2% (good quality ratio 50.4%) • Quality average: 88.2% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, wdcp.microsoft.com
- Report creation exceeded maximum time and may have missing d isassembly code information.
- 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

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

C:\Users\user\AppData\Local\Temp\Kontos.ini

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	54
Entropy (8bit):	4.838039816898156
Encrypted:	false
SSDEEP:	3:7KG/LmI/cXQQLQIfLBJXmgxv:OG/LmI/cXQQkIP2I

MD5:	FB5EE2C0CAC332EC8390F50016EF0769
SHA1:	11D9FB52FE5289140B9D52A38B56F99512B3A3A7
SHA-256:	C557AFE51AB22916E3423820A09D3805BF9DCDCECBEC4FE8DE2C67FB023BA631
SHA-512:	87CCEA7B203B8BFC4E21544FE4FE9693AF230E246C450E673410565791DFE8257E30354772FDCC114C7068D9295FDB491E9B52D1A3B490C0756E568B70B95C0A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	[Bedrock]..Interthing=user32::EnumWindows(i r1 ,i 0)..

C:\Users\user\AppData\Local\Temp\nss6D2B.tmp\System.dll

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.832316471889005
Encrypted:	false
SSDEEP:	192:4PtkiQJr7jHYT87RfwXQ6YSYtOuVDi7lsFW14Ll8CO:H78TQlgGCDp14LGC
MD5:	B0C77267F13B2F87C084FD86EF51CCFC
SHA1:	F7543F9E9B4F04386DFBF33C38CBED1BF205AFB3
SHA-256:	A0CAC4CF4852895619BC7743EBEB89F9E4927CCDB9E66B1BCD92A4136D0F9C77
SHA-512:	F2B57A2EEA00F52A3C7080F4B5F2BB85A7A9B9F16D12DA8F8FF673824556C62A0F742B72BE0FD82A2612A4B6DBD7E0FDC27065212DA703C2F7E28D199696F66E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....oZ.....!..... .....(.....0.....`.....@.....2.....0..P.....P.....0..X..... .....text...O..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3425316567-2969588382-3778222414-1001\1b1d0082738e9f9011266f86ab9723d2_11389406-0377-47ed-98c7-d564e683c6eb

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	1.1262763721961973
Encrypted:	false
SSDEEP:	3:/lSlIIEXln:AWE1
MD5:	D69FB7CE74DAC48982B69816C3772E4E
SHA1:	B1C04CDB2567DC2B50D903B0E1D0D3211191E065
SHA-256:	8CC6CA5CA4D0FA03842A60D90A6141F0B8D64969E830FC899DBA60ACB4905396
SHA-512:	7E4EC58DA8335E43A4542E0F6E05FA2D15393E83634BE973AA3E758A870577BA0BA136F6E831907C4B30D587B8E6EEAFA2A4B8142F49714101BA50ECC294DDB0

Malicious:	false
Preview:	.....user.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Brandmurens\Antirevolutionist\Nitrosobacterium\Eliksirens\dotnet.api

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Brandmurens\Antirevolutionist\Nitrosobacterium\Eliksirens\ebook-reader.png

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	555
Entropy (8bit):	7.499536740374189
Encrypted:	false
SSDEEP:	12:6v/7anZhFxDEKwjAq0kaO/yvSL6T1pjNngLpzPanwmB9HE4JqSjF:5bDEPxdqKLmpqLdynw29kEqSZ
MD5:	BFF011148B773FA44B9A9BB029E8CC52
SHA1:	F2B838927E320D12649CEFDEA3AFE383C6650D7C
SHA-256:	B21DE7B432A7A67544D007ECC0FDD95F8E8C6129AF558A32102EE04C08635653
SHA-512:	A57C83AEE0E1F4C530D2F5B90589C31FD6E2FF8F62F998963284218FAC5EE164BCA7A619A9597DC3E2ECD0095A2CF04467E89EDF86700E1A90B3DF60B5121C9B
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.....A....v...b.m.A..Q..Q..UD5.F.m.....fs{9.}...V.`....%.kt....R...+%7.}p..@.}:..u466`.6uu.tvv...N6....D"Q.....po".;.4....W..g.b..\.~?...<.../....$..5.....r.+..ah...F;.H.`b ....4.[...k.6.<..Kk.m[h..x`...R...z{.H.....Oax.e..{.....w._...c._>..6..T*HY.1! e.#....G.....{.AB..l.K"..P(..j..$.R.}L.5.....@.>.....X...hE....L.."L. ....=~..7n.2.,RJ.01.....B.AWW..<q.....Ng.,../.Z...+...N].r.5.EB.p$..!,....,.....SW.TD+U...K...ee._.N*.[..`..1q..v\#6..?;7..4..3....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Brandmurens\Antirevolutionist\Nitrosobacterium\Eliksirens\emblem-photos-symbolic.svg

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	680
Entropy (8bit):	5.109191824773878
Encrypted:	false
SSDEEP:	12:t4CP5GEA9xl7jhz4AeW02KdTwWjhz4AeW02KdTPqkoop4p:t4CBGEAgF4AeW0/N4AeW0/Zqg4p
MD5:	379690952AAA576521D51249D404CBCD
SHA1:	61A8A95B0454422AA47379CF983B99FFDD839439
SHA-256:	EAD402FB0B85DB153356EC695016FD4F2C4031367D8ED6D1C1EF5FF4F28A8DE8
SHA-512:	35B6BC866C3D02A2486D3447C82405103DE89D46940F7FE44A7009E714BBA57FBE601EEC939C3206ADB06FB31C4FD1D3822A0ED52A346ACFDE5908643432F92
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#000" fill="#474747"><path d="M13 5v2h1v5H4v2h12V5z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" font-weight="400" font-family="Sans" overflow="visible"/><path d="M0 2v9h12V2zm2 2h8v5H2z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" font-weight="400" font-family="Sans" overflow="visible"/><path d="M3 7c2.32 1 3.045-1.66 6 0v1H3z" style="marker:none" overflow="visible" opacity=".35"/></g></svg>

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Brandmurens\Antirevolutionist\Nitrosobacterium\Eliksirens\font-select-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	220
Entropy (8bit):	6.546211943247282
Encrypted:	false
SSDEEP:	6:6v/lhPysde0C1jngP3V95D2tOA/RDvhpLUxbVp:6v/7jC1zi3Sr/hW
MD5:	C84EE7522C124892455BB09DEBCF9340
SHA1:	AF87A2A5688346A3902762DD250328B7EF224620
SHA-256:	E0A3BD6FE1A1BAEFFE04BCA2980ADF755F888E31DCE3686B16C5DAC4202A38C8
SHA-512:	3BEED79366F15CD075781F677C0C9E84081D2189D1FB541A34AA25980B48701A3D93DC550E4ABEB550EFBE3167B1CAB8338E22F4603C6A71936876FBA75FAD58
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...=..P.../z.Q..Kx....l.b.)...x.....t.....Y~.).....7.....W.xk.'A...u.....%..!k.k5.|E=+X..,a.S.H4p*D8.8(FH.a..5.x...%.....7..8s:.....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Brandmurens\Antirevolutionist\Nitrosobacterium\Eliksirens\network-wired-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	144
Entropy (8bit):	5.708279548998072
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllAoSF1/LvgStjP9f9uvJYUo+/JHt//sup:6v/lhPysKo21/Lvlt7V9+YUouJH1/jp
MD5:	1ED278AD206D6EA33FF787DD326E0FC5
SHA1:	8CFF7AD12FC0E5545E71D05879A0245BEDAF4D46
SHA-256:	CC88E76F7C7D2E5B07E49D1F2AD88F8BAFC0542EB11CEB2B2FFF235C87AB4417
SHA-512:	7291085B6153C02EDBF679CDDB93B97DBB74943F216EB622CE9722E02613269F626F8A7A5BE8DA683153E9AEE22C40ED7264E8A0ED62A99F477E2B96642596BF
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....GIDAT8.c`..0...O.Z&J]0.. ...&u]..5?.....b....Q.E./.....t@..,....)1..,b...#.=....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Brandmurens\Antirevolutionist\Nitrosobacterium\Eliksirens\pan-start-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	140
Entropy (8bit):	5.529383944212929
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllDM9vFW0p/sXm1MMos9DwlTYTbklt/sbp:6v/lhPysx8vFW0pkX4iZlTYTI3Ebp
MD5:	4308BBBAB1DB146494AE5ABB07B8E6DB
SHA1:	58121574EEB070E26DDD75A964F3548E176E58A4
SHA-256:	EFB732049C674EB25BFCB2FA0CBCC45D24190BF1479C054647F424B31E34C828
SHA-512:	41C9B37516F8D6AB7155F890EE36C26FE4161383A93BFBF696AB18292774C3556642E898361D21CECCBFEFFAF5814495CFAC2C74791E02F068B055BD3AD87DE
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....CIDAT8.c`.J..R..(...\.`..2.Y3...k.i.....b..PN.....J.@6.I.`.Pd..A.....O...D....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Fadernes\Amphiaster213\printer-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	147
Entropy (8bit):	5.834297280344084

Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllPhF1MzoQxJrN7djpdXLImeR/mV2kg1p:6v/lhPysx1MzoQxlRZbCRaip
MD5:	38D787F55E22FB591135F9250CD259D4
SHA1:	0E135B0E1CA49A6E43DB4CB7596FAEA022E23924
SHA-256:	1ED839B015A67CAB9948469975411D982A96314CE82851EA2F9F6BB8D733A002
SHA-512:	4E21AB54B7110B4CD2EBC0E2CF6DF3F8C7C988495BCCA76949BC3C5EB669A793FCCDA5CB4DDB7B627A21734BD181FE44670757144CC2A007FCB695405F08EC2B
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....JIDAT8.c`..0b..O..&J]@5....tR.>.....`.8.(6....-Z....a..&..3 ....4...<.....IEND.B`.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\AEGISIIIRadeonHelper.dll

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	34016
Entropy (8bit):	6.1021284380541925
Encrypted:	false
SSDEEP:	384:JP7a6wQdSCVWSdoEdXjYmxzfkfIwuWR7UPMEdxsTStsBdMQJK2wKucYkcuhV3:N7a6eiHdFdr7W5UPMgy+OBG2X90uhV3
MD5:	4FC7FC174E80C178225C2509027DF961
SHA1:	9FF62413EC0DD462F5F016EBC804F1D736D24796
SHA-256:	866B31DD39B97DEDAFD0FBD5672639EE91B47AD319C47816B4F6D01BFF93FF8C
SHA-512:	29261B9ABC4AF2F51C05B61A37721BC737B411530361A4B48A7BFFAB0F8263EA75BFD51B6E6E94E91E1D02DC442B534C3334B05FD8324E7CF307FA08179A1ED9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.oPZ.oPZ.oPS..PR.oP..nQX.oP..jQK.oP..kQR.oP..IQ X.oP).nQY.oPZ.nPt.oP..fQY.oP..oQ[.oP..P[.oPZ..P[.oP..mQ[.oPRichZ.oP.....PE..d....5;a....." ....0...:.....F....`..... ..\.....]....H.....f.....H....O..p.....@P.....@..p.....text.....0..... ..`.rdata...#...@...$...4.....@..@.data...@....p..... X.....@....pdata.....Z.....@..@.rsrc...H.....^.....@..@.reloc..H.....d.....@..B..... .....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\Cementblander.Pfe

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	data
Category:	dropped
Size (bytes):	40788
Entropy (8bit):	4.589793625224697
Encrypted:	false
SSDEEP:	768:DUa4mGn6n+kvKNlpCMP7Llxd7kcrTZ7m3Rpck:QDm1+zHTrTZsP
MD5:	9B6AD96E03564D53EBE96EA4529819D3
SHA1:	74B86EC24C053C083CF85BC1B9B2A33E5C34FC81
SHA-256:	AE83602A47931BA1E9DD2A64C03A314AED410A4C5D100D6A724041C38213CEF2
SHA-512:	A913F2421FAD00A885C022380FE1CFF518D9368E439C355A0A90D6AE6548CFB4EDA1A9C35D19FD4CAA2062F9AA94D44BCBF78A6D43D3CC660B9C86235ACFD92
Malicious:	false
Preview:	......mmm.....99.EE.....^.....UU.....#.....rr.....yy.....d....._.....}}}..../.....ss.T.....U.....>.CCC.....yyyy.....``..c.c.....QQQ.. .....CC.444....X.....Y.....?.....--.....WW..V.....]....j.....s.ss....k.....PPPP.sss.....~~.....-....D.....G.*.....--.....111.....5..... .ii.....J.....MM.....9.h.X.....V..F.....OOOOO.....v.....7....JJJJJJJJ.....CCC...__..@@.....Z..... ..zz.....ooooo..LLL.....F.UU.....R../.....-.t...^.....))).....BB.....9.....-.....--.NNN..l.....<<<.....M. k.....nn.....M....8...JJJJ.yyyyy.....??.....VV.....p.....N.C.....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\Krugerite.Fri

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	data
Category:	dropped
Size (bytes):	291871
Entropy (8bit):	6.780687426184548
Encrypted:	false
SSDEEP:	3072:7YqIuagJ5wYGodW90uakeSjZJgDjhK+jtDTL+pQVrdYM8R4JvUHlFD4gELWSgoJI:uuPko0903YiZxV0QXwjD03LXgALpm
MD5:	2A43E2AF179CD9567C670A702490375F
SHA1:	55B83DDF870907571F22CA6951C6D335520D9B89
SHA-256:	2C3B071D869AC1DBD120A4F0628D1299016EE8C6338A7A3C1A25DB04E00A82A2

SHA-512:	E8EFA4DB3C5669E08C0DCF4E259B9AA04CA3C7977EE4409AF154A6299DC8E31A1C425892E70335274C99BE7B4CA57A1470849E9F8A917EA597EC07848296D29
	9
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\Krugerite.Fri, Author: Joe Security
Preview:	.....>..... ...uu.....F.KKK.'.....'".....O..".....**...@....z.1.....F...6.....<.....E.....555....~~...w.....UU.""".....]]....##..T.....M....22 .....*....l.....PP.....z....j.....$.t.....H.....{.....FF..88.....--.BBB.h.....yyyy...qq.....$.....QQQ.i.....))..... ...www.....888.....!!.....h.y.....]].....d.....K....R.....=.i.....{{{{{{{.....**.....pp.....K.:::.....PPP...d.....).....mm.....W... .../.G.....R.....99999.....G.`..U.....Y.....rrr...3.....uu..... .lll.....-.....2.X.....<...WW.....?....#.....mmm.HHH...t.....!..iii....e.... ....."...;;.....}}.....`````.....

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\LogoCanary.png

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	PNG image data, 600 x 600, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	16669
Entropy (8bit):	7.836876926418697
Encrypted:	false
SSDEEP:	384:dg1Ew+1FT+/6trrKWzge5jh2xmalhctpNy:W1E1c6tru1CUYa4tDy
MD5:	F80867A421C85C6E2865CF85FF7C4B02
SHA1:	C3EAB6B7E92646FE3407B2B3C5AFFE13A7873C48
SHA-256:	BCAA3B1333919176137D4DE4B1E3F31126159B12F959D7277BD8537B95139BD3
SHA-512:	06B51E660AEE86FC3BB068C6DEA046920E04F86B8EDD02E640EAC619F0F0D7E87E5CAE5BE1390CEBC5DFE70AA13BAB1710176E88C9D1C859182629D429745D
	78
Malicious:	false
Preview:	.PNG.....IHDR...X...X.....f.....tEXtSoftware.Adobe ImageReadyq.e<..@.IDATx.....\.}..../...].{`.....D.\..u.....#..V.eW.G>"W....V..d..IVU".:.D<$J.....{q/.....`0g./..z....A.`. .?..p....M....._'...L...]~.....;.....,..... ....X.....@`.. .....@`...,.... ....X.....@`.. .....@`...,.....X.....@`.. .....@`...,.....X..... .....@`...,.....X..... .....@`..., .....X..... .....@`...,.....X..... .....@`...,.....X..... .....@`...,.....X..... .....@`...,.....X...,.... ....~.....N...@...C{..o.?2.....x...?_.....sC..O8...n..J.ttbv9. ..w~...ym..O.....vq"f..qrjt9... ..].S..Hz.gf}.,.Sm!...>..Xh..:S.};d.....2..?.....2...1..ep...K.{.?..@`.7=...7U..C.....S...6....|a.}]..._..d...._.....+__..JS.....X.u...;..Q.x.z9...eP5f.H..nnz. &h...4.kz.....&....o)..=..x.=...y ....6i...wL.....Y(.2NRP..J...HL/K#^izqpbUp}...q...g....."....4R..#.VFrR|.LF>w~.Pm..\..4.5t{.-..

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\avatar-default-symbolic.svg

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	266
Entropy (8bit):	4.986245244009802
Encrypted:	false
SSDEEP:	6:tI9mc4slzc8SRIKMNo/aMhFI1OkUjq5eKVrGDVfqKlNK+:t4C8LKMuyMhPobjoprGDRlj
MD5:	8B727826F9D8C0C7C954EDE912CB0DEB
SHA1:	1518AA80747326B5353C22D32E57A33D61285119
SHA-256:	0783A7F518D3879C8F0F50B45FBD779A98652469E9B7C659CE41F14D1629D334
SHA-512:	0ABB243F9D1E0B6EDA0CB25D35C3449AB2B5B83078208F11B876A27FF11FF70B79F8BA97D4DA3AED21A8314C75FB2174D9378AF59B57DCB99DFF681D9AAB85
	61
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <path d="M8 1a3 3 0 100 6 3 3 0 000-6zM6.5 8A4.49 4.49 0 002 12.5V14c0 1 1 1 1 1h10s1 0 1-1v-1.5A4.49 4.49 0 009.5 8z" style="marker:none" color="#bebebe" overflow="visible" fill="#2e3436"/>.</svg>.

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\be.txt

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12193
Entropy (8bit):	4.4720152705808935
Encrypted:	false
SSDEEP:	192:i2PDEeaNB1PmcptkcDHxbTvPnc67bMxQxGx4ch/JuLQRcg/oN96bPNljYiYr197:ikDFKBFmcPLx3HPnIsqrJuqcgAN96b87
MD5:	3C21135144AC7452E7DB66F0214F9D68
SHA1:	B1EC0589D769EAB5E4E8F0F8C21B157EF5EBB47D
SHA-256:	D095879B8BBC67A1C9875C5E9896942BACF730BD76155C06105544408068C59E
SHA-512:	0446A0E2570A1F360FD8700FD4C869C7E2DBB9476BBDEC2526A53844074C79691542B91455343C50941B8A6D5E02A58EE6AA539CC4C4AE9CF000B4034EF663E
Malicious:	false

Preview:	.;!@Lang2@!UTF-8!..; : Kirill Gulyakevitch..; 9.07 : 2011-03-15 : Drive DRKA..;..;..;..;..;..;..;..;..0..7-Zip..Belarusian.....401..OK.....&.....&....&..... .....&.....440..... ... &..... ... .&.....&.....&.. ....&..... ....?..500..&.....&.....&.....&.....&.....&.....540..&..... ..... &..... .&.....&.....&.....&..... .....&..... .....&.....&..... .....&.'..... .....&.....&..... .....Diff..&..... .

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Lejningerne\changes-allow-symbolic.svg

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	998
Entropy (8bit):	5.186938379246791
Encrypted:	false
SSDEEP:	24:t4CBGD0QNRWLLxo2em0yKbRAecFxV0/wXK:gDrc0NtAecFiH
MD5:	CB1EEE7BDB582B756D0F68EF02D6D96D
SHA1:	9E9B0F25BC472EF1C1C13EEAC12FD11C4CC0D2D9
SHA-256:	20EA767E852A8EBF2C5BA16D56CBAE10BD09D6CBA89B372A57EAA973AD3281B4
SHA-512:	E22FAEAE78D244A0F4E7215B31125D5AA4FD66C0720B0DE61D12084EAB879D7A9E231CCD5CD431417115B0945B450DC348DA400D67DB1898513B7BD6B9C274DB
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g color="#bebebe" fill="#474747"><path d="M3 9h10c.554 0 1 .446 1 1v3c0 .554-.446 1-1 1H3c-.554 0-1-.446-1-1v-3c0-.554.446-1 1-1z" style="marker:none" overflow="visible"/><path d="M7 0s-.709-.014-1.447.356C4.814.725 4 1.666 4 3v3h2V3c0-.667.186-.725.447-.855C6.71 2.014 7 2 7 2h2s.291.014.553.145c.261.13.447.188.447.855v8h2V3c0-1.333-.814-2.275-1.553-2.644C9.71-.014 9 0 9 0z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M2 12h12v4H2z" style="marker:none" overflow="visible"/></g></svg>

C:\Users\user\AppData\Roaming\fumigatorium\Tertser\Omstrukturdnr\Preconstituent\Uforsonligere\Informationssystemernes\pt-br.txt

Process:	C:\Users\user\Desktop\SC_TR11670000.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	9515
Entropy (8bit):	5.04214621707661
Encrypted:	false
SSDEEP:	192:icoGT04mzNN8hYivh5gtE/PkjY09fdNQuQ:ibGg4mzNhi4tEHoDfHQuQ
MD5:	7B02E1AE16E2E709D7C97DE560B4DBE9
SHA1:	191A54644417F7D36F5CB4182DCDB3737D74BE51
SHA-256:	DA0B58F52BBC131F967942D1D8E9DE1B5721AE864BC21852A0AD4062332297CB
SHA-512:	4F689F854DB3F766B5E53CE2F19E9F8293C075EE3F9B18098EB05B352F2EC95DF85E49A78540781EB531BCE60C7B1F7890F1FE3C65200DEC3CB908E90FB827A1
Malicious:	false
Preview:	.;!@Lang2@!UTF-8!..; : Francisco Jr..; 4.37 : Fabricio Biazzotto ..; 18.05 : Atualizado por Felipe..;..;..;..;..;..;..;..0..7-Zip..Portuguese Brazilian..Portugu.s Brasileiro..401..OK..Cancelar.....&Sim..&N.o..&Fechar..Ajuda....&Continuar..440..Sim pra &Todos..N.o pra T&odos..Parar..Reiniciar..&Em 2. plano..&Em 1. plano..&Pausar..Pausado..Voc. tem certeza que voc. quer cancelar?..500..&Arquivo..&Editar..&Visualizar..F&avoritos..&Ferramentas..&Ajuda..540..&Abrir..Abrir &por Dentro..Abrir p&or Fora..&Visualizar..&Editar..Re&nomear..&Copiar Para.....&Mover Para.....&Apagar..&Dividir arquivo.....Com&binar arquivos.....P&ropriedades..Comen&t.rio..Calcular checksum..Diff..Criar Pasta..Criar Arquivo..S&air..Link..&Correntes Alternantes..600..Selecionar &Tudo..Desmarcar Tudo..&Inverter Sele..o..Selecionar.....Desmarcar...Selecionar por Tipo..Desfazer sele..o por Tipo..700...co&nes Grandes...c&ones Pequenos..&Lista..&Detalhes..730..Desorganizado..Visualiza..o

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.55806590652357
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SC_TR11670000.exe
File size:	329416
MD5:	778f9f61191bf812a829edfb93f5b442
SHA1:	20f3e834b759252210d047091bc98c47e7e6ffdd
SHA256:	47b5e835d443cde52de78c36998cf1e312d391501226238ea00968139790e32d
SHA512:	77e917288d88cbb90bc7e67f423546d766571d926ab3b0f9b0749735b3d4ef48020fc66a861bc15afc131ec8afca55504a2aeb2c604bd1c36b1591e8e0c4242d

SSDEEP:	6144:VDkBNYb/zy86tyPhzKpqs1z3WRA8ZbO7Sv4Zbf9CbTqGErmroIbvF:O3gUtuzaq+zwjZbrc4Tqxrmrh9
TLSH:	A064F1253AB1C033FD954170CAA5D6F3E229FE48C924C18777A43F6EB9315848549EBB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L...+.oZ.....`.....

File Icon

Icon Hash:	08c2b0d8cc64b046

Static PE Info

General

Entrypoint:	0x4031d6
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5A6FED2B [Tue Jan 30 03:57:31 2018 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:	3abe302b6d9a1256e6a915429af4ffd2

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Forureningsraads@Selvbebrejdelser.Bve, OU="nucal bisserups Nigher ", O=Admirer, L=Eastabuchie, S=Mississippi, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 08/07/2022 04:08:29 07/07/2025 04:08:29
Subject Chain	• E=Forureningsraads@Selvbebrejdelser.Bve, OU="nucal bisserups Nigher ", O=Admirer, L=Eastabuchie, S=Mississippi, C=US
Version:	3
Thumbprint MD5:	F6FF0FF5CCC259F19FAA81DDC8079502
Thumbprint SHA-1:	AC5B272F037D232BD3181F065A062D0D45E91C45
Thumbprint SHA-256:	9D58D97305576E4D1E04A49E8F14AADA686A7693DCBEF30297267F3B724593AD
Serial:	421F24E2B8A1818548F8C8D7DBE6D51C18A183FA

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A0h]
call dword ptr [0040709Ch]
and eax, BFFFFFFFh

Instruction
cmp ax, 00000006h
mov dword ptr [0042370Ch], eax
je 00007FB75D177323h
push ebx
call 00007FB75D17A3FAh
cmp eax, ebx
je 00007FB75D177319h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007FB75D17A376h
push esi
call dword ptr [00407098h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FB75D1772FDh
push 0000000Ah
call 00007FB75D17A3CEh
push 00000008h
call 00007FB75D17A3C7h
push 00000006h
mov dword ptr [00423704h], eax
call 00007FB75D17A3BBh
cmp eax, ebx
je 00007FB75D177321h
push 0000001Eh
call eax
test eax, eax
je 00007FB75D177319h
or byte ptr [0042370Fh], 00000040h
push ebp
call dword ptr [00407044h]
push ebx
call dword ptr [00407288h]
mov dword ptr [004237D8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407178h]
push 00409188h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories			
Name	**Virtual Address**	**Virtual Size**	**Is in Section**
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x36000	0xa3c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x4fcb8	0xa10	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x7000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5f0d	0x6000	False	0.6649169921875	data	6.450520423955375	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1248	0x1400	False	0.4275390625	data	5.007650149182371	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1a818	0x400	False	0.6376953125	data	5.129587811765307	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x24000	0x12000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x36000	0xa3c0	0xa400	False	0.0760766006097561	data	1.8822021165260459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x36268	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x365d0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 0	English	United States
RT_DIALOG	0x3fa78	0x144	data	English	United States
RT_DIALOG	0x3fbc0	0x13c	data	English	United States
RT_DIALOG	0x3fd00	0x120	data	English	United States
RT_DIALOG	0x3fe20	0x11c	data	English	United States
RT_DIALOG	0x3ff40	0xc4	data	English	United States
RT_DIALOG	0x40008	0x60	data	English	United States
RT_GROUP_ICON	0x40068	0x14	data	English	United States
RT_MANIFEST	0x40080	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetTempPathA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, Sleep, GetTickCount, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GetWindowsDirectoryA, SetCurrentDirectoryA, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, lstrcmpiA, CreateThread, GlobalLock, lstrcmpA, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor

DLL	Import
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

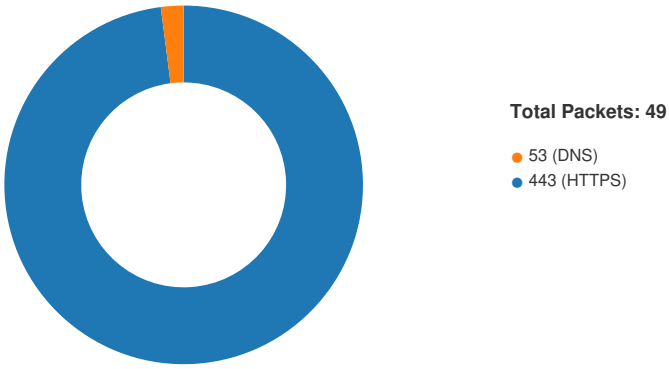
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20171.22.30.14749842802024317 03/17/23-08:58:50.216236	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49842	80	192.168.11.20	171.22.30.147
192.168.11.20171.22.30.14749842802025381 03/17/23-08:58:50.216236	TCP	2025381	ET TROJAN LokiBot Checkin	49842	80	192.168.11.20	171.22.30.147
192.168.11.20171.22.30.14749842802021641 03/17/23-08:58:50.216236	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49842	80	192.168.11.20	171.22.30.147
192.168.11.20171.22.30.14749842802825766 03/17/23-08:58:50.216236	TCP	2825766	ETPRO TROJAN LokiBot Checkin M2	49842	80	192.168.11.20	171.22.30.147
192.168.11.20171.22.30.14749842802024312 03/17/23-08:58:50.216236	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49842	80	192.168.11.20	171.22.30.147

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 08:58:48.597004890 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.597106934 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.597336054 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.617896080 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.617924929 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.657238007 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.657501936 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.726515055 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.726622105 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.727859974 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.728156090 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.731024981 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.772418022 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.985445976 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.985666037 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.985692024 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.985740900 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.985861063 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.985937119 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986161947 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986183882 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.986257076 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986341953 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.986458063 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986543894 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.986618042 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986665964 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.986759901 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986830950 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.986903906 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.986951113 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.987122059 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.987150908 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:48.987226009 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:48.987456083 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.099929094 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100255013 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.100286961 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100368977 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100435972 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.100577116 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.100610018 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100723982 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100778103 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.100805044 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100919962 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.100919962 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.100965023 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.100991011 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101126909 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.101172924 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101329088 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.101355076 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101459026 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.101485014 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101614952 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101630926 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.101658106 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101748943 CET	49841	443	192.168.11.20	188.114.97.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 08:58:49.101748943 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.101783037 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.101898909 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.101922035 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102080107 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.102103949 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102260113 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.102288008 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102408886 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102432013 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.102459908 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102556944 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.102605104 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.102629900 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102653980 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102792025 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.102818012 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.102973938 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.103008032 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.103034973 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.103125095 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.103169918 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.103192091 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.103395939 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.216362953 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.216634989 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.216645956 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.216674089 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.216805935 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.216805935 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.216847897 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.217000008 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.217021942 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.217061043 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.217171907 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.217191935 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.217246056 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.217272043 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.217370987 CET	49841	443	192.168.11.20	188.114.97.3
Mar 17, 2023 08:58:49.217392921 CET	443	49841	188.114.97.3	192.168.11.20
Mar 17, 2023 08:58:49.217451096 CET	49841	443	192.168.11.20	188.114.97.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 17, 2023 08:58:48.561542988 CET	54874	53	192.168.11.20	1.1.1.1
Mar 17, 2023 08:58:48.591098070 CET	53	54874	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 17, 2023 08:58:48.561542988 CET	192.168.11.20	1.1.1.1	0xdc9e	Standard query (0)	zed-unusual-activity-com.velda effertz.ml	A (IP address)	IN (0x0001)	false

DNS Answers

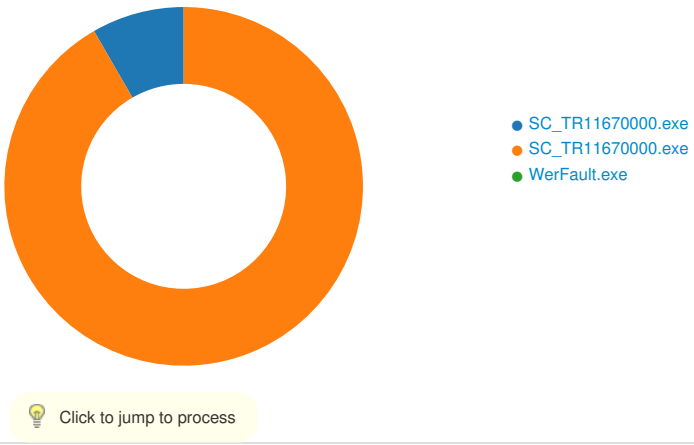
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 17, 2023 08:58:48.591098070 CET	1.1.1.1	192.168.11.20	0xdc9e	No error (0)	zed-unusual-activity-com.velda effertz.ml		188.114.97.3	A (IP address)	IN (0x0001)	false
Mar 17, 2023 08:58:48.591098070 CET	1.1.1.1	192.168.11.20	0xdc9e	No error (0)	zed-unusual-activity-com.velda effertz.ml		188.114.96.3	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- zed-unusual-activity-com.veldaeffertz.ml
- 171.22.30.147

Statistics

Behavior



System Behavior

Analysis Process: SC_TR11670000.exe PID: **2852**, Parent PID: **4664**

General	
Target ID:	1
Start time:	08:57:13
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\SC_TR11670000.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC_TR11670000.exe
Imagebase:	0x400000
File size:	329416 bytes
MD5 hash:	778F9F61191BF812A829EDFB93F5B442
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000001.00000003.23294314112.00000000028DD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000001.00000002.24272353899.0000000003330000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.24272353899.0000000003E2A000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: SC_TR11670000.exe PID: **6728**, Parent PID: **2852**

General

Target ID:	4
Start time:	08:58:32
Start date:	17/03/2023
Path:	C:\Users\user\Desktop\SC_TR11670000.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC_TR11670000.exe
Imagebase:	0x400000
File size:	329416 bytes
MD5 hash:	778F9F61191BF812A829EDFB93F5B442
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000004.00000002.24273911659.0000000001660000.00000040.00000400.00020000.00000000.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	2496253	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2496253	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2496253	InternetOpenUrlA
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	2496253	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2496253	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2496253	InternetOpenUrlA
C:\Users\user\AppData\Roaming\5D4ACB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5D4ACB\B73EF6.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	3920	success or wait	1	40415C	ReadFile

Analysis Process: WerFault.exe PID: **2396**, Parent PID: **6728**

General

Target ID:	7
Start time:	08:58:51
Start date:	17/03/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6728 -s 212
Imagebase:	0xa20000
File size:	482640 bytes
MD5 hash:	40A149513D721F096DDF50C04DA2F01F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly