ID: 382651
Sample Name: ddff.exe
Cookbook: default.jbs
Time: 12:37:48
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

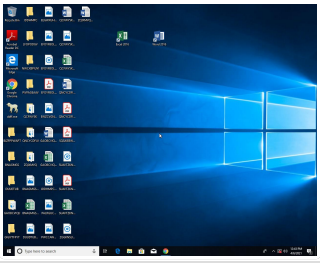
Analysis Report ddff.exe

Overview

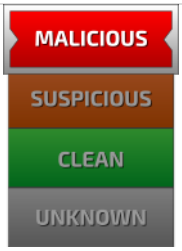
General Information

Sample Name:	ddff.exe
Analysis ID:	382651
MD5:	ded56210e44917..
SHA1:	7a1ca12b56aee8..
SHA256:	422287b67dd187..
Infos:	

Most interesting Screenshot:



Detection



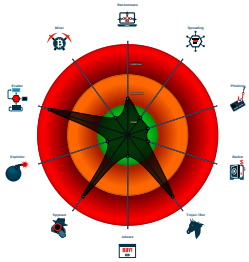
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: RegAsm connects …
- Yara detected AgentTesla
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run

Classification



Startup

- **System is w10x64**
- ddff.exe (PID: 5444 cmdline: 'C:\Users\user\Desktop\ddff.exe' MD5: DED56210E4491797F704B4B0525238D8)
  - RegAsm.exe (PID: 3924 cmdline: 'C:\Users\user\Desktop\ddff.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 5528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "edeiF78",
  "URL: ": "https://t8vI5nXseaUv.com",
  "To: ": "sanetbehin.co@gmail.com",
  "ByHost: ": "mail.gcclatinoamerica.com:587",
  "Password: ": "6VomwXsWgiEV7",
  "From: ": "jobs@gcclatinoamerica.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.847807886.0000000000F02000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 3924	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

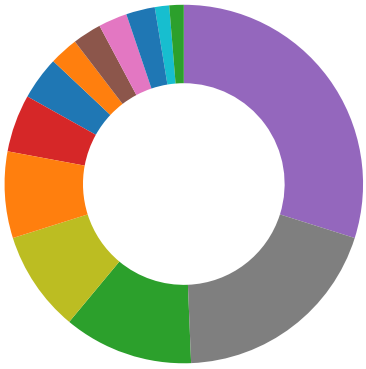
Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 3924	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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)

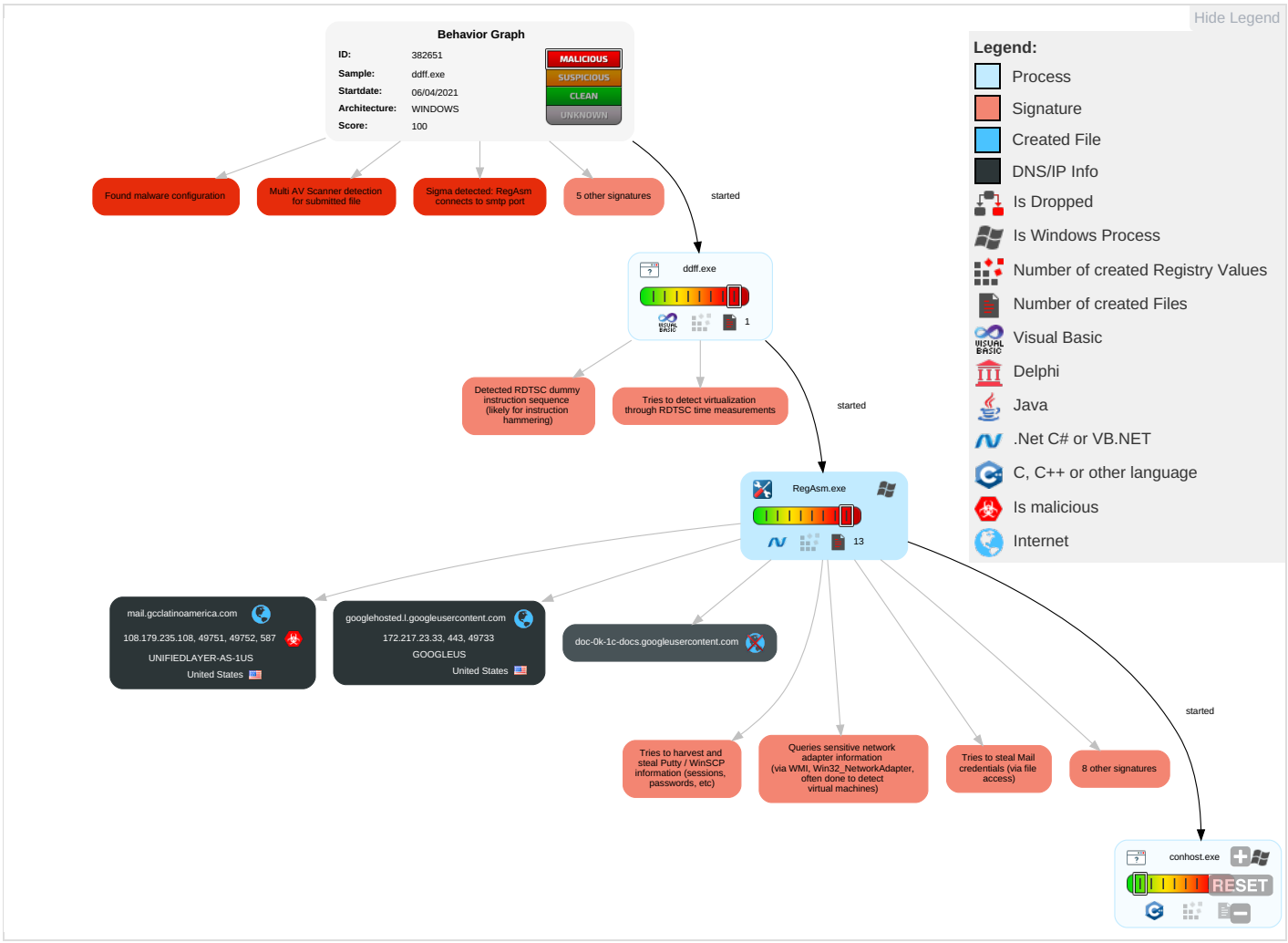
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1 1 1	Security Software Discovery 6 3 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-Standa Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 4 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Applic Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Virtualization/Sandbox Evasion 3 4 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 2	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port

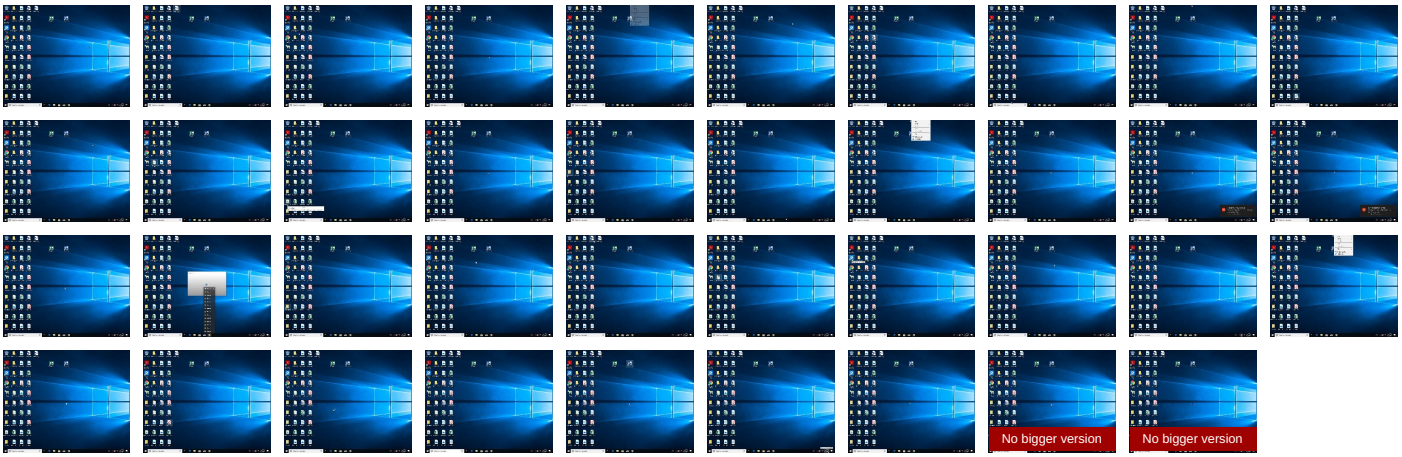
Behavior Graph



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
ddff.exe	16%	Virustotal		Browse
ddff.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mail.gcclatinoamerica.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://ChSulR.com	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	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	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://mail.gcclatinoamerica.com	0%	Virustotal		Browse
http://mail.gcclatinoamerica.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://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://t8vI5nXseaUv.com	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.gcclatinoamerica.com	108.179.235.108	true	true	• 0%, Virustotal, Browse	unknown
googlehosted.l.googleusercontent.com	172.217.23.33	true	false		high
doc-0k-1c-docs.googleusercontent.com	unknown	unknown	false		high

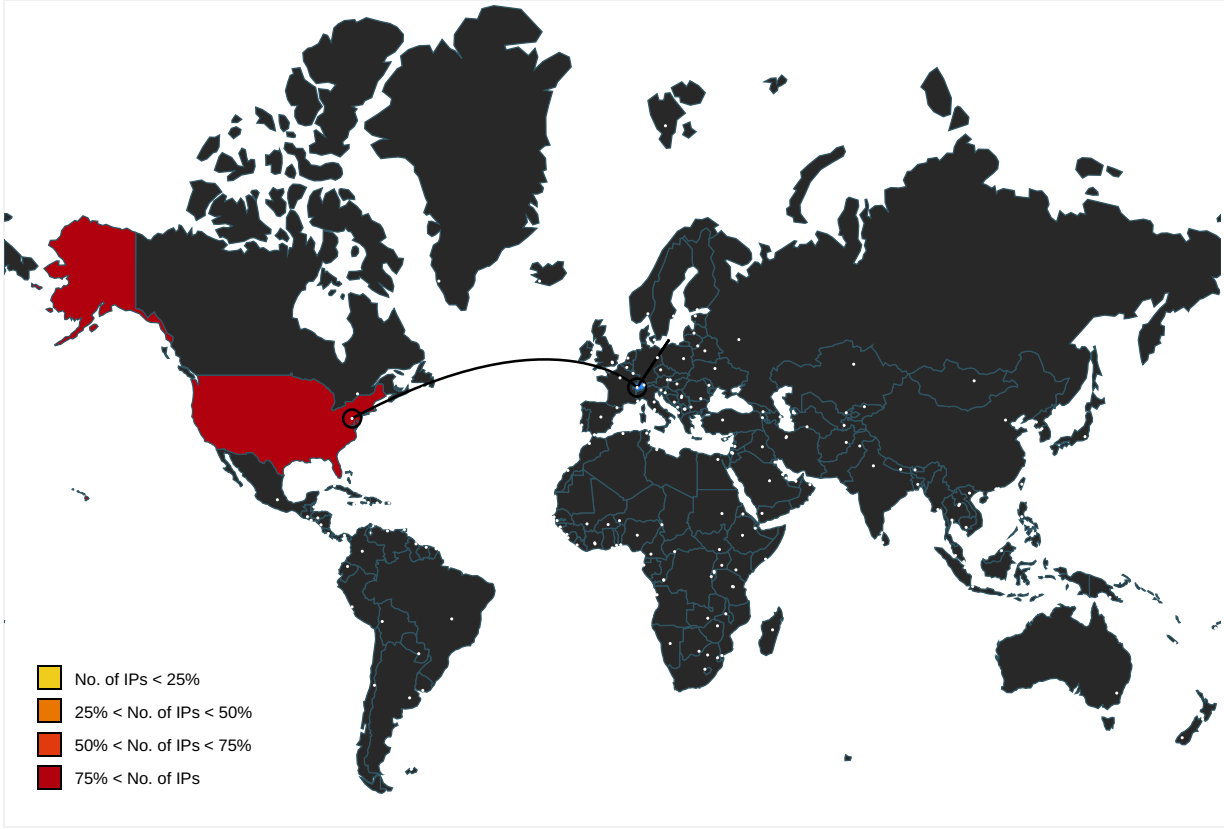
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://t8vl5nXseaUv.com	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, 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-0k-1c-docs.googleusercontent.com/su	RegAsm.exe, 00000013.00000002.850646188.00000000013AE000.00000004.00000020.sdmp	false		high
http://cps.letsencrypt.org0	RegAsm.exe, 00000013.00000002.857466252.000000001DF85000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-0k-1c-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/55mju4ru	RegAsm.exe, 00000013.00000002.850763791.00000000013CC000.00000004.00000020.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ChSulR.com	RegAsm.exe, 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	RegAsm.exe, 00000013.00000002.850882210.00000000013F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	RegAsm.exe, 00000013.00000002.857466252.000000001DF85000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	RegAsm.exe, 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://pki.goog/gsr2/GTS1O1.crt0	RegAsm.exe, 00000013.00000002.850882210.00000000013F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.gcclatinoamerica.com	RegAsm.exe, 00000013.00000002.857466252.000000001DF85000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	RegAsm.exe, 00000013.00000002.850882210.00000000013F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	RegAsm.exe, 00000013.00000002.850882210.00000000013F0000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	RegAsm.exe, 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://cps.root-x1.letsencrypt.org0	RegAsm.exe, 00000013.00000002.857466252.000000001DF85000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	RegAsm.exe, 00000013.00000002.857466252.000000001DF85000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc-0k-1c-docs.googleusercontent.com/	RegAsm.exe, 00000013.00000002.850646188.00000000013AE000.00000004.00000020.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
108.179.235.108	mail.gcclatinoamerica.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382651
Start date:	06.04.2021
Start time:	12:37:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ddff.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:	40
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@3/2@2/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.1% (good quality ratio 4.3%) • Quality average: 50.6% • Quality standard deviation: 35.9%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • 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, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 184.30.21.219, 92.122.145.220, 13.88.21.125, 13.64.90.137, 168.61.161.212, 184.30.20.56, 2.20.142.210, 2.20.142.209, 20.82.209.183, 104.43.193.48, 52.147.198.201, 92.122.213.247, 92.122.213.194, 20.54.26.129, 172.217.20.238, 20.82.210.154, 52.155.217.156, 20.190.160.9, 20.190.160.7, 20.190.160.74, 20.190.160.135, 20.190.160.3, 20.190.160.1, 20.190.160.70, 20.190.160.72, 20.44.239.154, 40.74.108.123, 40.127.240.158 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, login.live.com, audownload.windowsupdate.nsatc.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, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, 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, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:40:20	API Interceptor	1305x 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
UNIFIEDLAYER-AS-1US	PowerShell_Input.ps1	Get hash	malicious	Browse	• 162.241.61.203
	New PO#700-20-HDO410444RF217,pdf.exe	Get hash	malicious	Browse	• 192.185.122.118
	Purchase Order.9000.scan.pdf...exe	Get hash	malicious	Browse	• 162.241.148.243
	document-1848152474.xlsm	Get hash	malicious	Browse	• 192.185.48.186
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 162.241.54.59
	pySsaGoiCT.dll	Get hash	malicious	Browse	• 162.241.54.59
	QOpv1PykFc.dll	Get hash	malicious	Browse	• 162.241.54.59
	S4caD0RhXL.dll	Get hash	malicious	Browse	• 162.241.54.59
	pH8YW11W1x.dll	Get hash	malicious	Browse	• 162.241.54.59
	7z7Q51Y8Xd.dll	Get hash	malicious	Browse	• 162.241.54.59
	pySsaGoiCT.dll	Get hash	malicious	Browse	• 162.241.54.59
	QOpv1PykFc.dll	Get hash	malicious	Browse	• 162.241.54.59
	S4caD0RhXL.dll	Get hash	malicious	Browse	• 162.241.54.59
	pH8YW11W1x.dll	Get hash	malicious	Browse	• 162.241.54.59
	CI-2100403L.exe	Get hash	malicious	Browse	• 192.254.180.165
	wrtKaH8g28.dll	Get hash	malicious	Browse	• 162.241.54.59
	Ip6jHpq61F.dll	Get hash	malicious	Browse	• 162.241.54.59
	y7GBATGcnw.dll	Get hash	malicious	Browse	• 162.241.54.59
	wrtKaH8g28.dll	Get hash	malicious	Browse	• 162.241.54.59
	Ip6jHpq61F.dll	Get hash	malicious	Browse	• 162.241.54.59

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Doc_58YJ54-521DERG701-55YH701.exe	Get hash	malicious	Browse	• 172.217.23.33
	1e#U0414.exe	Get hash	malicious	Browse	• 172.217.23.33
	svhost.exe	Get hash	malicious	Browse	• 172.217.23.33
	beaconxx.exe	Get hash	malicious	Browse	• 172.217.23.33
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 172.217.23.33
	5H957qLghX.exe	Get hash	malicious	Browse	• 172.217.23.33
	FK58.vbs	Get hash	malicious	Browse	• 172.217.23.33
	ZgaBWrz3HH.exe	Get hash	malicious	Browse	• 172.217.23.33
	RFQ#8086A_461A_0000086_300_3550_2021.exe	Get hash	malicious	Browse	• 172.217.23.33
	wzdu53.exe	Get hash	malicious	Browse	• 172.217.23.33
	Opik_lk.exe	Get hash	malicious	Browse	• 172.217.23.33
	document-895003104.xls	Get hash	malicious	Browse	• 172.217.23.33
	Dimmock5.exe	Get hash	malicious	Browse	• 172.217.23.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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):	5.729364262794313

General

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:	ddff.exe
File size:	122880
MD5:	ded56210e4491797f704b4b0525238d8
SHA1:	7a1ca12b56aee84bab41abb6cd4b6eb50a64ef21
SHA256:	422287b67dd187c3fae4472cdf654ef69354ab78ac094dee6711874c9e59f1f4
SHA512:	a5e2399e1b18ac416036658db449c2c77e30a31242d2c827870022989ff5b5cff6cf183b5e04b1a20be72ad615782b8f43975cd42c27d1b961745ee70e6fef3b
SSDEEP:	1536:FGouBWGIDtxQCg53OuHKuSx2ig9TWb1yihGo:FGZBWG+tebq3x2nCb1yihG
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...>..T.....p...`.....(.....@.....

File Icon

Icon Hash:	0ccea09899191898

Static PE Info

General

Entrypoint:	0x401328
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:	0x54DD953E [Fri Feb 13 06:10:06 2015 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:	efa774b90ad6b9ab8c4fabb031ebe78d

Entrypoint Preview

Instruction
push 00413DF0h
call 00007F6C00804D35h
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
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, BBh

Instruction
sub al, 88h
mov ebx, DB9B42F0h
xchg eax, esp
imul edi, dword ptr [eax+001FFE45h], 00h
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi+4D018250h], al
inc ecx
dec ecx
inc esp
inc ebp
dec esi
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
sub byte ptr [ecx], dh
js 00007F6C00804D41h
das
movsd
pop ss
into
dec edi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x175f4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x4856	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
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	0xd4	.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	0x169e4	0x17000	False	0.347486413043	data	6.18979858125	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0xa88	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x4856	0x5000	False	0.414111328125	data	4.36025980168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1b2ae	0x25a8	data		
RT_ICON	0x1a206	0x10a8	data		
RT_ICON	0x1987e	0x988	data		
RT_ICON	0x19416	0x468	GLS_BINARY_LSB_FIRST		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x193d8	0x3e	data		
RT_VERSION	0x19180	0x258	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaVarForInit, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	nyanlgg
FileVersion	3.00
CompanyName	Salty
Comments	Salty
ProductName	Salty
ProductVersion	3.00
FileDescription	Salty
OriginalFilename	nyanlgg.exe

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 98

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 12:40:10.254446983 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.295238018 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.295432091 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.296657085 CEST	49733	443	192.168.2.3	172.217.23.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 12:40:10.337526083 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.351098061 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.351195097 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.351248980 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.351259947 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.351289988 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.351295948 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.351300001 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.351363897 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.364321947 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.405380011 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.405553102 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.406564951 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.451906919 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.651345015 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.651422977 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.651462078 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.651473999 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.651499033 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.651524067 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.651539087 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.651582956 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.651583910 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.651643038 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.654021025 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.654078960 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.654099941 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.654149055 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.656913996 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.656971931 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.656991959 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.657046080 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.659732103 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.659790039 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.659805059 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.659856081 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.662596941 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.662646055 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.662668943 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.662710905 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.664926052 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.664979935 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.665019989 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.665044069 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.692289114 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.692349911 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.692431927 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.692480087 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.693635941 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.693692923 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.693773985 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.693820000 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.696532965 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.696590900 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.696675062 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.696719885 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.699392080 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.699450970 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.699522018 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.699567080 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.702272892 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.702332020 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.702398062 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.702445030 CEST	49733	443	192.168.2.3	172.217.23.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 12:40:10.705205917 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.705260992 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.705332041 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.705378056 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.707999945 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.708055973 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.708143950 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.708189964 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.710887909 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.710947037 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.710975885 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.711003065 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.713692904 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.713759899 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.713761091 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.713937998 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.716240883 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.716296911 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.716316938 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.716358900 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.718739033 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.718800068 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.718806982 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.718856096 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.721297979 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.721350908 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.721368074 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.721409082 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.723886013 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.723939896 CEST	443	49733	172.217.23.33	192.168.2.3
Apr 6, 2021 12:40:10.723957062 CEST	49733	443	192.168.2.3	172.217.23.33
Apr 6, 2021 12:40:10.724001884 CEST	49733	443	192.168.2.3	172.217.23.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 12:38:26.490256071 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:26.549189091 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:27.416503906 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:27.480247021 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:28.519505024 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:28.575723886 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:29.014059067 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:29.072041035 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:30.183959961 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:30.229957104 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:31.505867958 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:31.552011967 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:52.675306082 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:52.724174976 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:53.792023897 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:53.837938070 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:55.091465950 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:55.137310028 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 6, 2021 12:38:56.338965893 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:38:56.385159969 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:05.734342098 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:05.807686090 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:21.900122881 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:21.959518909 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:24.274601936 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:24.320872068 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:26.891315937 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:26.940251112 CEST	53	53195	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 12:39:28.500572920 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:28.549417973 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:30.388962030 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:30.438782930 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:31.387197018 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:31.433409929 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:32.174664021 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:32.223575115 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:35.404690981 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:35.452562094 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:36.924537897 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:36.971714020 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:37.874058008 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:37.922924042 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:39.459230900 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:39.515553951 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:40.542083979 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:40.588284016 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:41.355058908 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:41.403889894 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 6, 2021 12:39:52.314244986 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:39:52.384251118 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 6, 2021 12:40:07.986004114 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:40:08.048541069 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 6, 2021 12:40:08.731096983 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:40:08.776892900 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 6, 2021 12:40:10.189623117 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:40:10.252120018 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 6, 2021 12:40:13.892976999 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:40:13.947936058 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 6, 2021 12:40:44.937808990 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:40:44.993721008 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 6, 2021 12:40:46.527230978 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:40:46.573290110 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:21.843970060 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:21.927680969 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:22.512407064 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:22.567893028 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:22.960082054 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:23.318380117 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:23.886065960 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:23.943433046 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:24.556430101 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:24.612591982 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:25.342679977 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:25.415327072 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:25.958585024 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:26.018208027 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:26.713805914 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:26.771321058 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:27.935620070 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:27.990155935 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:28.673451900 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:28.719708920 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 6, 2021 12:41:45.341291904 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:41:45.547538042 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 6, 2021 12:43:18.767577887 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:43:18.822230101 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 6, 2021 12:43:19.421952963 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:43:19.486018896 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 6, 2021 12:43:23.231192112 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:43:23.285566092 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 6, 2021 12:43:29.205905914 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:43:29.276460886 CEST	53	56803	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 12:43:30.403588057 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 6, 2021 12:43:30.471645117 CEST	53	57145	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 12:40:10.189623117 CEST	192.168.2.3	8.8.8.8	0xf3b	Standard query (0)	doc-0k-1c-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Apr 6, 2021 12:41:45.341291904 CEST	192.168.2.3	8.8.8.8	0x53fd	Standard query (0)	mail.gcclatinoamerica.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 12:40:10.252120018 CEST	8.8.8.8	192.168.2.3	0xf3b	No error (0)	doc-0k-1c-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 12:40:10.252120018 CEST	8.8.8.8	192.168.2.3	0xf3b	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.33	A (IP address)	IN (0x0001)
Apr 6, 2021 12:41:45.547538042 CEST	8.8.8.8	192.168.2.3	0x53fd	No error (0)	mail.gcclatinoamerica.com		108.179.235.108	A (IP address)	IN (0x0001)
Apr 6, 2021 12:43:18.822230101 CEST	8.8.8.8	192.168.2.3	0x572c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	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 6, 2021 12:40:10.351300001 CEST	172.217.23.33	443	192.168.2.3	49733	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

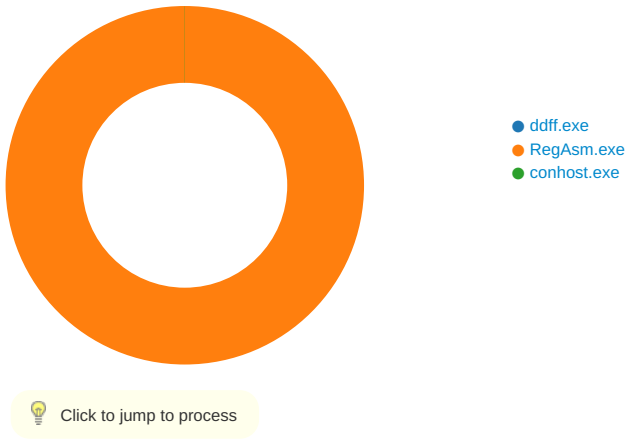
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 6, 2021 12:41:46.038834095 CEST	587	49751	108.179.235.108	192.168.2.3	220-gator4253.hostgator.com ESMTP Exim 4.93 #2 Tue, 06 Apr 2021 05:41:45 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 6, 2021 12:41:46.039329052 CEST	49751	587	192.168.2.3	108.179.235.108	EHLO 760639
Apr 6, 2021 12:41:46.195832014 CEST	587	49751	108.179.235.108	192.168.2.3	250-gator4253.hostgator.com Hello 760639 [84.17.52.79] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 6, 2021 12:41:46.196239948 CEST	49751	587	192.168.2.3	108.179.235.108	STARTTLS
Apr 6, 2021 12:41:46.355518103 CEST	587	49751	108.179.235.108	192.168.2.3	220 TLS go ahead
Apr 6, 2021 12:41:49.212441921 CEST	587	49752	108.179.235.108	192.168.2.3	220-gator4253.hostgator.com ESMTP Exim 4.93 #2 Tue, 06 Apr 2021 05:41:49 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 6, 2021 12:41:49.212722063 CEST	49752	587	192.168.2.3	108.179.235.108	EHLO 760639

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 6, 2021 12:41:49.373460054 CEST	587	49752	108.179.235.108	192.168.2.3	250-gator4253.hostgator.com Hello 760639 [84.17.52.79] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 6, 2021 12:41:49.374119043 CEST	49752	587	192.168.2.3	108.179.235.108	STARTTLS
Apr 6, 2021 12:41:49.538451910 CEST	587	49752	108.179.235.108	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ddff.exe PID: 5444 Parent PID: 5600

General

Start time:	12:38:32
Start date:	06/04/2021
Path:	C:\Users\user\Desktop\ddff.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ddff.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	DED56210E4491797F704B4B0525238D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 3924 Parent PID: 5444

General

Start time:	12:39:57
Start date:	06/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ddff.exe'
Imagebase:	0xae0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000013.00000002.847807886.0000000000F02000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.857079971.000000001DC21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.857079971.000000001DC21000.00000004.00000001.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	F04607	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	F04607	InternetOpenUrlA
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	F04607	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	F04607	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	F04607	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	F04607	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	6D2ACF06	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	6D2ACF06	unknown
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1FBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1FBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1FBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1FDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome\Default\Cookies	success or wait	1	6C1F6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C1F1B4F	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	6C1F1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1FDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D285705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D28CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D28CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D28CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D285705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1F1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1F1B4F	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\1a95558a-7811-432a-9965-aa2eb87db5e7	unknown	4096	success or wait	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Roaming\ifg4v0bb.jfl\Chrome\Default\Cookies	unknown	16384	success or wait	1	6C1F1B4F	ReadFile

Analysis Process: conhost.exe PID: 5528 Parent PID: 3924

General

Start time:	12:39:58
Start date:	06/04/2021
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