ID: 830834
Sample Name: widnOAntje.exe
Cookbook: default.jbs
Time: 18:24:13
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

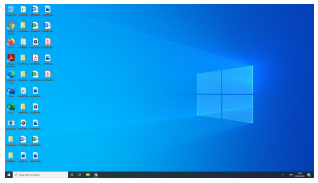
Windows Analysis Report

widnOAntje.exe

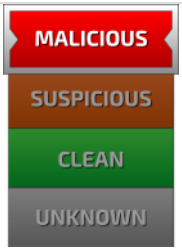
Overview

General Information

Sample Name:	widnOAntje.exe
Analysis ID:	830834
MD5:	4d5ea75ef0273..
SHA1:	cdd8e983ba55…
SHA256:	0b3b2b8094ce…
Infos:	



Detection



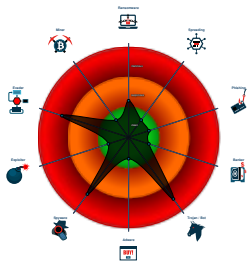
AgentTesla

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Uses the Telegram API (likely for C…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- widnOAntje.exe (PID: 5392 cmdline: C:\Users\user\Desktop\widnOAntje.exe MD5: 4D5EA75EF0273DF2B1E2463DD7472CF1)
  - widnOAntje.exe (PID: 4812 cmdline: C:\Users\user\Desktop\widnOAntje.exe MD5: 4D5EA75EF0273DF2B1E2463DD7472CF1)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot5494052141:AAF2aO4sQ_tu4BOnk0pmxB995km7Mslduy0/sendMessage?chat_id=1745136123"
}
```

Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot5494052141:AAF2aO4sQ_tu4BOnk0pmxB995km7Mslduy0/sendMessage"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.25227665436.0000000003411000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.25227665436.0000000003411000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000002.25227665436.0000000003411000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
Process Memory Space: widnOAntje.exe PID: 4812	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: widnOAntje.exe PID: 4812	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Uses the Telegram API (likely for C&C communication)

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information

- Yara detected Telegram RAT
- 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)

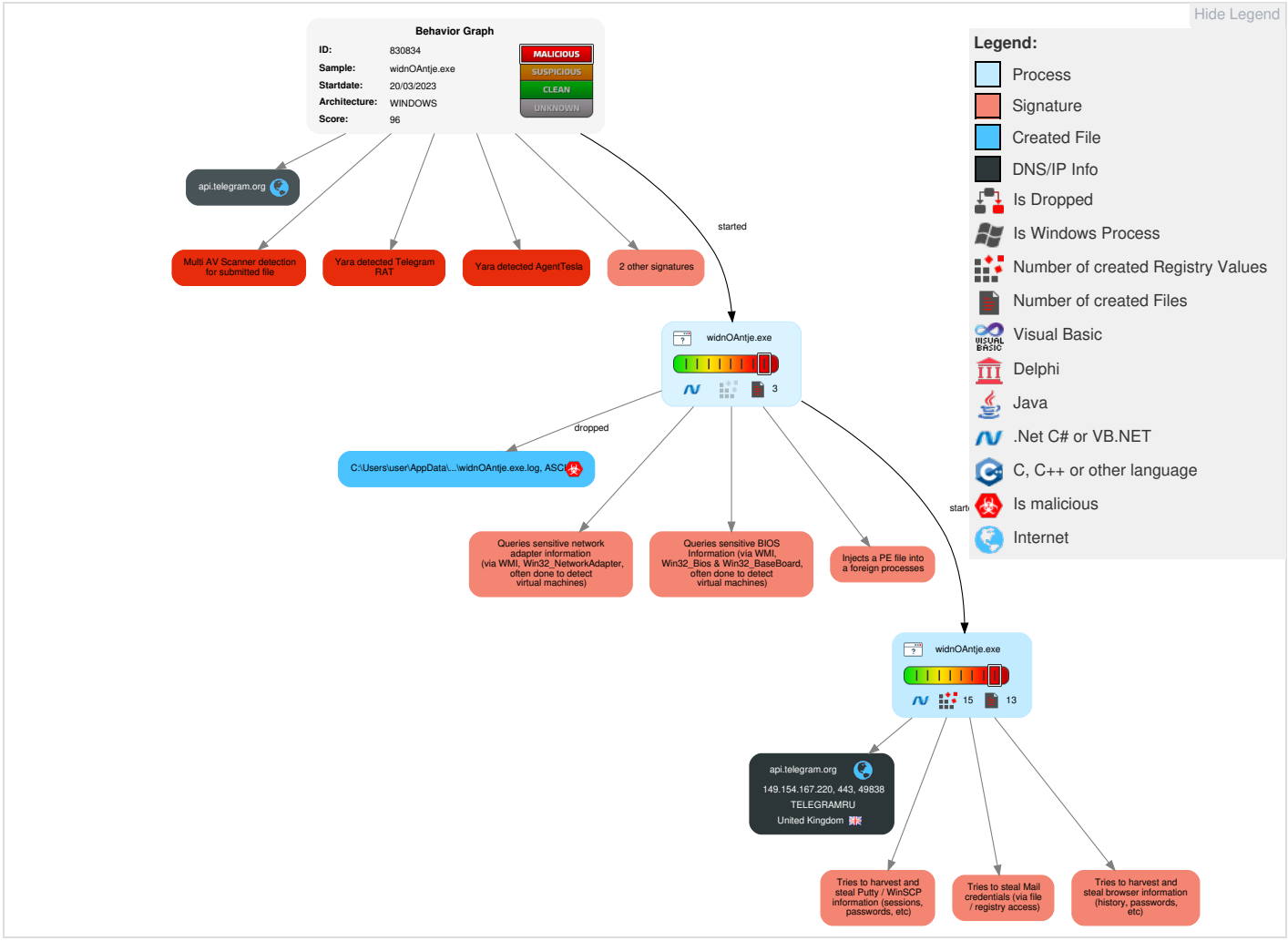
Remote Access Functionality

- Yara detected Telegram RAT
- 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	1 DLL Side-Loading	1 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	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)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	2 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 1 Process Injection	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 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	1 1 4 System Information 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	2 Software Packing	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
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	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
widnOAntje.exe	53%	Virustotal		Browse
widnOAntje.exe	33%	ReversingLabs	Win32.Trojan.Pwsx	
widnOAntje.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://krdict.korean.go.kr/api/search?key=AEBB6D3290D88C645CF1452F7DA3229D0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

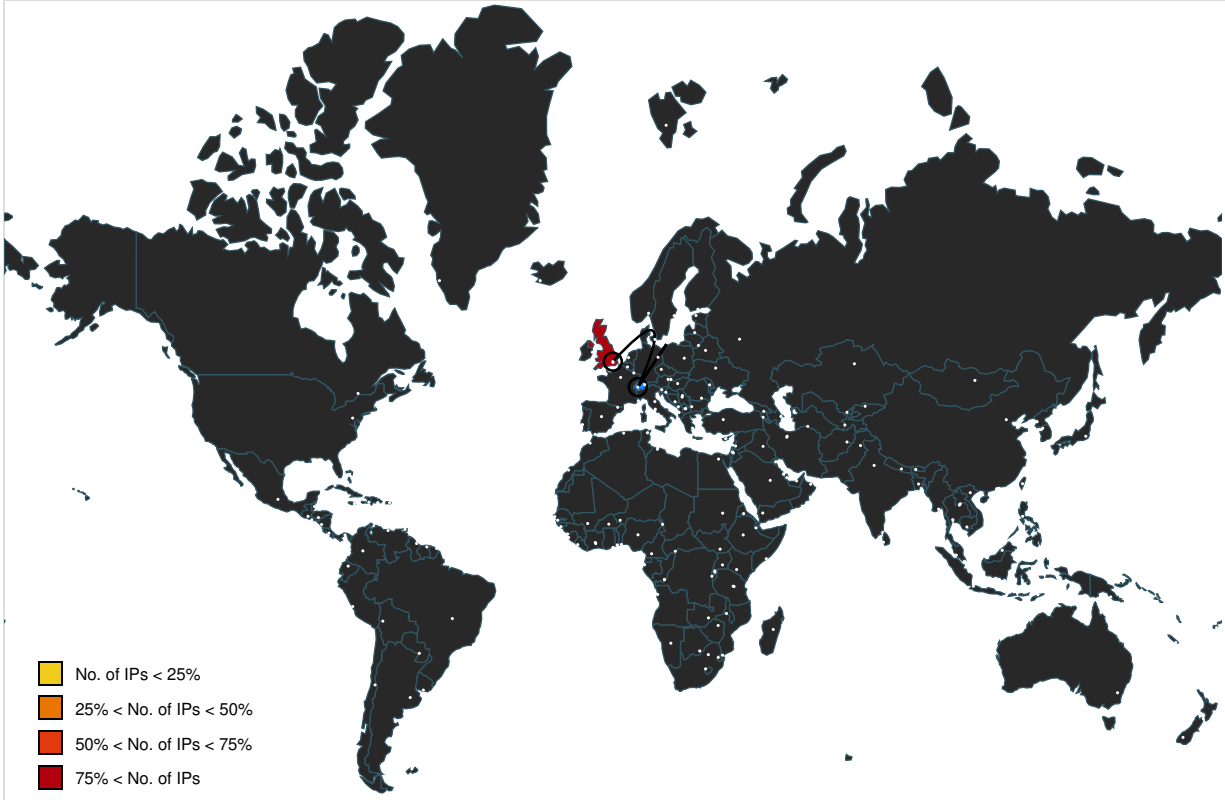
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5494052141:AAF2aO4sQ_tu4BOnk0pmxB995km7Mslduy0/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://picsum.photos/80	widnOAntje.exe	false		high
http://https://krdict.korean.go.kr/api/search?key=AEBB6D3290D88C645CF1452F7DA3229D0	widnOAntje.exe	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot5494052141:AAF2aO4sQ_tu4BOnk0pmxB995km7Mslduy0/	widnOAntje.exe, 00000005.00000002.252276 65436.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://api.telegram.org	widnOAntje.exe, 00000005.00000002.252276 65436.0000000003490000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://api.telegram.org	widnOAntje.exe, 00000005.00000002.252276 65436.00000000034B3000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	widnOAntje.exe, 00000005.00000002.252276 65436.0000000003490000.00000004.00000800 .00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830834
Start date and time:	2023-03-20 18:24:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
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:	widnOAntje.exe
Detection:	MAL
Classification:	mal96.troj.spyw.evad.winEXE@3/4@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, wdcp.microsoft.com
- 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

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\Microsoft\CLR_v4.0_32\UsageLogs\widnOAntje.exe.log

Process:	C:\Users\user\Desktop\widnOAntje.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.3584340594103494
Encrypted:	false
SSDEEP:	24:MLUE4K5E4KGN1qE4qXKDE4KhKzKhPKIE4oKXKoZAE4Kz9fhfE4x84j:MlHK5HKGN1qHiYHKhSoPtHokhAHKzTfp
MD5:	52D666938F0111F0BFD0456A12623437
SHA1:	0E88A434C23CAD5BC0EF4C11E8E263C824E0530D
SHA-256:	7C207D29E8EFC73141C4BDD33C763C4CD0286BD8C63E814E7FDEC8C4129B7E51
SHA-512:	E05AA6A4237D2D69F07DF60BCE2E16B1B1C030D76A966C3B3DF6C6C5754AAD7C5AD2FCD71E0BE5F2320805FC517429555943F2D004AD8EA3AA417E587AAD7C6
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490

C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\widnOAntje.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000, file counter 36, database pages 24, 1st free page 14, free pages 11, cookie 0x5, schema 4, UTF-8, version-valid-for 36
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	2.9216957692876595
Encrypted:	false
SSDEEP:	384:ST8XNcKu0iTwbAziYN570RMZXVuKnQM2V6ofbDO4xmTgZcZygSA2O9RVHfwrhhxV:JNcgiD5Q6luKQM2V7DXcAgSA2KD4jL
MD5:	1A706D20E96086886B5D00D9698E09DF
SHA1:	DACF81D90647457585345BEDD6DE222E83FDE01F
SHA-256:	759F62B61AA65D6D5FAC95086B26D1D053CE1FB24A8A0537ACB42DDF45D2F19F
SHA-512:	CFF7D42AA3B089759C5ACE934A098009D1A58111FE7D99AC7669B7F0A1C973907FD16A4DC1F37B5BE5252EC51B8D876511F4F6317583FA9CC48897B1B913C7F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ ...$.....$..S`.....g.....[.[.[.....

C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default\Cookies

Process:	C:\Users\user\Desktop\widnOAntje.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, file counter 7, database pages 5, cookie 0x4, schema 4, UTF-8, version-valid-for 7

Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.3172897780113213
Encrypted:	false
SSDEEP:	96:oNwCz2C+NR73QOaq9kozeav2RT3VnnnekEEN9ORelnasL:ouZC+NJLaqe0LUTpnn1DN9ORONj
MD5:	D5ECE7413F423743B368D55921D78C0A
SHA1:	3F1E854E373FB2F9BFD868AF38AF5C6B3CD2A71D
SHA-256:	D38D8A693CD4B718EA9E4995939262749893878EE9A0931BEB0F33781979FD77
SHA-512:	F54CAB99D2795DF2D01E54D1E1184D116A56E8053140BAF868ADBFC7EE35EFBC59F83E3FF26C84E0D6D1A118BB79CAB82527F1502D328483953A0A58BEED8E0B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....O}.....g....8..... ....

C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite

Process:	C:\Users\user\Desktop\widnOAntje.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3036000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08231524779339361
Encrypted:	false
SSDEEP:	12:DQANJfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQANJff32mNVpP965Ra8KN0MG/lO
MD5:	886A5F9308577FDF19279AA582D0024D
SHA1:	CDCCC11837CDDB657EB0EF6A01202451ECDF4992
SHA-256:	BA7EB45B7E9B6990BC63BE63836B74FA2CCB64DCD0C199056B6AE37B1AE735F2
SHA-512:	FF0692E52368708B36C161A4BFA91EE01CCA1B86F66666F7FC4979C6792D598FF7720A9FAF258F61439DAD61DB55C50D992E99769B1E4D321EC5B98230684BC5
Malicious:	false
Preview:	SQLite format 3.....@ .....S`.....}..}..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.604490455328884
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	widnOAntje.exe
File size:	950784
MD5:	4d5ea75ef0273df2b1e2463dd7472cf1
SHA1:	cdd8e983ba556f08faf43b29dcdc134658c39b55
SHA256:	0b3b2b8094ce254dcd224e91a84b116e806b8cc7fc895fed43cf9ea350743338
SHA512:	48a50cdd055dc5ab9e9774b72c76f630eb6e0ce4090da9a1d5b7cbdf0f9397d69101affc5f14a76ad66435f0f6b65922196a21bc2996ff9081b85a28b16db20b
SSDEEP:	12288:zbfcmhVDQlRn34LAkkgnlST9R/zUp73YmEY4UKiej/d4WYqyOLKOeU+9E1ExzPr7:PF434LAkk2Yz673YGc/dxYqy4KmEu6
TLSH:	31157C8533B19473E99A057B0534A49E1D39A10BB09BF33ABA273741E20057BB77EF91
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....9.....0..x..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e9612
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xC839C00D [Fri Jun 12 22:51:57 2076 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
shr byte ptr [eax+00005500h], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe95c0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xea000	0x5ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xec000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe95a4	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe7620	0xe7800	False	0.8233613576538877	data	7.606320578559565	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xea000	0x5ac	0x600	False	0.4212239583333333	data	4.078781937836637	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xec000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xea090	0x31c	data		
RT_MANIFEST	0xea3bc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

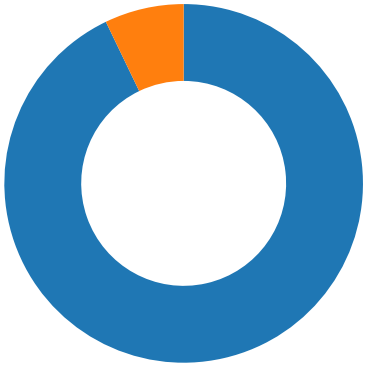
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution

Total Packets: 14

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:27:58.758272886 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.758358002 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.758622885 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.814476967 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.814510107 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.862833977 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.863112926 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.865655899 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.865681887 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.866009951 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.921283007 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.925597906 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.945740938 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.946321964 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.946414948 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.946544886 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.946795940 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.946861982 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:58.947051048 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:58.947122097 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:59.050021887 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:59.050322056 CET	443	49838	149.154.167.220	192.168.11.20
Mar 20, 2023 18:27:59.050510883 CET	49838	443	192.168.11.20	149.154.167.220
Mar 20, 2023 18:27:59.052402020 CET	49838	443	192.168.11.20	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 18:27:58.741096973 CET	57786	53	192.168.11.20	1.1.1.1
Mar 20, 2023 18:27:58.750574112 CET	53	57786	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 20, 2023 18:27:58.741096973 CET	192.168.11.20	1.1.1.1	0x8b4d	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

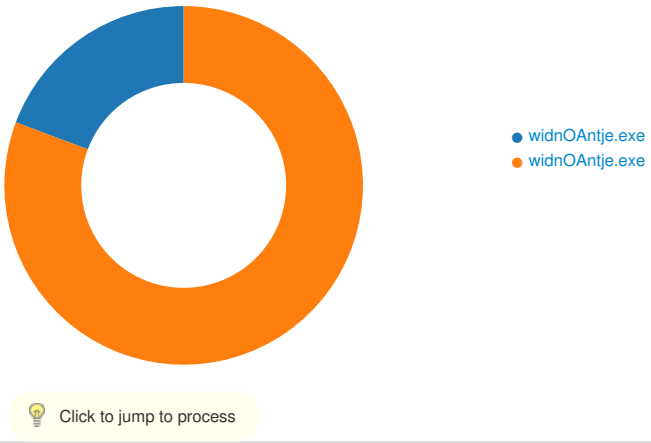
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 18:27:58.750574112 CET	1.1.1.1	192.168.11.20	0x8b4d	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.telegram.org

Statistics

Behavior



System Behavior

Analysis Process: widnOAntje.exe PID: **5392**, Parent PID: **5016**

General

Target ID:	1
Start time:	18:26:07
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\widnOAntje.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\widnOAntje.exe
Imagebase:	0x6b0000
File size:	950784 bytes
MD5 hash:	4D5EA75EF0273DF2B1E2463DD7472CF1
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

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	72CD3263	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	72CD3263	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\widnOAntje.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	730CA037	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\widnOAntje.exe.log	0	1216	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	730CA0C7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72CD099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72CD099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72C262DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72CDD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	72C262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72C262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	72C262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72C262DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72CD099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72CD099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71B69B71	ReadFile

Analysis Process: widnOAntje.exe PID: **4812**, Parent PID: **5392**

General

Target ID:	5
Start time:	18:27:46
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\widnOAntje.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\widnOAntje.exe
Imagebase:	0xe60000
File size:	950784 bytes
MD5 hash:	4D5EA75EF0273DF2B1E2463DD7472CF1
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: 00000005.00000002.25227665436.0000000003411000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.25227665436.0000000003411000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.25227665436.0000000003411000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72CD3263	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	72CD3263	unknown
C:\Users\user\AppData\Roaming\trktna5t.oee	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71B713BB	CopyFileW
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71B713BB	CopyFileW
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71B70794	CreateDirectoryW
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71B713BB	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default\Cookies	success or wait	1	71B6E04E	DeleteFileW
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default\Cookies	success or wait	1	71B6E04E	DeleteFileW
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	success or wait	1	71B6E04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default\Cookies	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 24 00 00 00 18 00 00 00 0e 00 00 00 0b 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 2e 53 60 0d 0c fd 00 04 09 fd 00 0f 67 0f fd 09 fd 0c 5b 0c 5b 0c 5b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ $$.S`g[[[	success or wait	1	71B713BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 4f 7d 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0c fd 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}g8	success or wait	1	71B713BB	CopyFileW
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 53 60 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .S`}}	success or wait	1	71B713BB	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72CD099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72CD099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72C262DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72CDD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	72C262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72C262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	72C262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72C262DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72CD099B	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72CD099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71B69B71	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	72C262DE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	25	71B69B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\06c3706b-7097-4a0b-91b3-dea437ee0d53	unknown	4096	success or wait	2	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\06c3706b-7097-4a0b-91b3-dea437ee0d53	unknown	4096	success or wait	2	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default\Cookies	unknown	16384	success or wait	6	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\trktna5t.oee\Chrome\Default\Cookies	unknown	16384	end of file	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default\Cookies	unknown	16384	success or wait	2	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\trktna5t.oee\Edge Chromium\Default\Cookies	unknown	16384	end of file	1	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	success or wait	6	71B69B71	ReadFile
C:\Users\user\AppData\Roaming\trktna5t.oee\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	end of file	1	71B69B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	success or wait	1	73DBFDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	EnableFileTracing	dword	0	success or wait	1	73DBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	73DBFDB8	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	73DBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	73DBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	73DBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	73DBFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\widnOAntje_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	73DBFDB8	unknown

Disassembly

No disassembly