ID: 381541
Sample Name: Dimmock5.exe
Cookbook: default.jbs
Time: 21:26:12
Date: 03/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Dimmock5.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
Static File Info 13
General 13
File Icon 13
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 15

Sections 16
Resources 16
Imports 16
Version Infos 16
Possible Origin 16
Network Behavior 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 19
DNS Queries 20
DNS Answers 20
HTTPS Packets 20
SMTP Packets 21
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: Dimmock5.exe PID: 4708 Parent PID: 5740 22
General 22
File Activities 22
Analysis Process: RegAsm.exe PID: 5596 Parent PID: 4708 22
General 22
File Activities 22
File Created 22
File Written 23
File Read 23
Analysis Process: conhost.exe PID: 5856 Parent PID: 5596 24
General 24
Disassembly 24
Code Analysis 24

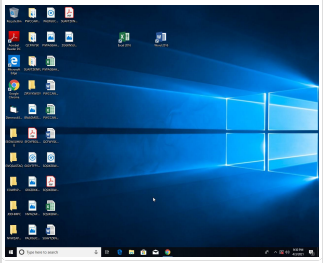
Analysis Report Dimmock5.exe

Overview

General Information

Sample Name:	Dimmock5.exe
Analysis ID:	381541
MD5:	1f6c8e6472b60d4.
SHA1:	1770766f6cfb517..
SHA256:	e0e93e3b786608..
Tags:	GuLoader
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

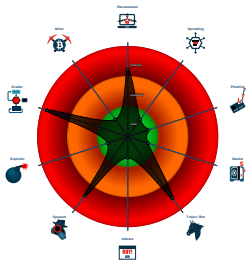
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Sigma detected: RegAsm connects …
- Yara detected AgentTesla
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Found evasive API chain (trying to d…
- Hides threads from debuggers
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- Dimmock5.exe (PID: 4708 cmdline: 'C:\Users\user\Desktop\Dimmock5.exe' MD5: 1F6C8E6472B60D49704703C99B28A4B8)
  - RegAsm.exe (PID: 5596 cmdline: 'C:\Users\user\Desktop\Dimmock5.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 5856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "kpYtlUSCkDM",
  "URL: ": "http://JgAptYOPYbQxfk.net",
  "To: ": "",
  "ByHost: ": "mail.palacioguevara.com:587",
  "Password: ": "sUUgblUr6c",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.728202576.000000000135 1000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000016.00000002.734840874.000000001E0F 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000002.734840874.000000001E0F 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

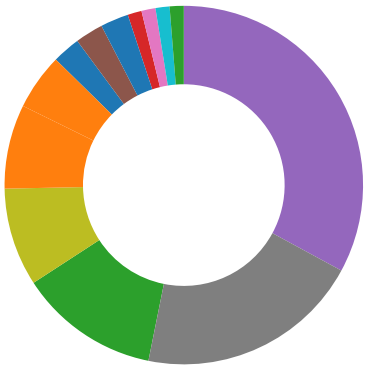
Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 5596	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 5596	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: RegAsm connects to smtp port

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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

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

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

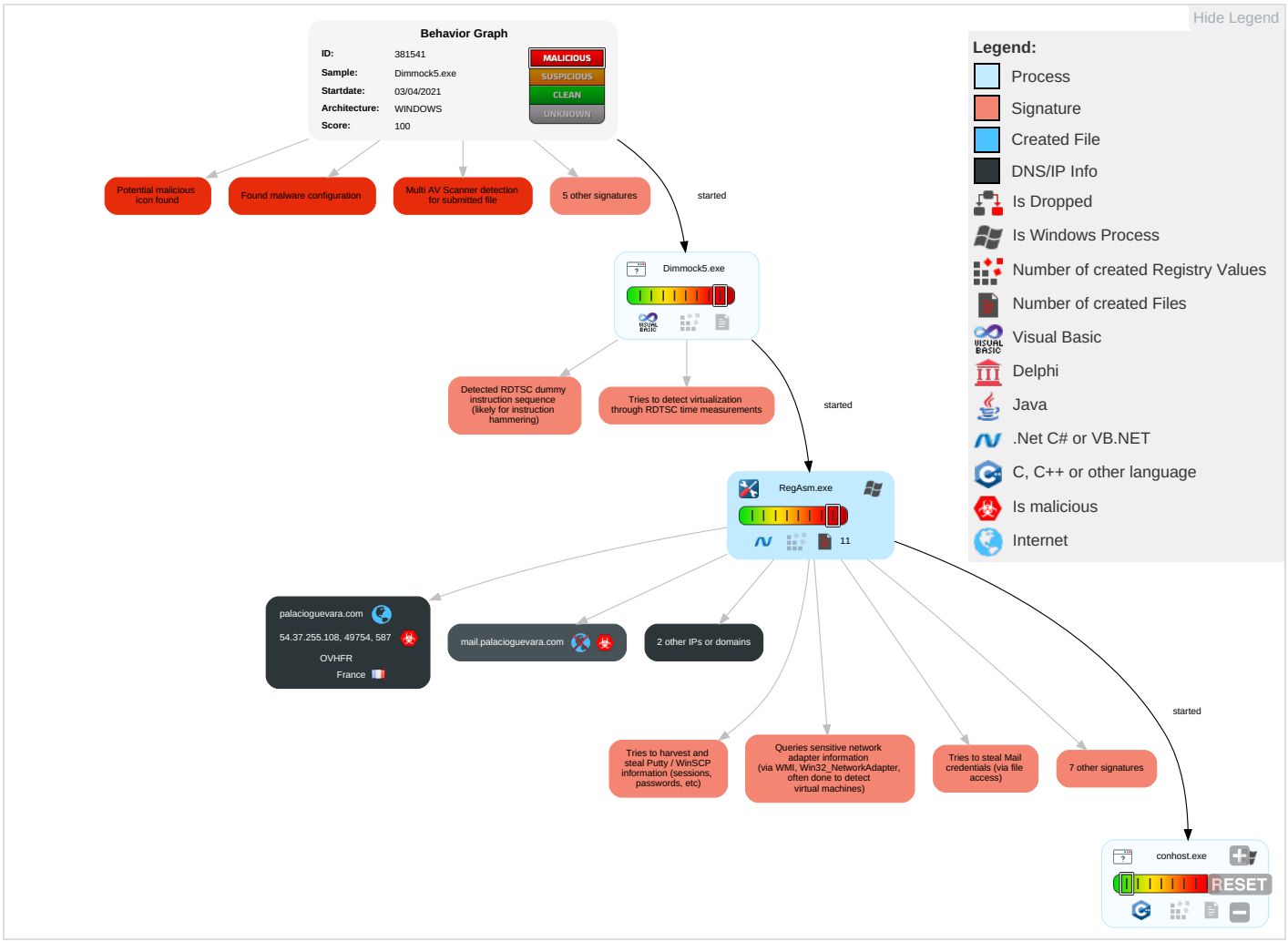
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Security Software Discovery 6 3 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 2	Virtualization/Sandbox Evasion 3 4 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Access Token Manipulation 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 3 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Ingress Tool Transfer 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Laye Protocol 1 1 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 3 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

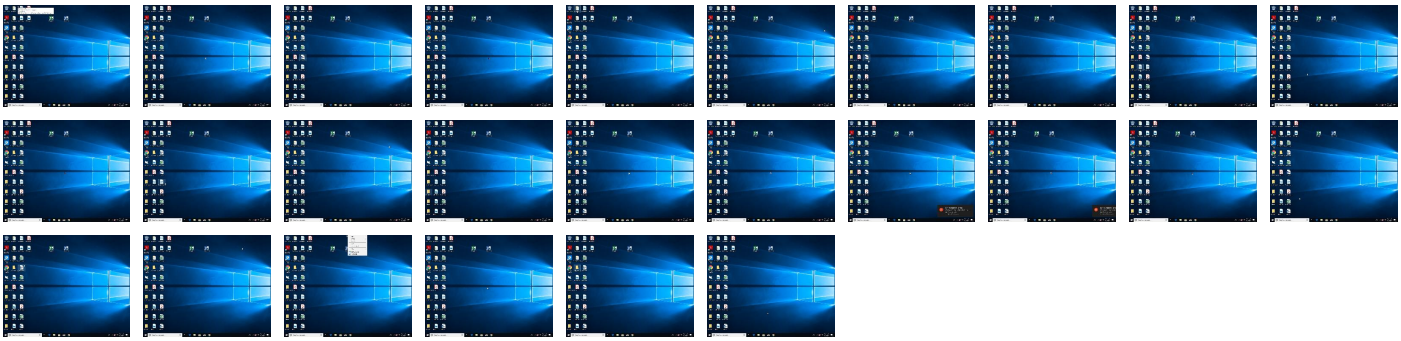
Behavior Graph



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
Dimmock5.exe	57%	Virustotal		Browse
Dimmock5.exe	27%	Metadefender		Browse
Dimmock5.exe	72%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
palacioguevara.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ENtKzK.com	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	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://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://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://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://JgAptYOPYbQxfk.net	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
palacioguevara.com	54.37.255.108	true	true	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
doc-14-04-docs.googleusercontent.com	unknown	unknown	false		high
mail.palacioguevara.com	unknown	unknown	true		unknown

Contacted URLs

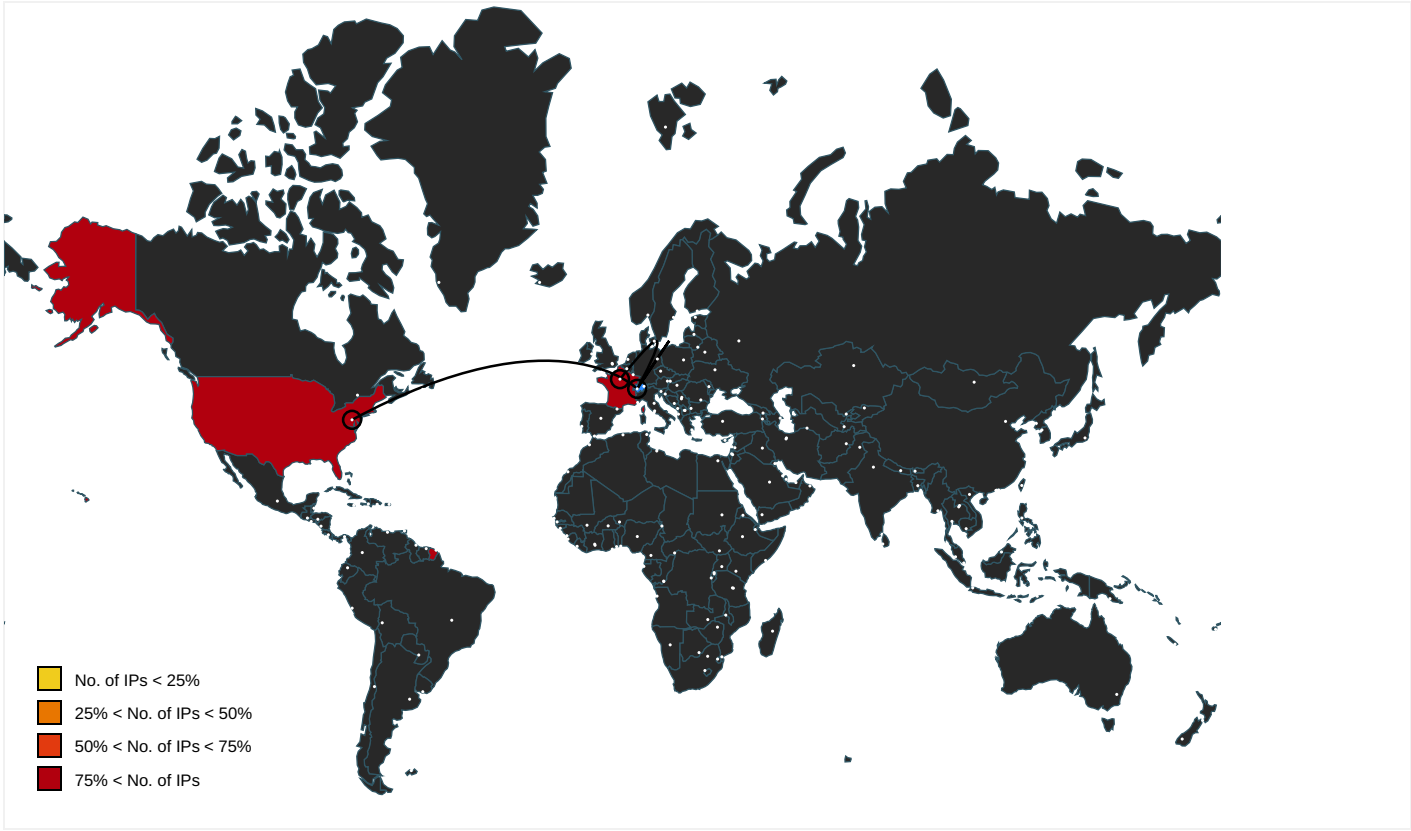
Name	Malicious	Antivirus Detection	Reputation
http://JgAptYOPYbQxfk.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000016.00000002.734840874.000000001E0F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000016.00000002.734840874.000000001E0F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 00000016.00000003.685186556.0000000001681000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ENtKzK.com	RegAsm.exe, 00000016.00000002.734840874.000000001E0F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 00000016.00000003.685186556.0000000001681000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pki.goog/repository/0	RegAsm.exe, 00000016.00000003.685186556.0000000001681000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000016.00000002.734840874.000000001E0F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 00000016.00000003.685186556.0000000001681000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.37.255.108	palacioguevara.com	France		16276	OVHFR	true
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381541
Start date:	03.04.2021
Start time:	21:26:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dimmock5.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:	32
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.rans.troj.spyw.evad.winEXE@3/1@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 67% (good quality ratio 41%) • Quality average: 41.7% • Quality standard deviation: 40%
HCA Information:	• Successful, ratio: 97% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 40.88.32.150, 93.184.220.29, 168.61.161.212, 52.255.188.83, 104.43.139.144, 104.42.151.234, 184.30.24.56, 20.190.159.131, 40.126.31.140, 40.126.31.136, 40.126.31.3, 40.126.31.7, 40.126.31.9, 40.126.31.142, 40.126.31.2, 20.82.209.183, 92.122.213.247, 92.122.213.194, 20.54.26.129, 20.82.210.154, 172.217.20.238, 52.155.217.156 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:29:05	API Interceptor	1029x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	document-1302325198.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1031166636.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-2021014062.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1568991333.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1012037614.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1307680126.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-986812161.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-550881172.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1042699213.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1455377818.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-980795635.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-340500177.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-921217151.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1500258943.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1823104059.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1434617389.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-103083228.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-1913529948.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-758557531.xls	Get hash	malicious	Browse	• 198.50.218.68
	document-707357347.xls	Get hash	malicious	Browse	• 198.50.218.68

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	pQlSDfwyYkf.js	Get hash	malicious	Browse	• 172.217.23.33
	Balance payment..exe	Get hash	malicious	Browse	• 172.217.23.33
	pQlSDfwyYkf.js	Get hash	malicious	Browse	• 172.217.23.33
	document-1641473761.xls	Get hash	malicious	Browse	• 172.217.23.33
	ObJRDAd8jZ.exe	Get hash	malicious	Browse	• 172.217.23.33
	SecuriteInfo.com.Trojan.Encoder.33750.22954.exe	Get hash	malicious	Browse	• 172.217.23.33
	yKthoYkcfg.exe	Get hash	malicious	Browse	• 172.217.23.33
	Confirmation Payment Receipt.doc	Get hash	malicious	Browse	• 172.217.23.33
	Friday, April 2nd, 2021, 20210402062906.8CE1B73ADE2A192C@compassionarmy.com.htm	Get hash	malicious	Browse	• 172.217.23.33
	documents-602438418.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	1006.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	262.xlsm	Get hash	malicious	Browse	• 172.217.23.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1193.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	1094.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	1366.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	2086.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	1430.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	581.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	3324.xlsm	Get hash	malicious	Browse	• 172.217.23.33
	871.xlsm	Get hash	malicious	Browse	• 172.217.23.33

Dropped Files

No context

Created / dropped Files

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.5051992825729466
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Dimmock5.exe
File size:	57344
MD5:	1f6c8e6472b60d49704703c99b28a4b8
SHA1:	1770766f6cfb51725e035b0f38f560bf03d73fae
SHA256:	e0e93e3b7866085b8384948d12a2eb613fc9eb0bc283fbb e12841a5dca11ba9f
SHA512:	9e7e671c36f9f7a7206e236a5932dcefdecee4781fcb105 e9c7fc458e0632383b4982cf2401e0ec7dc5eafd4619b88 8a74ac1b06983aa1d67d9493c85f55c8db
SSDEEP:	768:5hf6jt9ZzkkIH1f6W+iitWmyQJkVWy+qaEmTqtid:5d 6jtH9IHNKNWHtIt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...~ae`.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40169c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x6065617E [Thu Apr 1 06:00:30 2021 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:	b983fc96c0bd34be8388eeea33042759

Entrypoint Preview

Instruction
push 00401874h
call 00007F8844ED7FB5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dh, cl
bound edi, dword ptr [esi-74DBD20Eh]
dec ebx
sahf
mov bh, D0h
mov ah, 21h
stc
push ebp
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
call 00007F88A7F07B44h
imul esi, dword ptr [edx+63h], 6F766D75h
insb
jne 00007F8844ED8036h
add byte ptr [eax], cl
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax

Instruction
add eax, 671CB2E9h
cmpsb
xchg dword ptr [ebx], edx
dec ebx
stosd
popfd
push esi
out dx, al
push ebx
movsd
jmp 00007F87E69A3C8Eh
shl ebx, 1
inc eax
dec eax
xchg eax, esi
pop eax
push ss
jmp far 4F3Ah : 9B80EEF1h
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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 dword ptr [eax], eax
add byte ptr [eax+00h], cl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [esi+75h], cl
popad
outsb
arpl word ptr [ebp+72h], sp
jnc 00007F8844ED7FC2h
or eax, 47000901h
outsd
outsb
outsd
jc 00007F8844ED802Bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xaf14	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe000	0x9d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa528	0xb000	False	0.537863991477	data	6.38736816411	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xc000	0x11b4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe000	0x9d8	0x1000	False	0.1806640625	data	2.12896103936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe8a8	0x130	data		
RT_ICON	0xe5c0	0x2e8	data		
RT_ICON	0xe498	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xe468	0x30	data		
RT_VERSION	0xe150	0x318	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaAryMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaI2Str, __vbaFPException, __vbaStrVarVal, __vbaDateVar, _CIlog, __vbaErrorOverflow, __vbaFileOpen, __vbaVar2Vec, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarAdd, __vbaLateMemCall, __vbaInStrB, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Collutions
InternalName	Dimmock5
FileVersion	1.00
CompanyName	Collutions
LegalTrademarks	Collutions
Comments	Collutions
ProductName	Collutions
ProductVersion	1.00
FileDescription	Creepy Collutions
OriginalFilename	Dimmock5.exe

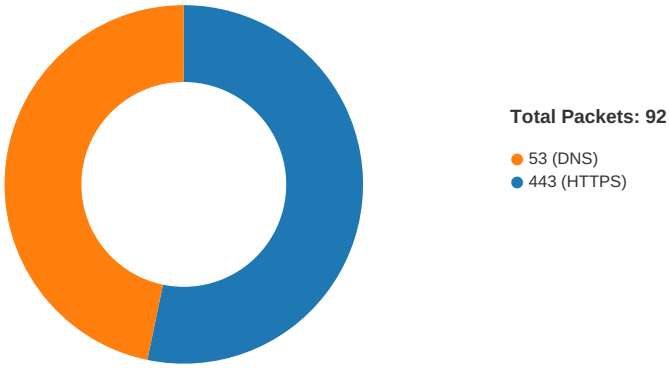
Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 3, 2021 21:28:57.063009024 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.104257107 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.104377985 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.104971886 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.148574114 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.162067890 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.162125111 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.162149906 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.162163973 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.162199974 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.162213087 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.162225008 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.162273884 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.178500891 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.219722986 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.220861912 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.221852064 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.267597914 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.623802900 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.623862982 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.623898029 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.623936892 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.623975992 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.624003887 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.624044895 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.624052048 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.624057055 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.626981974 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.627096891 CEST	49741	443	192.168.2.3	172.217.23.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 3, 2021 21:28:57.627722979 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.627768993 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.627799988 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.627825975 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.630914927 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.630968094 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.631012917 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.631051064 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.633925915 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.633970022 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.634013891 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.634205103 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.636962891 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.637058020 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.638370991 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.638412952 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.638499022 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.638520956 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.667357922 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.667468071 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.667634964 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.668855906 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.668895006 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.669025898 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.669043064 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.671967983 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.672013044 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.672055960 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.672091961 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.674973011 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.675021887 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.675065041 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.675108910 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.678006887 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.678050041 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.678093910 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.678137064 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.681075096 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.681117058 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.681170940 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.681217909 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.684149027 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.684191942 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.684227943 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.684251070 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.687216043 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.687258959 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.687311888 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.687336922 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.690288067 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.690329075 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.690386057 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.690412998 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.693048000 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.693090916 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.693126917 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.693152905 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.695774078 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.695825100 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.695856094 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.695909023 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.698532104 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.698606014 CEST	443	49741	172.217.23.33	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 3, 2021 21:28:57.698622942 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.698710918 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.701239109 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.701280117 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.701330900 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.701368093 CEST	49741	443	192.168.2.3	172.217.23.33
Apr 3, 2021 21:28:57.704010010 CEST	443	49741	172.217.23.33	192.168.2.3
Apr 3, 2021 21:28:57.704060078 CEST	443	49741	172.217.23.33	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 3, 2021 21:26:52.658694029 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:52.788124084 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:52.850121021 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:52.898739100 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:52.953587055 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:53.630685091 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:53.682168007 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:54.569523096 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:54.615592957 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:55.393383980 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:55.447717905 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:56.192456961 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:56.241266012 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:57.439815998 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:57.489022970 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:58.349874973 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:58.409580946 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 3, 2021 21:26:59.526803017 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:26:59.581473112 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:00.619247913 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:00.667506933 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:01.702913046 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:01.753806114 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:02.654890060 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:02.702331066 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:03.492252111 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:03.552632093 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:04.467761040 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:04.525242090 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:05.409342051 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:05.458154917 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:06.331608057 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:06.379941940 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:07.264858961 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:07.313739061 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:08.121592999 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:08.177475929 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:09.064527988 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:09.112958908 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:10.016024113 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:10.068330050 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:29.675410032 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:29.734827042 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:52.581410885 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:52.654979944 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:52.782737970 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:52.841981888 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 3, 2021 21:27:56.902631044 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:27:56.959047079 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 3, 2021 21:28:05.641415119 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:28:05.711725950 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 3, 2021 21:28:18.511337042 CEST	55435	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 3, 2021 21:28:18.580071926 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 3, 2021 21:28:33.490812063 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:28:33.562118053 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 3, 2021 21:28:37.936959982 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:28:37.993304968 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 3, 2021 21:28:56.176302910 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:28:56.239506006 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 3, 2021 21:28:56.981240034 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:28:57.060580015 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:10.735685110 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:10.783648968 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:12.790719032 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:12.863223076 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:46.144838095 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:46.251244068 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:46.961075068 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:47.026693106 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:47.554347038 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:47.616621971 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:48.290796041 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:48.349611998 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:49.052926064 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:49.101422071 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:49.878793955 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:49.938471079 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:50.413161993 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:50.472553015 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:51.515624046 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:51.570697069 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:52.409864902 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:52.466906071 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 3, 2021 21:29:52.909982920 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:29:52.965461969 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 3, 2021 21:30:28.843709946 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 3, 2021 21:30:28.948357105 CEST	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 3, 2021 21:28:56.981240034 CEST	192.168.2.3	8.8.8.8	0x8fa2	Standard query (0)	doc-14-04-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 3, 2021 21:30:28.843709946 CEST	192.168.2.3	8.8.8.8	0x613a	Standard query (0)	mail.palacioguevara.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 3, 2021 21:27:52.654979944 CEST	8.8.8.8	192.168.2.3	0xe744	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 3, 2021 21:28:57.060580015 CEST	8.8.8.8	192.168.2.3	0x8fa2	No error (0)	doc-14-04-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 3, 2021 21:28:57.060580015 CEST	8.8.8.8	192.168.2.3	0x8fa2	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)
Apr 3, 2021 21:30:28.948357105 CEST	8.8.8.8	192.168.2.3	0x613a	No error (0)	mail.palacioguevara.com	palacioguevara.com		CNAME (Canonical name)	IN (0x0001)
Apr 3, 2021 21:30:28.948357105 CEST	8.8.8.8	192.168.2.3	0x613a	No error (0)	palacioguevara.com		54.37.255.108	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 3, 2021 21:28:57.162213087 CEST	172.217.23.33	443	192.168.2.3	49741	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

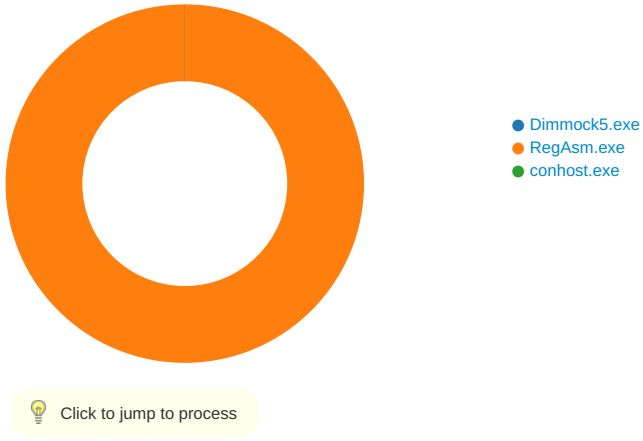
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 3, 2021 21:30:29.168144941 CEST	587	49754	54.37.255.108	192.168.2.3	220-hosting.itecan.es ESMTP Exim 4.94 #2 Sat, 03 Apr 2021 21:30:29 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 3, 2021 21:30:29.168565035 CEST	49754	587	192.168.2.3	54.37.255.108	EHLO 899552
Apr 3, 2021 21:30:29.219896078 CEST	587	49754	54.37.255.108	192.168.2.3	250-hosting.itecan.es Hello 899552 [84.17.52.79] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 3, 2021 21:30:29.221116066 CEST	49754	587	192.168.2.3	54.37.255.108	STARTTLS
Apr 3, 2021 21:30:29.275417089 CEST	587	49754	54.37.255.108	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Dimmock5.exe PID: 4708 Parent PID: 5740

General

Start time:	21:27:00
Start date:	03/04/2021
Path:	C:\Users\user\Desktop\Dimmock5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Dimmock5.exe'
Imagebase:	0x400000
File size:	57344 bytes
MD5 hash:	1F6C8E6472B60D49704703C99B28A4B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 5596 Parent PID: 4708

General

Start time:	21:28:47
Start date:	03/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Dimmock5.exe'
Imagebase:	0xf80000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000016.00000002.728202576.0000000001351000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.734840874.000000001E0F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.734840874.000000001E0F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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	1351DC1	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1351DC1	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1351DC1	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1351DC1	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1351DC1	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1351DC1	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FA60AC	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	72FA60AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FA60AC	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	72FA60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	208C0EA3	WriteFile
\Device\ConDrv	unknown	30	4e 6f 72 64 56 50 4e 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 21 0d 0a	NordVPN directory not found!..	success or wait	1	208C0EA3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FD5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FD5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FD5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FD5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FD8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FD8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FD8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FD5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FD5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	208C0EA3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	208C0EA3	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	208C0EA3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\7d075de3-bfe8-4d61-b585-59e461dcbe8f	unknown	4096	success or wait	1	208C0EA3	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	208C0EA3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	208C0EA3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	208C0EA3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	208C0EA3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	success or wait	1	208C0EA3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4096	end of file	1	208C0EA3	ReadFile

Analysis Process: conhost.exe PID: 5856 Parent PID: 5596

General

Start time:	21:28:47
Start date:	03/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis