ID: 830729
Sample Name:
g0PWOnCNZH.exe
Cookbook: default.jbs
Time: 16:40:05
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

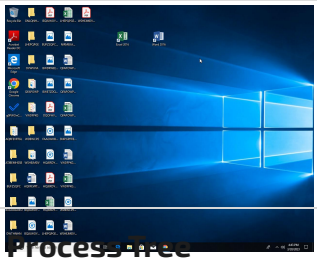
Windows Analysis Report

g0PWOnCNZH.exe

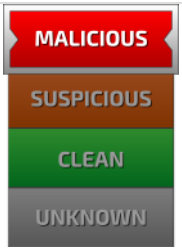
Overview

General Information

Sample Name:	g0PWOnCNZH.exe
Original Sample Name:	87be1ac6122e…
Analysis ID:	830729
MD5:	87be1ac6122e…
SHA1:	28954d7b8138…
SHA256:	de673c657760…
Tags:	32 AgentTesla exe trojan
Infos:	



Detection



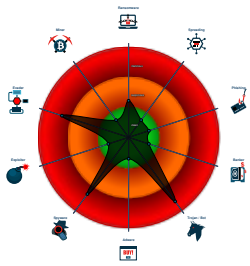
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Uses the Telegram API (likely for C…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- May check the online IP address of…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- g0PWOnCNZH.exe (PID: 5956 cmdline: C:\Users\user\Desktop\g0PWOnCNZH.exe MD5: 87BE1AC6122ED0C75B3AF80696B9E686)
  - RegSvcs.exe (PID: 6088 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/sendMessage"
}
```

Copyright Joe Security LLC 2023

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/sendMessage?chat_id=1295185895"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegSvcs.exe PID: 6088	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegSvcs.exe PID: 6088	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 149.154.167.220

Timestamp:	192.168.2.3149.154.167.220496854432851779 03/20/23-16:41:25.765012
SID:	2851779
Source Port:	49685
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

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

May check the online IP address of the machine

Copyright Joe Security LLC 2023

Malware Analysis System Evasion

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

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

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

Remote Access Functionality

Yara detected Telegram RAT

Yara detected AgentTesla

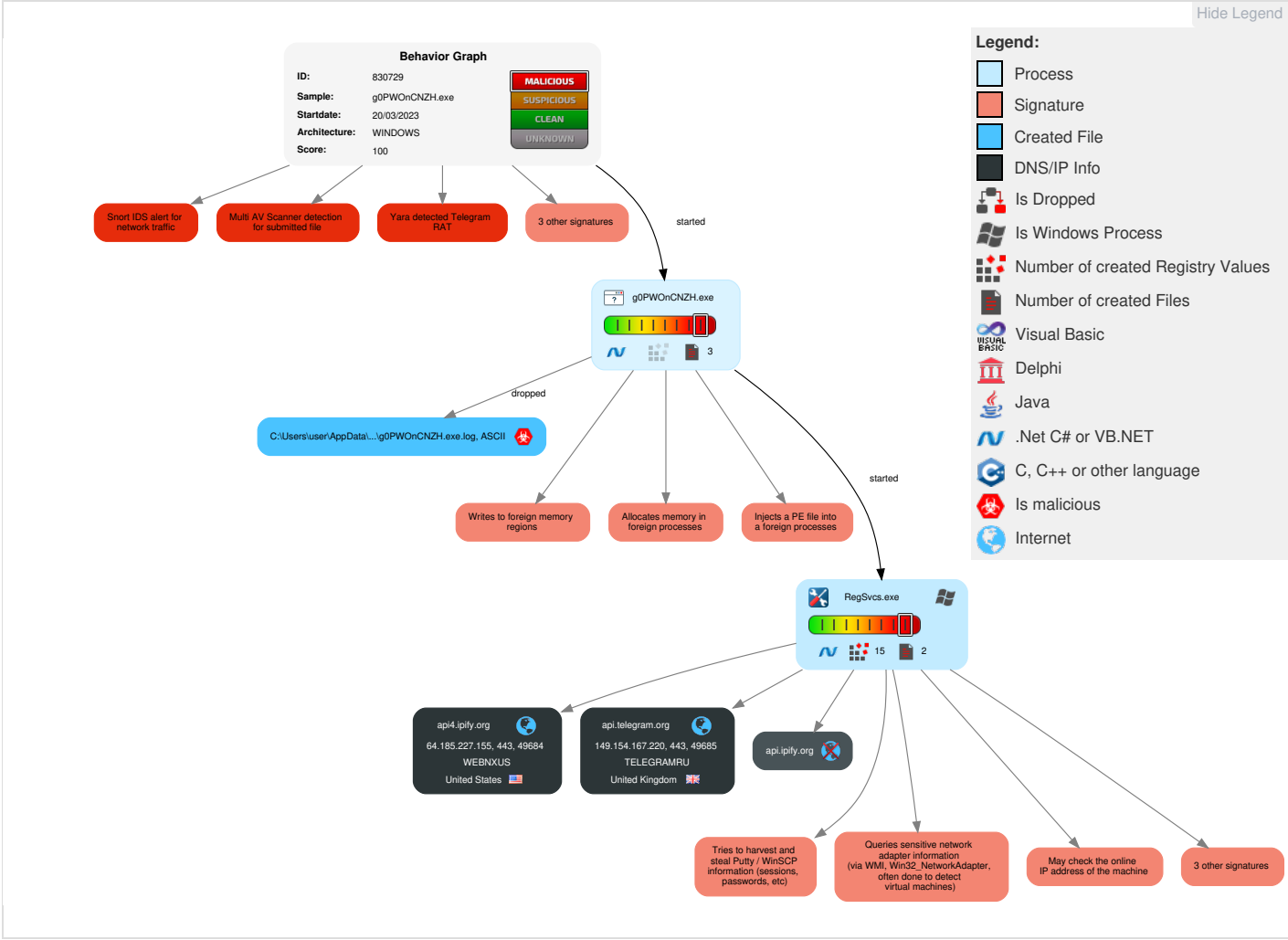
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	3 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	1 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Copyright Joe Security LLC 2023

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 1 4 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

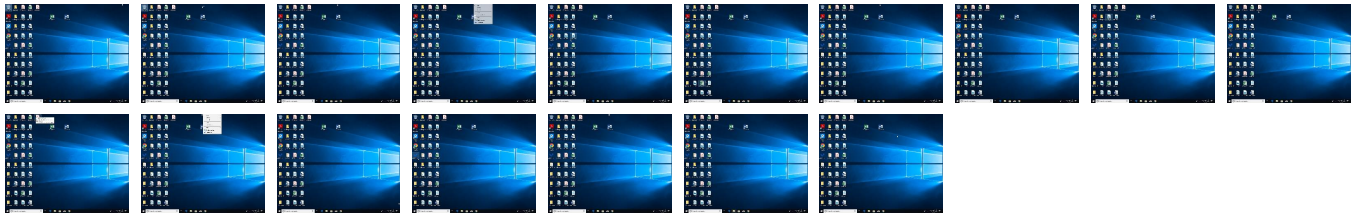
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2023

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
g0PWOnCNZH.exe	43%	Virustotal		Browse
g0PWOnCNZH.exe	26%	ReversingLabs	Win32.Trojan.Generic	
g0PWOnCNZH.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

Copyright Joe Security LLC 2023

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.founder.com.cn/cnD	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comTF	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.com(	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.monotype.U	0%	Avira URL Cloud	safe	
http://www.tiro.comw	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comq	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmR	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmR	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api4.ipify.org	64.185.227.155	true	false		high
api.telegram.org	149.154.167.220	true	false		high
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high
http://https://api.telegram.org/bot2134979594:AAFk4QkrIHlt2a-q-EhIoHZBbzxSH0QxiBI/sendDocument	false		high

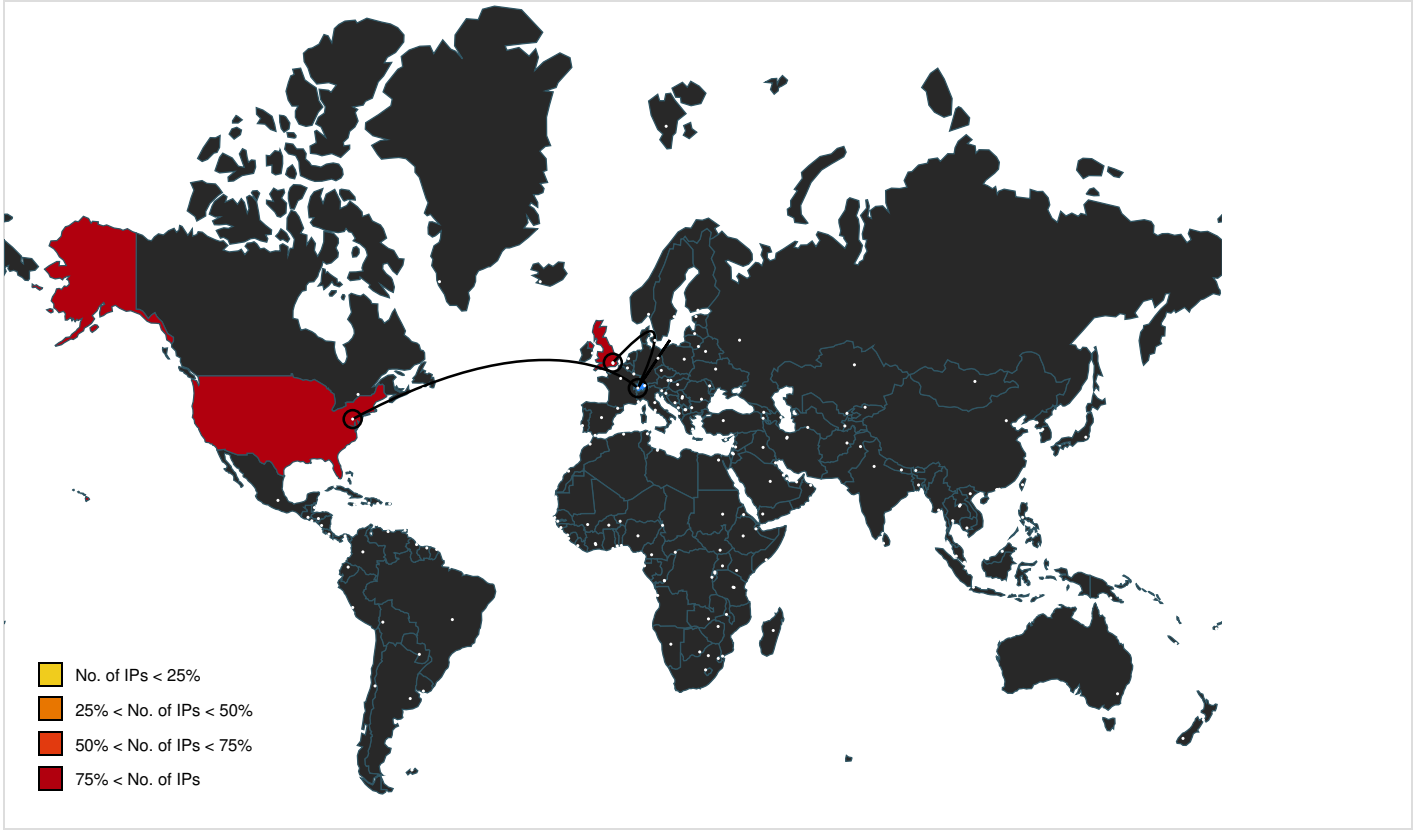
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.U	g0PWOnCNZH.exe, 00000000.00000003.261959194.0000000005D5B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comiv	g0PWOnCNZH.exe, 00000000.00000003.252565247.0000000005D6B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com2	g0PWOnCNZH.exe, 00000000.00000003.252565247.0000000005D6B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	RegSvcs.exe, 00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersB	g0PWOnCNZH.exe, 00000000.00000003.263731883.0000000005D55000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.tiro.com	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	g0PWOnCNZH.exe, 00000000.00000003.270701555.0000000005D50000.00000004.00000020.00020000.00000000.sdmp, g0PWOnCNZH.exe, 00000000.00000003.255937391.0000000005D5E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coml1	g0PWOnCNZH.exe, 00000000.00000002.275360961.0000000001517000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnD	g0PWOnCNZH.exe, 00000000.00000003.253963556.0000000005D58000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org	RegSvcs.exe, 00000001.00000002.524290015.00000000028A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	RegSvcs.exe, 00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrito	g0PWOnCNZH.exe, 00000000.00000002.275360961.0000000001517000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com(	g0PWOnCNZH.exe, 00000000.00000003.254042499.0000000005D58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.zhongyicts.com.cn	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmR	g0PWOnCNZH.exe, 00000000.00000003.261346015.0000000005D55000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 00000001.00000002.524290015.00000000028A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comw	g0PWOnCNZH.exe, 00000000.00000003.254042499.0000000005D5E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comq	g0PWOnCNZH.exe, 00000000.00000003.252565247.0000000005D6B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comTF	g0PWOnCNZH.exe, 00000000.00000003.252565247.0000000005D6B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	g0PWOnCNZH.exe, 00000000.00000003.255937391.0000000005D5E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/	RegSvcs.exe, 00000001.00000002.524290015.00000000028A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	g0PWOnCNZH.exe, 00000000.00000003.253963556.0000000005D58000.00000004.00000020.00020000.00000000.sdmp, g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.	g0PWOnCNZH.exe, 00000000.00000003.261959194.0000000005D5B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	g0PWOnCNZH.exe, 00000000.00000002.275360961.0000000001517000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	g0PWOnCNZH.exe, 00000000.00000002.297868542.0000000006F62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://api.telegram.org	RegSvcs.exe, 00000001.00000002.524290015.0000000002921000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
64.185.227.155	api4.ipify.org	United States		18450	WEBNXUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830729
Start date and time:	2023-03-20 16:40:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	g0PWOnCNZH.exe
Original Sample Name:	87be1ac6122ed0c75b3af80696b9e686.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

Copyright Joe Security LLC 2023

HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:41:07	API Interceptor	1x Sleep call for process: g0PWOnCNZH.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0PWOnCNZH.exe.log

Process:	C:\Users\user\Desktop\g0PWOnCNZH.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A

SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	
Entropy (8bit):	7.86252276593653
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	g0PWOnCNZH.exe
File size:	746496
MD5:	87be1ac6122ed0c75b3af80696b9e686
SHA1:	28954d7b81380a52dc012eb21c4769fe54070a5c
SHA256:	de673c6577604d1036c5df6d67d9f5f9010eeb367a43ec7712b5614f70b725cd
SHA512:	a58b7039d2967f214534f0609e9e2fa16b0ae2520265bac212cfd8a2d3a908276b1ef54bd8536028ddd1614eafd686d9effdd7d7a3472845c668c1cb1bc7f947
SSDEEP:	12288:r9umYMUnFW/Nhb/kpGsc1WgkAhK6KttQM2AW+DYXoRf0D9u1pHG8RTiy4uhyNv6n:r9uUT2wogkAg6K7Q4pMXomwRhhyNv6
TLSH:	76F402782F8A9538F1321BBD85E8264467AEB3B26713D55D18F511CE4B63B034ED0A2F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...;..d.....0..N.....fm... .....@.. .....@.....

File Icon

Icon Hash:	209480e66eb84902

Network Behavior

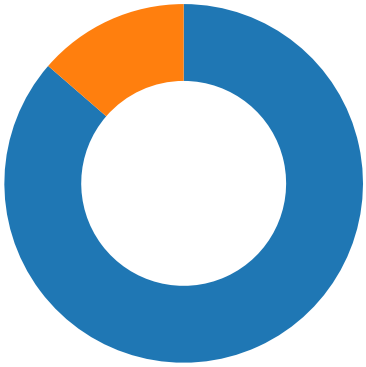
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3149.154.167.220496854432851779 03/20/23-16:41:25.765012	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49685	443	192.168.2.3	149.154.167.220

Network Port Distribution

Total Packets: 22

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:41:11.823951960 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:11.824016094 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:11.824614048 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:11.861870050 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:11.861911058 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.289160013 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.289249897 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:13.293323994 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:13.293349981 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.293910980 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.336273909 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:13.603498936 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:13.603526115 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.702334881 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.703789949 CET	443	49684	64.185.227.155	192.168.2.3
Mar 20, 2023 16:41:13.703888893 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:13.705327988 CET	49684	443	192.168.2.3	64.185.227.155
Mar 20, 2023 16:41:25.648309946 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.648375988 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.648475885 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.649236917 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.649266005 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.715833902 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.715944052 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.718837976 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.718869925 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.719206095 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.721429110 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.721477032 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.762315035 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.764890909 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.764924049 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.857546091 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.857656956 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.858115911 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.858155012 CET	49685	443	192.168.2.3	149.154.167.220
Mar 20, 2023 16:41:25.858175039 CET	443	49685	149.154.167.220	192.168.2.3
Mar 20, 2023 16:41:25.858217001 CET	49685	443	192.168.2.3	149.154.167.220

UDP Packets

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:41:11.759686947 CET	58974	53	192.168.2.3	8.8.8.8
Mar 20, 2023 16:41:11.779360056 CET	53	58974	8.8.8.8	192.168.2.3
Mar 20, 2023 16:41:11.789952040 CET	63722	53	192.168.2.3	8.8.8.8
Mar 20, 2023 16:41:11.807668924 CET	53	63722	8.8.8.8	192.168.2.3
Mar 20, 2023 16:41:25.629864931 CET	65522	53	192.168.2.3	8.8.8.8
Mar 20, 2023 16:41:25.647144079 CET	53	65522	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:41:11.759686947 CET	192.168.2.3	8.8.8.8	0x745e	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:11.789952040 CET	192.168.2.3	8.8.8.8	0xb647	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:25.629864931 CET	192.168.2.3	8.8.8.8	0x9cef	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

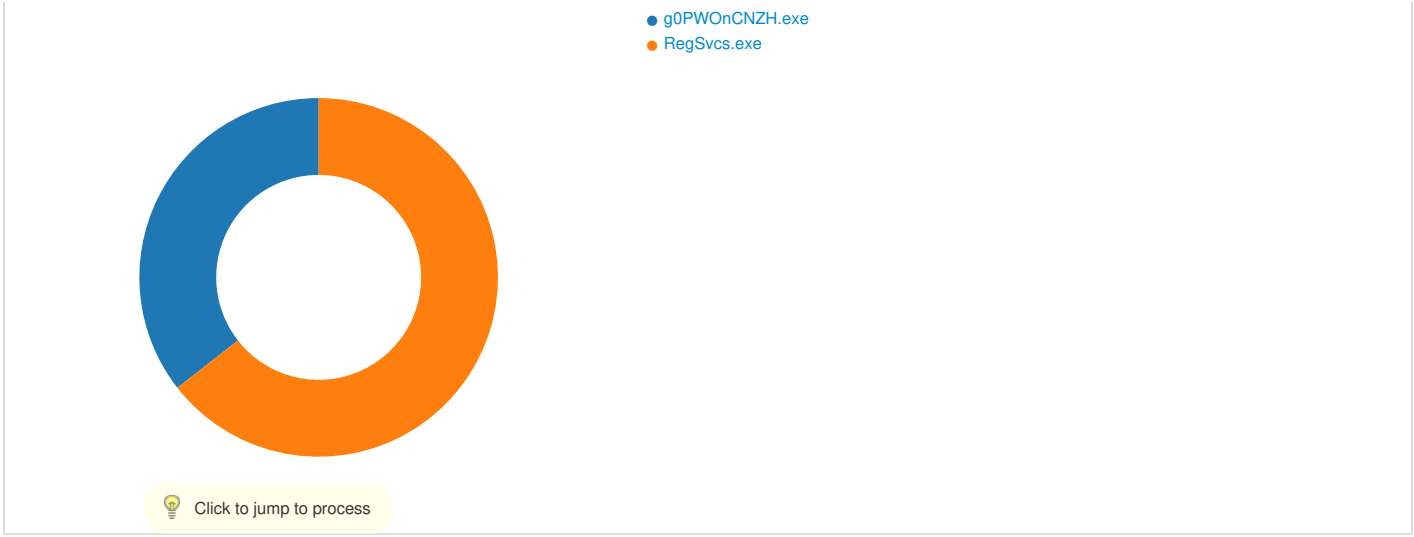
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 16:41:11.779360056 CET	8.8.8.8	192.168.2.3	0x745e	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 16:41:11.779360056 CET	8.8.8.8	192.168.2.3	0x745e	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:11.779360056 CET	8.8.8.8	192.168.2.3	0x745e	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:11.779360056 CET	8.8.8.8	192.168.2.3	0x745e	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:11.807668924 CET	8.8.8.8	192.168.2.3	0xb647	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 16:41:11.807668924 CET	8.8.8.8	192.168.2.3	0xb647	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:11.807668924 CET	8.8.8.8	192.168.2.3	0xb647	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:11.807668924 CET	8.8.8.8	192.168.2.3	0xb647	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:41:25.647144079 CET	8.8.8.8	192.168.2.3	0x9cef	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org
- api.telegram.org

Statistics

Behavior



System Behavior

Analysis Process: g0PWOnCNZH.exe PID: 5956, Parent PID: 3452

General

Target ID:	0
Start time:	16:41:00
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\g0PWOnCNZH.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g0PWOnCNZH.exe
Imagebase:	0x990000
File size:	746496 bytes
MD5 hash:	87BE1AC6122ED0C75B3AF80696B9E686
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0PWOnCNZH.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g0PWOnCNZH.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: RegSvcs.exe PID: **6088**, Parent PID: **5956**

General

Target ID:	1
Start time:	16:41:09
Start date:	20/03/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x570000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2023

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.524290015.00000000028EC000.00000004.00000800.00020000.00000000.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	7299CF06	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	7299CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly