ID: 800718
Sample Name: e-dekont-20230206.exe
Cookbook: default.jbs
Time: 18:40:32
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

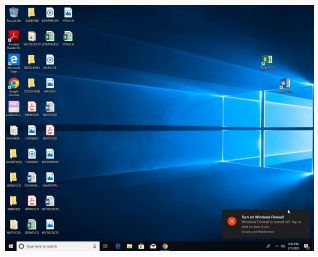
Windows Analysis Report

e-dekont-20230206.exe

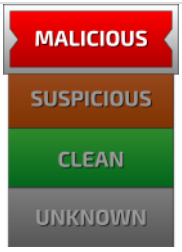
Overview

General Information

Sample Name:	e-dekont-20230206.exe
Analysis ID:	800718
MD5:	33a5f92deee38..
SHA1:	7e6daec4a2a4…
SHA256:	e3b440683630…
Tags:	exe geo TUR
Infos:	



Detection



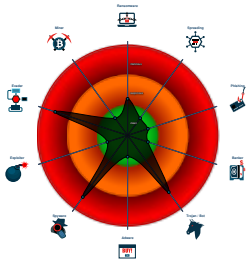
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Contains functionality to register a lo…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- May check the online IP address of…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- e-dekont-20230206.exe (PID: 5124 cmdline: C:\Users\user\Desktop\e-dekont-20230206.exe MD5: 33A5F92DEEE382035467CAFF29A8D487)
  - CasPol.exe (PID: 2256 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.558103667.00000000033DC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CasPol.exe PID: 2256	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: CasPol.exe PID: 2256	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.5 - Destination IP: 162.159.135.232

Timestamp:	192.168.2.5162.159.135.232497034432851779 02/07/23-18:41:32.301093
SID:	2851779
Source Port:	49703
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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 browser information (history, passwords, etc)

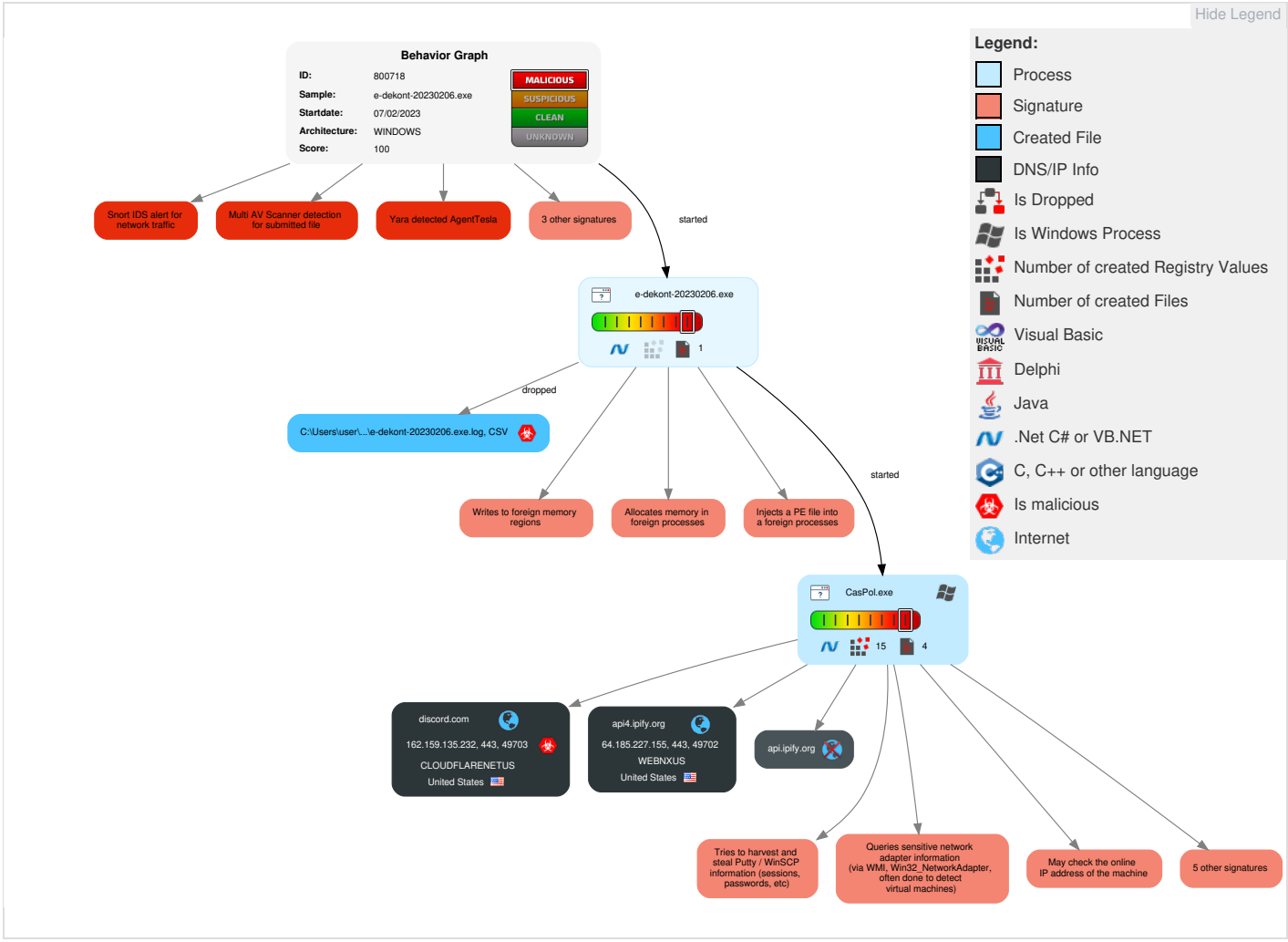
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 1 4 System Information Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 1 1 Security Software Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 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)	2 2 Software Packing	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	1 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 Remote System Discovery	SSH	1 Clipboard Data	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 Masquerading	Cached Domain Credentials	1 System Network Configuration 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 3 1 Virtualization/Sandbox Evasion	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	3 1 1 Process Injection	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

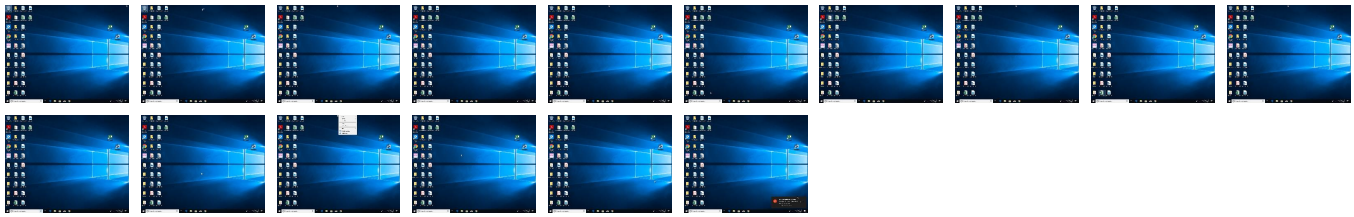
Behavior Graph



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
e-dekont-20230206.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.GenSteal	
e-dekont-20230206.exe	55%	Virustotal		Browse
e-dekont-20230206.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.CasPol.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://discord.com	0%	URL Reputation	safe	
http://discord.com	0%	URL Reputation	safe	
http://https://discord.com/api/webhooks/1063267560818233445/Ga1uL1m9HE258QH4hqiVhVH5m98lA3rsO835awvMXcR1F31nnHHfghtrbDwRtJci1Osr	0%	Avira URL Cloud	safe	
http://https://discord.com/api/webhooks/1063267560818233445/Ga1uL1m9HE258QH4hqiVhVH5m98lA3rsO835awvMXcR1F31	0%	Avira URL Cloud	safe	
http://https://discord.com4Dp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.135.232	true	true		unknown
api4.ipify.org	64.185.227.155	true	false		high
api.ipify.org	unknown	unknown	false		high

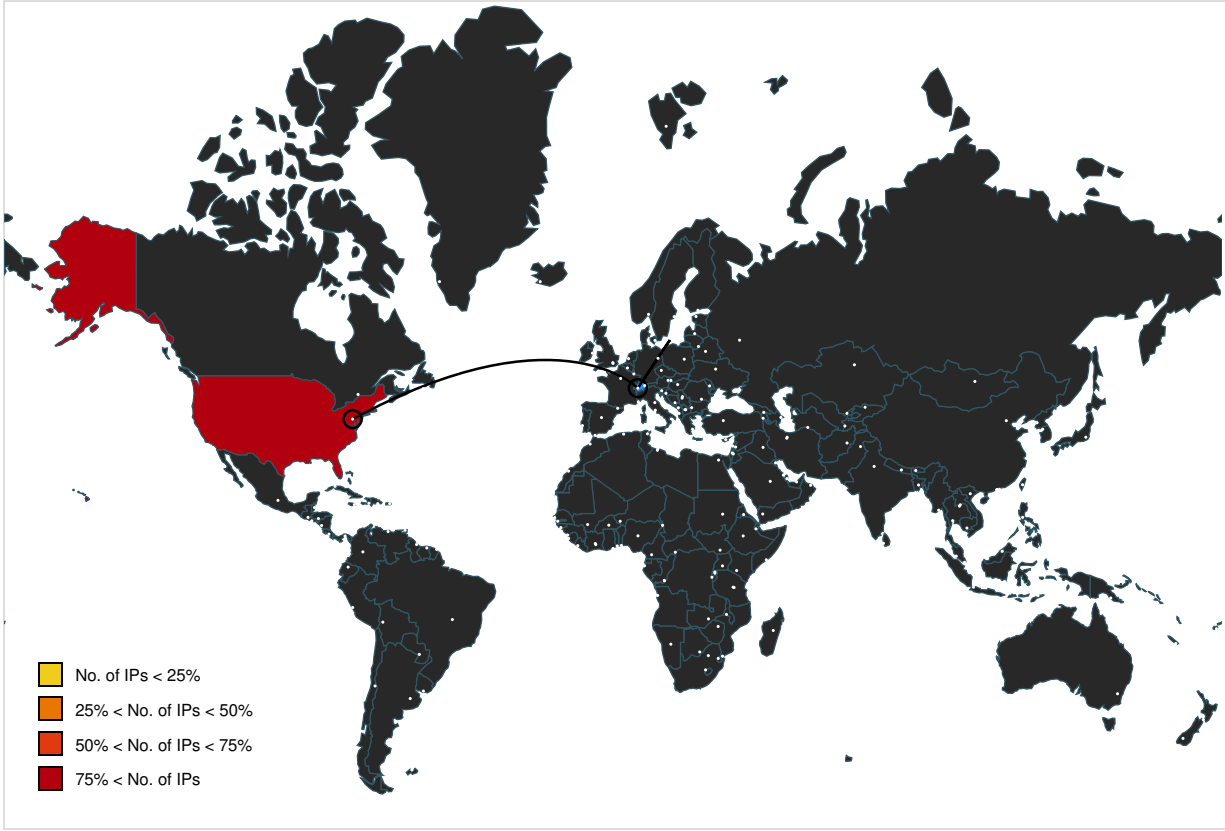
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://https://discord.com/api/webhooks/1063267560818233445/Ga1uL1m9HE258QH4hqiVhVH5m98lA3rsO835awvMXcR1F31nnHHfghtrbDwRtJci1Osr	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org	CasPol.exe, 00000001.00000002.558103667.0000000003391000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.com	CasPol.exe, 00000001.00000002.558103667.00000000033F4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://discord.com	CasPol.exe, 00000001.00000002.558103667.00000000033F4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000001.00000002.558103667.0000000003391000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://discord.com4Dp	CasPol.exe, 00000001.00000002.558103667.00000000033F4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/api/webhooks/1063267560818233445/Ga1uL1m9HE258QH4hqiVhVH5m98lA3rsO835awvMXcR1F31	CasPol.exe, 00000001.00000002.558103667.0000000003391000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.185.227.155	api4.ipify.org	United States		18450	WEBNXUS	false
162.159.135.232	discord.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800718
Start date and time:	2023-02-07 18:40:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 54s
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:	5
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:	e-dekont-20230206.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 17.5% (good quality ratio 13.2%) • Quality average: 49.2% • Quality standard deviation: 37.2%

HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:41:28	API Interceptor	994x Sleep call for process: CasPol.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\e-dekont-20230206.exe.log

Process:	C:\Users\user\Desktop\e-dekont-20230206.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZilv:Q3La/KDLI4MWuPTxAlv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D

SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	**true**
Reputation:	high, very likely benign file
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..

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.959804344180061
TrID:	• Win64 Executable GUI Net Framework (217006/5) 47.53% • Win64 Executable GUI (202006/5) 44.25% • Win64 Executable (generic) Net Framework (21505/4) 4.71% • Win64 Executable (generic) (12005/4) 2.63% • Generic Win/DOS Executable (2004/3) 0.44%
File name:	e-dekont-20230206.exe
File size:	695808
MD5:	33a5f92deee382035467caff29a8d487
SHA1:	7e6daec4a2a4dde0f5148df4165fa8cebb7011e4
SHA256:	e3b4406836308220da7989e5d539486ee1b71b4cc25a822e056993ab44675666
SHA512:	c2c3a2ffc2719245166a561050a0c4d9ece584dea47997bb5db1cc30885e31e2a5af3cfbb27526835b10bdda71b572c307e8704a1ac53e9119cfe63c760f66af
SSDEEP:	12288:vjsouJ3dUctF0KHbYXj/oNmsNjMQWwBTMYvwgScpK3J+ZBJwsscBDZn0Vx1NdB:2NUc7TbEDoNtQQWwKYvJScg63scDnu
TLSH:	46E422177ACF0214D49829B282EF076503E95B85A1B7DABD3F4573AD06723E6BE43702
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....z... ....@..... .....` .....

File Icon

Icon Hash:	92aca8b2b2a2b286

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xEC8B859F [Tue Oct 4 11:38:07 2095 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

Instruction
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	0xac000	0x1b8c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa98da	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	0x2008	0x48	.text

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa7974	0xa7a00	False	0.9695758179530202	data	7.97077131969678	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.sdata	0xaa000	0x1e8	0x200	False	0.86328125	data	6.5950997415198165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xac000	0x1b8c	0x1c00	False	0.34444754464285715	data	5.438495976746426	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

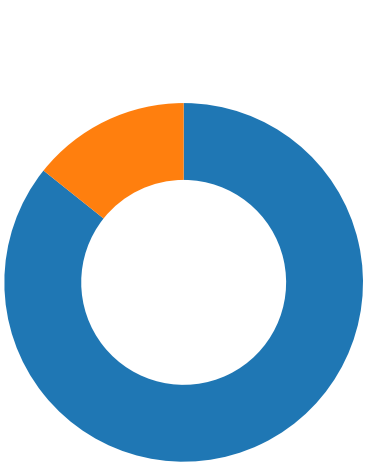
Name	RVA	Size	Type	Language	Country
RT_ICON	0xac160	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0xad208	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0xad670	0x22	data		
RT_VERSION	0xad694	0x30c	data		
RT_MANIFEST	0xad9a0	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5162.159.135.232497034432851779 02/07/23-18:41:32.301093	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49703	443	192.168.2.5	162.159.135.232

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:27.266633987 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:27.266757011 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:27.266869068 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:27.355532885 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:27.355787039 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:27.679862976 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:27.680044889 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:27.696712971 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:27.696759939 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:27.697472095 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:27.746340990 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:28.034023046 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:28.034092903 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:28.132925987 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:28.133024931 CET	443	49702	64.185.227.155	192.168.2.5
Feb 7, 2023 18:41:28.133107901 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:28.134315968 CET	49702	443	192.168.2.5	64.185.227.155
Feb 7, 2023 18:41:32.177478075 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.177515984 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.177587032 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.178462982 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.178472042 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.237952948 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.238046885 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.240590096 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.240601063 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.241060019 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.243566990 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.243582010 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.300604105 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.300971985 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.300987959 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.434633017 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.434804916 CET	443	49703	162.159.135.232	192.168.2.5
Feb 7, 2023 18:41:32.434914112 CET	49703	443	192.168.2.5	162.159.135.232
Feb 7, 2023 18:41:32.509637117 CET	49703	443	192.168.2.5	162.159.135.232

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:27.189271927 CET	60649	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:41:27.209341049 CET	53	60649	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:41:27.222088099 CET	51441	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:41:27.244609118 CET	53	51441	8.8.8.8	192.168.2.5
Feb 7, 2023 18:41:32.139256954 CET	49177	53	192.168.2.5	8.8.8.8
Feb 7, 2023 18:41:32.159280062 CET	53	49177	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:41:27.189271927 CET	192.168.2.5	8.8.8.8	0x302e	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:27.222088099 CET	192.168.2.5	8.8.8.8	0x612d	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:32.139256954 CET	192.168.2.5	8.8.8.8	0x8350	Standard query (0)	discord.com	A (IP address)	IN (0x0001)	false

DNS Answers

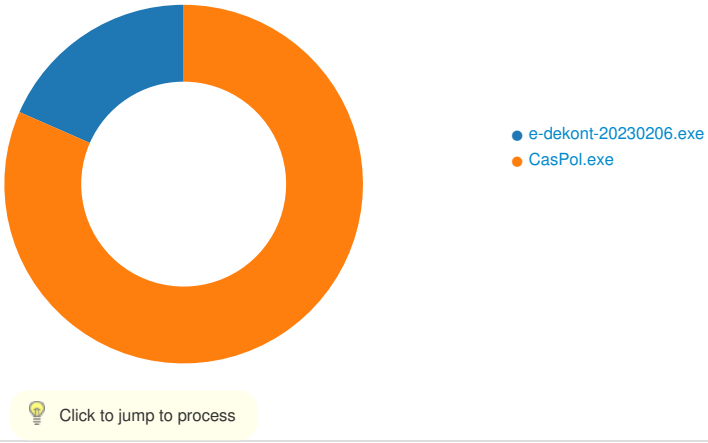
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:41:27.209341049 CET	8.8.8.8	192.168.2.5	0x302e	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:41:27.209341049 CET	8.8.8.8	192.168.2.5	0x302e	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:27.209341049 CET	8.8.8.8	192.168.2.5	0x302e	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:27.209341049 CET	8.8.8.8	192.168.2.5	0x302e	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:27.244609118 CET	8.8.8.8	192.168.2.5	0x612d	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:41:27.244609118 CET	8.8.8.8	192.168.2.5	0x612d	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:27.244609118 CET	8.8.8.8	192.168.2.5	0x612d	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:27.244609118 CET	8.8.8.8	192.168.2.5	0x612d	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:32.159280062 CET	8.8.8.8	192.168.2.5	0x8350	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:32.159280062 CET	8.8.8.8	192.168.2.5	0x8350	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:32.159280062 CET	8.8.8.8	192.168.2.5	0x8350	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:32.159280062 CET	8.8.8.8	192.168.2.5	0x8350	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:41:32.159280062 CET	8.8.8.8	192.168.2.5	0x8350	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- discord.com

Statistics

Behavior



System Behavior

Analysis Process: e-dekont-20230206.exe PID: 5124, Parent PID: 3324

General

Target ID:	0
Start time:	18:41:24
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\e-dekont-20230206.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\e-dekont-20230206.exe
Imagebase:	0x22e8d880000
File size:	695808 bytes
MD5 hash:	33A5F92DEEE382035467CAFF29A8D487
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\e-dekont-20230206.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA059B86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\e-dekont-20230206.exe.log	0	226	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	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",0	success or wait	1	7FFA059B8769	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	7FFA0541B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA0541B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA054F12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA05422625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA054F12E7	ReadFile

Analysis Process: CasPol.exe PID: **2256**, Parent PID: **5124**

General

Target ID:	1
Start time:	18:41:25
Start date:	07/02/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Caspol.exe
Imagebase:	0xc80000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.558103667.00000000033DC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7222CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	71071B4F	ReadFile

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

Disassembly

No disassembly