ID: 552884
Sample Name: macdonzx.exe
Cookbook: default.jbs
Time: 21:23:28
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

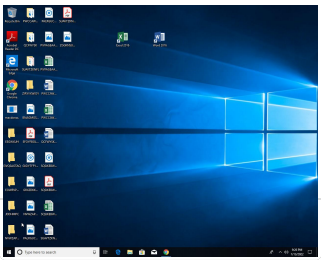
Windows Analysis Report macdonzx.exe

Overview

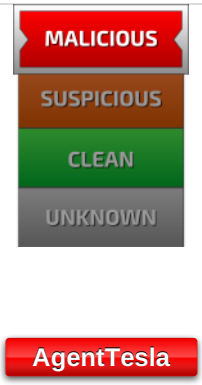
General Information

Sample Name:	macdonzx.exe
Analysis ID:	552884
MD5:	e1cdd88e54fde67.
SHA1:	facde9af9ce38ca…
SHA256:	734acbd591b35c..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

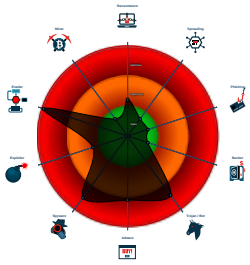


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- macdonzx.exe (PID: 5652 cmdline: "C:\Users\user\Desktop\macdonzx.exe" MD5: E1CDD88E54FDE674768D48D248CB24CE)
  - macdonzx.exe (PID: 2056 cmdline: C:\Users\user\Desktop\macdonzx.exe MD5: E1CDD88E54FDE674768D48D248CB24CE)
  - macdonzx.exe (PID: 756 cmdline: C:\Users\user\Desktop\macdonzx.exe MD5: E1CDD88E54FDE674768D48D248CB24CE)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "macdonlog@milax.tk",
  "Password": "7213575aceACE@#$",
  "Host": "milax.tk"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000000.322102466.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000000.322102466.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000D.00000002.551245127.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.551245127.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000D.00000000.321599749.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.macdonzx.exe.36f3980.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.macdonzx.exe.36f3980.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.macdonzx.exe.26bf800.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
13.0.macdonzx.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.0.macdonzx.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

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:

Yara detected AntiVM3

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

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:

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

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 ftp login credentials

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

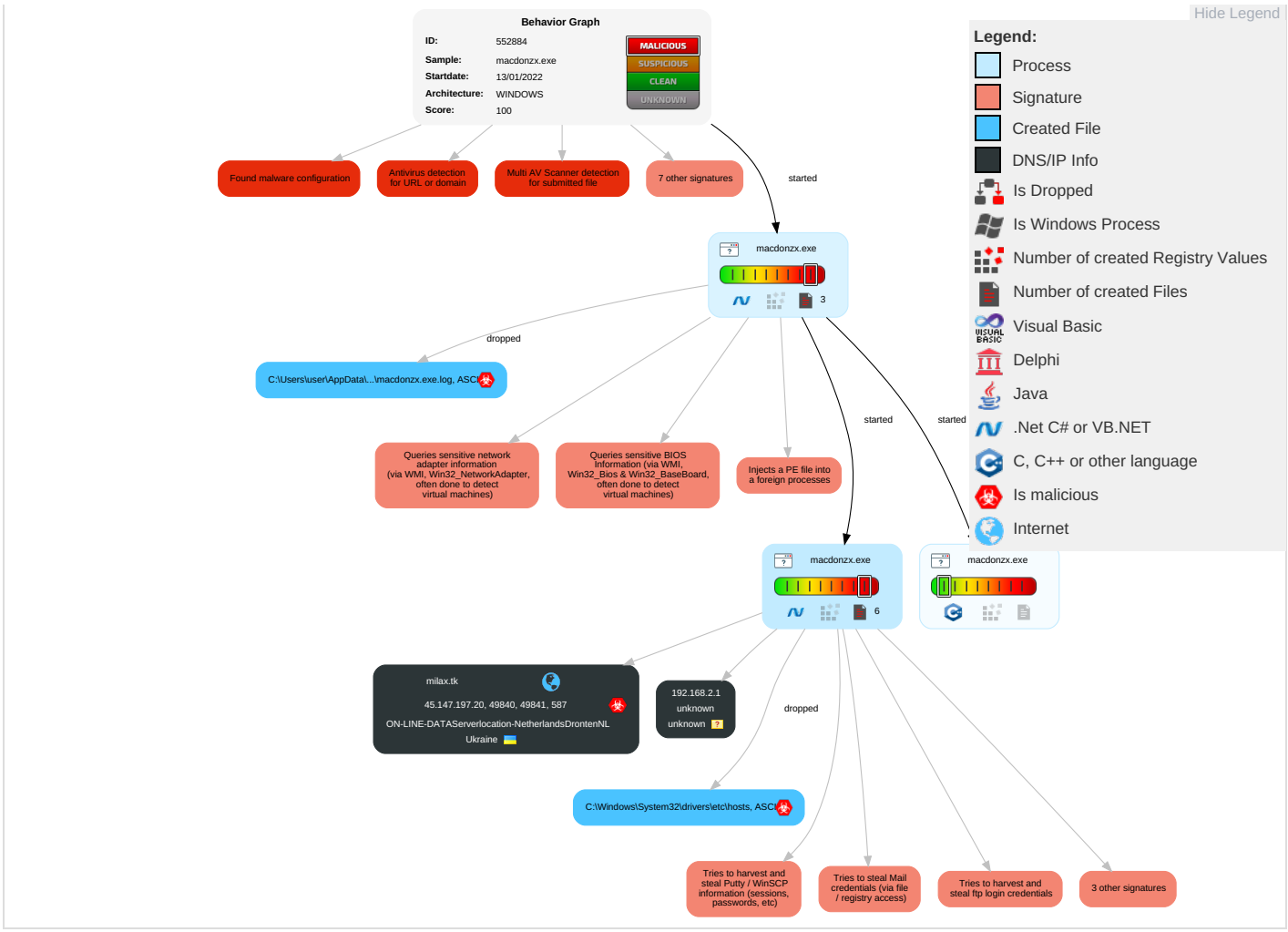
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File and Directory Permissions Modification 1	Input Capture 1 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Applicatio Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 3 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Applicatio Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Prot

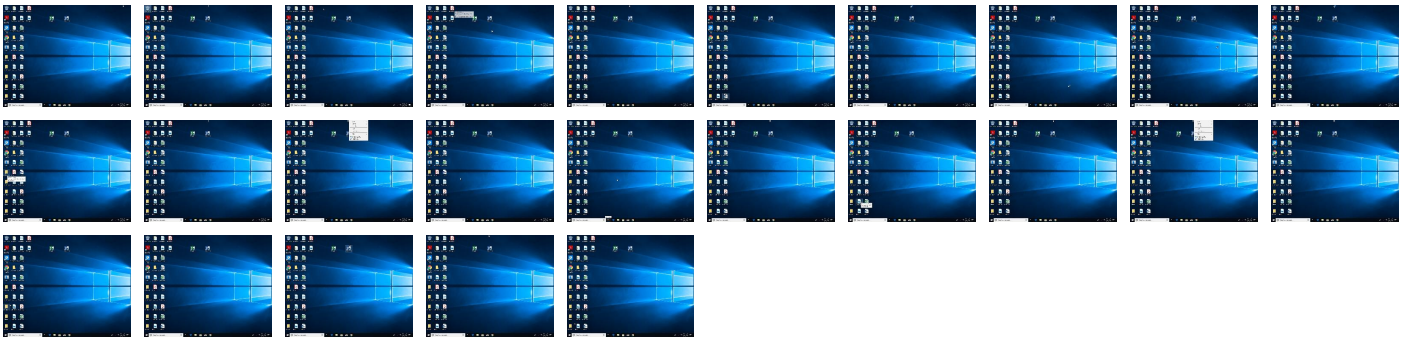
Behavior Graph



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
macdonzx.exe	45%	Virustotal		Browse
macdonzx.exe	46%	ReversingLabs	Win32.Trojan.Bulz	
macdonzx.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.macdonzx.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.macdonzx.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.macdonzx.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.macdonzx.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.0.macdonzx.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
13.2.macdonzx.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
milax.tk	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cnue	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comas	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a-e	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/soft	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr.TTF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comF	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnn-uA	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.carterandcone.comue	0%	URL Reputation	safe	
http://www.goodfont.co.krQ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/Q	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.typography.netZ.TTFi	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/&	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://Xd7k9rd8DlSNF.org	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.fontbureau.comI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Z	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.typography.nete	0%	Avira URL Cloud	safe	
http://www.carterandcone.comZ	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsof	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.W	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/I	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.tiro.compt-p	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnl	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cntan-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://milax.tk	100%	Avira URL Cloud	malware	
http://ajXUgt.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/g	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/s-cu	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
milax.tk	45.147.197.20	true	true	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.147.197.20	milax.tk	Ukraine		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552884
Start date:	13.01.2022
Start time:	21:23:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	macdonzx.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
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
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@5/3@2/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 6.8% (good quality ratio 2.8%) • Quality average: 23.9% • Quality standard deviation: 34.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:24:34	API Interceptor	660x Sleep call for process: macdonzx.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\macdonzx.exe.log

Process:	C:\Users\user\Desktop\macdonzx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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\f1d8480152e0da9a60ad49c6d16a3b6d\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\8d67d92724ba494b6c7fd089d6f25b48\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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\0e3dvfqb.hnn\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\macdonzx.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\macdonzx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.782856510786613
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	macdonzx.exe
File size:	474624
MD5:	e1cdd88e54fde674768d48d248cb24ce
SHA1:	facde9af9ce38ca5c0c30f343dfa525a9931a57d
SHA256:	734acbd591b35c3ab42e36ed5b97712ff3d1935a756d915 8dbb1fcbaf8b5c1d6
SHA512:	155905cedfea51ee8682d2a5a733c4595bd164afd7ed52f b5b8fe2d909cd2df6d8c6cc3eb05af463d49bbe0da49572 2002bc7e5f552487bf617d948589b45929
SSDEEP:	12288:sK777777777777OPHfTjKqhQQRvS7+mFNE:sK 777777777777OPSqhQE6/

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....~.a.....0..4.....~S... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47537e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E07E06 [Thu Jan 13 19:31:18 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x73384	0x73400	False	0.897081751627	data	7.79486516147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x5e4	0x600	False	0.4296875	data	4.16698632714	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x78000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 21:26:21.000920057 CET	192.168.2.3	8.8.8.8	0x5fd4	Standard query (0)	milax.tk	A (IP address)	IN (0x0001)
Jan 13, 2022 21:26:23.028445959 CET	192.168.2.3	8.8.8.8	0x317b	Standard query (0)	milax.tk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 21:26:21.035761118 CET	8.8.8.8	192.168.2.3	0x5fd4	No error (0)	milax.tk		45.147.197.20	A (IP address)	IN (0x0001)
Jan 13, 2022 21:26:23.062062025 CET	8.8.8.8	192.168.2.3	0x317b	No error (0)	milax.tk		45.147.197.20	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2022 21:26:21.254138947 CET	587	49840	45.147.197.20	192.168.2.3	220 s20.server-panel.net ESMTP Exim 4.92.2 Thu, 13 Jan 2022 22:26:21 +0200
Jan 13, 2022 21:26:21.254787922 CET	49840	587	192.168.2.3	45.147.197.20	EHLO 210979
Jan 13, 2022 21:26:21.281109095 CET	587	49840	45.147.197.20	192.168.2.3	250-s20.server-panel.net Hello 210979 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN CRAM-MD5 250-CHUNKING 250-STARTTLS 250 HELP
Jan 13, 2022 21:26:21.282515049 CET	49840	587	192.168.2.3	45.147.197.20	AUTH login bWFjZG9ubG9nQG1pbGF4LnRr
Jan 13, 2022 21:26:21.308669090 CET	587	49840	45.147.197.20	192.168.2.3	334 UGFzc3dvcmQ6
Jan 13, 2022 21:26:21.335298061 CET	587	49840	45.147.197.20	192.168.2.3	235 Authentication succeeded
Jan 13, 2022 21:26:21.337088108 CET	49840	587	192.168.2.3	45.147.197.20	MAIL FROM:<macdonlog@milax.tk>
Jan 13, 2022 21:26:21.362592936 CET	587	49840	45.147.197.20	192.168.2.3	250 OK
Jan 13, 2022 21:26:21.363178015 CET	49840	587	192.168.2.3	45.147.197.20	RCPT TO:<macdon@milax.tk>
Jan 13, 2022 21:26:21.406872988 CET	587	49840	45.147.197.20	192.168.2.3	550 Sender rate overlimit - 35.4 / 1h / macdonlog@milax.tk
Jan 13, 2022 21:26:21.436141968 CET	587	49840	45.147.197.20	192.168.2.3	421 s20.server-panel.net lost input connection
Jan 13, 2022 21:26:23.147528887 CET	587	49841	45.147.197.20	192.168.2.3	220 s20.server-panel.net ESMTP Exim 4.92.2 Thu, 13 Jan 2022 22:26:23 +0200
Jan 13, 2022 21:26:23.147855043 CET	49841	587	192.168.2.3	45.147.197.20	EHLO 210979
Jan 13, 2022 21:26:23.174637079 CET	587	49841	45.147.197.20	192.168.2.3	250-s20.server-panel.net Hello 210979 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN CRAM-MD5 250-CHUNKING 250-STARTTLS 250 HELP
Jan 13, 2022 21:26:23.174928904 CET	49841	587	192.168.2.3	45.147.197.20	AUTH login bWFjZG9ubG9nQG1pbGF4LnRr
Jan 13, 2022 21:26:23.202395916 CET	587	49841	45.147.197.20	192.168.2.3	334 UGFzc3dvcmQ6
Jan 13, 2022 21:26:23.230205059 CET	587	49841	45.147.197.20	192.168.2.3	235 Authentication succeeded
Jan 13, 2022 21:26:23.231792927 CET	49841	587	192.168.2.3	45.147.197.20	MAIL FROM:<macdonlog@milax.tk>
Jan 13, 2022 21:26:23.258584976 CET	587	49841	45.147.197.20	192.168.2.3	250 OK
Jan 13, 2022 21:26:23.258799076 CET	49841	587	192.168.2.3	45.147.197.20	RCPT TO:<macdon@milax.tk>
Jan 13, 2022 21:26:23.305896044 CET	587	49841	45.147.197.20	192.168.2.3	550 Sender rate overlimit - 36.3 / 1h / macdonlog@milax.tk
Jan 13, 2022 21:26:23.332994938 CET	587	49841	45.147.197.20	192.168.2.3	421 s20.server-panel.net lost input connection

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: macdonzx.exe PID: 5652 Parent PID: 244

General

Start time:	21:24:22
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\macdonzx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\macdonzx.exe"
Imagebase:	0x170000
File size:	474624 bytes
MD5 hash:	E1CDD88E54FDE674768D48D248CB24CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.325356794.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.325423946.00000000026DC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.325855720.0000000003699000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.325855720.0000000003699000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: macdonzx.exe PID: 2056 Parent PID: 5652

General

Start time:	21:24:35
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\macdonzx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\macdonzx.exe
Imagebase:	0x60000
File size:	474624 bytes
MD5 hash:	E1CDD88E54FDE674768D48D248CB24CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: macdonzx.exe PID: 756 Parent PID: 5652

General

Start time:	21:24:36
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\macdonzx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\macdonzx.exe
Imagebase:	0x890000
File size:	474624 bytes
MD5 hash:	E1CDD88E54FDE674768D48D248CB24CE
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: 0000000D.00000000.322102466.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.322102466.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.551245127.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000002.551245127.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.321599749.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.321599749.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.321170477.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.321170477.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.322547714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000D.00000000.322547714.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.562575155.0000000002C11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.562575155.0000000002C11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis