ID: 736948
Sample Name:
rzN2ckYW24.exe
Cookbook: default.jbs
Time: 12:20:04
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

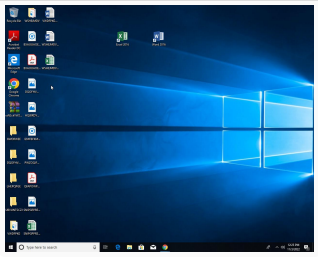
Windows Analysis Report

rzN2ckYW24.exe

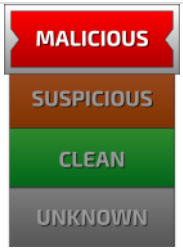
Overview

General Information

Sample Name:	rzN2ckYW24.exe
Analysis ID:	736948
MD5:	44159444c9bc99..
SHA1:	baf57ff497d2e20..
SHA256:	9e4f0e0a10a778..
Tags:	AgentTesla exe
Infos:	



Detection



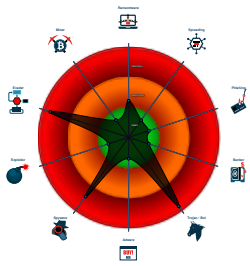
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Uses the Telegram API (likely for C…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- rzN2ckYW24.exe (PID: 3044 cmdline: C:\Users\user\Desktop\rzN2ckYW24.exe MD5: 44159444C9BC9980871B80B3AE071FFB)
  - rzN2ckYW24.exe (PID: 6132 cmdline: C:\Users\user\Desktop\rzN2ckYW24.exe MD5: 44159444C9BC9980871B80B3AE071FFB)
  - rzN2ckYW24.exe (PID: 6128 cmdline: C:\Users\user\Desktop\rzN2ckYW24.exe MD5: 44159444C9BC9980871B80B3AE071FFB)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5577155192:AAEz6ZTkghx2RsdTxeeE-sDulPHc5WQblVg/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot5577155192:AAEz6ZTkghx2RsdTxeeE-sDulPHc5WQblVg/"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.522788647.0000000002854000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.522788647.0000000002854000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000000.279572374.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.279572374.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000000.279572374.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31d21:$a13: get_DnsResolver • 0x30402:$a20: get_LastAccessed • 0x3274f:$a27: set_InternalServerPort • 0x32a84:$a30: set_GuidMasterKey • 0x30514:$a33: get_Clipboard • 0x30522:$a34: get_Keyboard • 0x3191b:$a35: get_ShiftKeyDown • 0x3192c:$a36: get_AltKeyDown • 0x3052f:$a37: get_Password • 0x31062:$a38: get_PasswordHash • 0x32183:$a39: get_DefaultCredentials
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.rzN2ckYW24.exe.3dd31a8.13.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.rzN2ckYW24.exe.3dd31a8.13.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.rzN2ckYW24.exe.3dd31a8.13.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c5f:$s10: logins • 0x326d9:$s11: credential • 0x2e914:$g1: get_Clipboard • 0x2e922:$g2: get_Keyboard • 0x2e92f:$g3: get_Password • 0x2fd0b:$g4: get_CtrlKeyDown • 0x2fd1b:$g5: get_ShiftKeyDown • 0x2fd2c:$g6: get_AltKeyDown
0.2.rzN2ckYW24.exe.3dd31a8.13.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30121:$a13: get_DnsResolver • 0x2e802:$a20: get_LastAccessed • 0x30b4f:$a27: set_InternalServerPort • 0x30e84:$a30: set_GuidMasterKey • 0x2e914:$a33: get_Clipboard • 0x2e922:$a34: get_Keyboard • 0x2fd1b:$a35: get_ShiftKeyDown • 0x2fd2c:$a36: get_AltKeyDown • 0x2e92f:$a37: get_Password • 0x2f462:$a38: get_PasswordHash • 0x30583:$a39: get_DefaultCredentials
2.0.rzN2ckYW24.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 28 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:	192.168.2.3149.154.167.220497034432851779 11/03/22-12:21:37.839026
SID:	2851779
Source Port:	49703
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

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

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 ftp login credentials

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

Remote Access Functionality

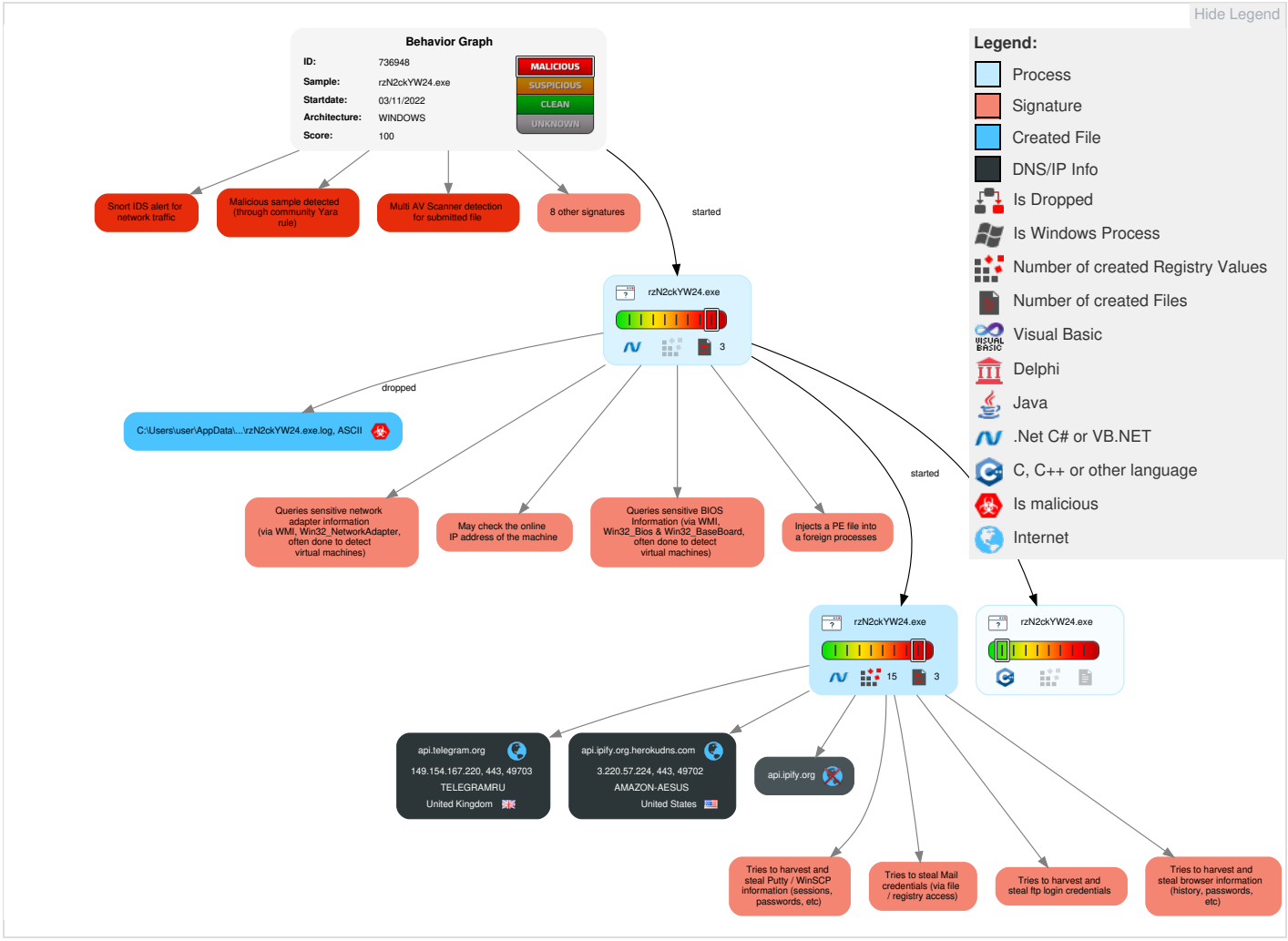
Yara detected Telegram RAT

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	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 Account Discovery	Remote Services	1 1 Archive Collected Data	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 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	2 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	1 Process 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 Timestomp	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	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	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 System Owner/User 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	1 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

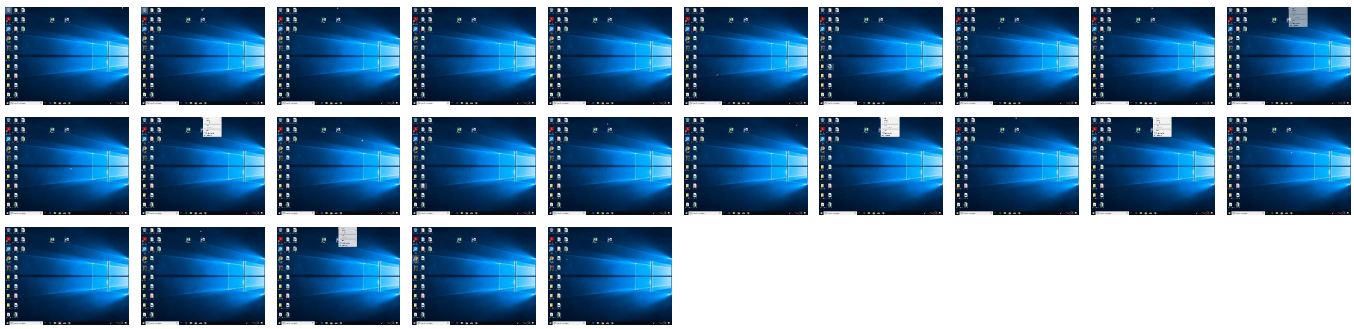
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
rzN2ckYW24.exe	30%	Virustotal		Browse
rzN2ckYW24.exe	32%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
rzN2ckYW24.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.rzN2ckYW24.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
api.ipify.org.herokudns.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sakkal.comrm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	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.jiyu-kobo.co.jp/dz	0%	Virustotal		Browse
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://api.ipify.orgappdatajVuurjVuur.exe/TMVuQQ.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cB	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/dz	0%	Avira URL Cloud	safe	
http://www.fontbureau.commTTF	0%	Avira URL Cloud	safe	
http://https://api.telegram.org4Tkh	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comp	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comitum	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/b	0%	URL Reputation	safe	
http://wmwpuO0P35oL9Q.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//ra	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cns-ea	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.ipify.org.herokudns.com	3.220.57.224	true	false	• 0%, Virustotal, Browse	unknown
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/bot5577155192:AAEz6ZTkghx2RsdTxeeE-sDulPHc5WQblVg/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	rzN2ckYW24.exe, 00000000.00000002.305428250.000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comiv	rzN2ckYW24.exe, 00000000.00000003.258445715.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257102086.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259940209.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259819475.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259520848.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257053691.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258806192.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261728305.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260344832.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257296101.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260291295.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261561559.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258343538.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260210658.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.2616 92319.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257200608.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258935636.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261197728.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257254857.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258324367.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261444840.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	rzN2ckYW24.exe, 00000000.00000002.305428250.000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	rzN2ckYW24.exe, 00000000.00000002.305428250.000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

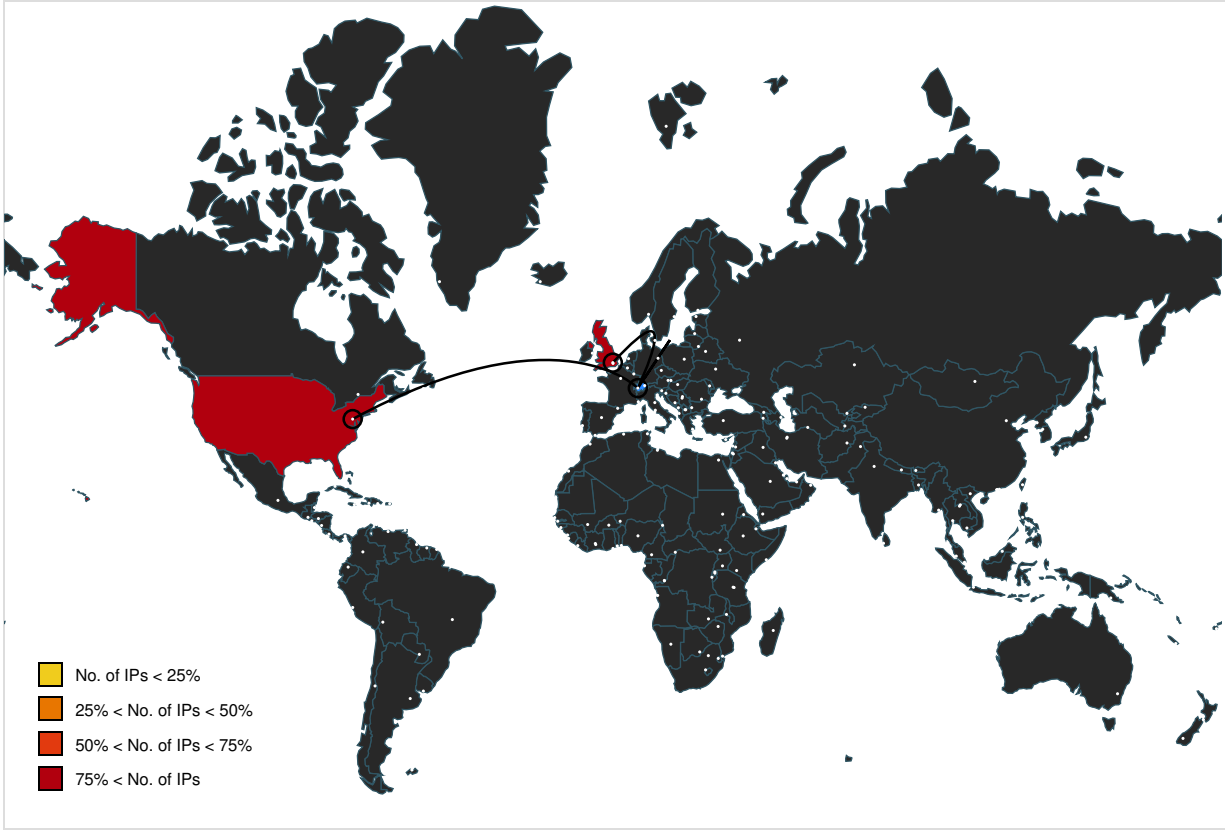
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org	rzN2ckYW24.exe, 00000002.00000002.525368476.0000000002ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.comrm	rzN2ckYW24.exe, 00000000.00000003.262413128.0000000005CB5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/a-d	rzN2ckYW24.exe, 00000000.00000003.261577709.0000000005C8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot5577155192:AAEz6ZTkghx2RsdTxeeE-sDulPHc5WQblVg/	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.orgappdatajVuurjVuur.exe/TMVuQQ.com	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/dz	rzN2ckYW24.exe, 00000000.00000003.261577709.0000000005C8B000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot5577155192:AAEz6ZTkghx2RsdTxeeE-sDulPHc5WQblVg/5596534279%discordapi%yyy	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cB	rzN2ckYW24.exe, 00000000.00000003.259617773.0000000005C87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersS	rzN2ckYW24.exe, 00000000.00000003.271274480.0000000005C88000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	rzN2ckYW24.exe, 00000000.00000003.261392765.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	rzN2ckYW24.exe, 00000000.00000003.262479660.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.262420491.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.coma	rzN2ckYW24.exe, 00000000.00000003.258445715.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257102086.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259940209.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259819475.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259520848.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257053691.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258806192.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261728305.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260344832.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257296101.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260291295.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261561559.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258343538.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260210658.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261692319.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257200608.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258935636.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261197728.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.257254857.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.258324367.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261444840.0000000005C9B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commTTF	rzN2ckYW24.exe, 00000000.00000003.271274480.0000000005C88000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000002.304989135.0000000005C80000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.272003113.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.271826229.0000000005C87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org4Tkh	rzN2ckYW24.exe, 00000002.00000002.525368476.0000000002ADC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	rzN2ckYW24.exe, 00000000.00000003.260307774.0000000005C87000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.260356342.0000000005C87000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	rzN2ckYW24.exe, 00000000.00000003.265445027.0000000005C8E000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.265034269.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.265360818.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	rzN2ckYW24.exe, 00000000.00000003.265445027.0000000005C8E000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.264972803.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comitum	rzN2ckYW24.exe, 00000000.00000003.265445027.0000000005C8E000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.265360818.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	rzN2ckYW24.exe, 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcomp	rzN2ckYW24.exe, 00000000.00000003.265445027.0000000005C8E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.wikipedia	rzN2ckYW24.exe, 00000000.00000003.256683274.0000000005CA3000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.256591750.0000000005CA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://wmwpuO0P35oL9Q.com	rzN2ckYW24.exe, 00000002.00000002.525344688.0000000002AD6000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000002.00000002.525368476.0000000002ADC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmp	rzN2ckYW24.exe, 00000000.00000002.304989135.0000000005C80000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//ra	rzN2ckYW24.exe, 00000000.00000003.262479660.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.262420491.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	rzN2ckYW24.exe, 00000000.00000003.262479660.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.262420491.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	rzN2ckYW24.exe, 00000000.00000003.271274480.0000000005C88000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000002.304989135.0000000005C80000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.272003113.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.271826229.0000000005C87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	rzN2ckYW24.exe, 00000000.00000003.265445027.0000000005C8E000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.265360818.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	rzN2ckYW24.exe, 00000000.00000003.257245989.0000000005C86000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	rzN2ckYW24.exe, 00000000.00000003.259617773.0000000005C87000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259464865.0000000005C87000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.259543069.0000000005C88000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	rzN2ckYW24.exe, 00000000.00000003.265034269.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comcomF	rzN2ckYW24.exe, 00000000.00000003.265034269.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	rzN2ckYW24.exe, 00000000.00000003.271826229.0000000005C87000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	rzN2ckYW24.exe, 00000000.00000003.261577709.0000000005C8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comp	rzN2ckYW24.exe, 00000000.00000003.265360818.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	rzN2ckYW24.exe, 00000000.00000002.305428250.0000000006E92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	rzN2ckYW24.exe, 00000000.00000003.266665020.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.265445027.0000000005C8E000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.265360818.0000000005C8C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cns-ea	rzN2ckYW24.exe, 00000000.00000003.259617773.0000000005C87000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.telegram.org	rzN2ckYW24.exe, 00000002.00000002.525368476.0000000002ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/b	rzN2ckYW24.exe, 00000000.00000003.262479660.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.262420491.0000000005C8D000.00000004.00000800.00020000.00000000.sdmp, rzN2ckYW24.exe, 00000000.00000003.261577709.0000000005C8B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
3.220.57.224	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736948
Start date and time:	2022-11-03 12:20:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rzN2ckYW24.exe
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:	14
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@5/1@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 97% • 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
12:21:13	API Interceptor	488x Sleep call for process: rzN2ckYW24.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\rzN2ckYW24.exe.log

Process:	C:\Users\user\Desktop\rzN2ckYW24.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:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.915053550313837
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	rzN2ckYW24.exe
File size:	684032
MD5:	44159444c9bc9980871b80b3ae071ffb
SHA1:	baf57ff497d2e202a1a119e8719e44c0aa100475
SHA256:	9e4f0e0a10a778fb94e7631c17082b44bf75170d7ca81b393574fd3f4c004f47
SHA512:	5599a5eb0bf29de8db3d3177e2a80049101884fe179bdd28d24fd5d61bdcc6132444a8096f530d94c22151731d08d67835dc2a9844eb3764827bef48361be54f
SSDEEP:	12288:XzFouHH1JJ2iNqkejwFGfnH/OE9ZAFAkG1Z/dSzo3Jz4ABQyxh:XCu1j1UeGPHBA4wqJzr/
TLSH:	92E4124162B64F55F0BE03F90AF6921047BA7D16E662E78C5CC72AEF19A1F80C512B73
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M0.....0.."...L.....>... ...`....@.. .....@.....

File Icon

Icon Hash:	ce9c9496e4949c9e

Static PE Info

General

Entrypoint:	0x4a3e1a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xBEFF304D [Fri Jul 17 21:44:45 2071 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
int CCh
int3
int3
int3
int3
cld
aas
xor esi, dword ptr [ebx]
xor esi, dword ptr [ebx]
xor esi, dword ptr [ebx]
add eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], dl
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push ss
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
sub byte ptr [eax+66h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa3dc8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa6000	0x4854	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa3dac	0x1c	.text
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa2050	0xa2200	False	0.9359384035273709	data	7.934508263967678	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x4854	0x4a00	False	0.5450802364864865	data	6.213792802382621	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa6130	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384		
RT_GROUP_ICON	0xaa358	0x14	data		
RT_VERSION	0xaa36c	0x2fc	data		
RT_MANIFEST	0xaa668	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

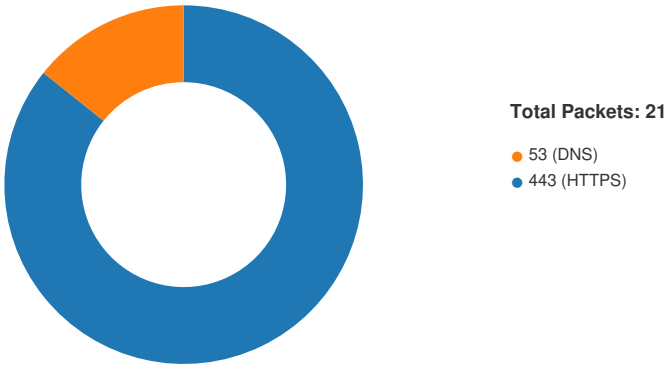
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3149.154.167.220497034432851779 11/03/22-12:21:37.839026	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49703	443	192.168.2.3	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:21:25.394248962 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:25.394336939 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:25.394505978 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:25.438405037 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:25.438488960 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:25.732002020 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:25.732249022 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:25.737373114 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:25.737407923 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:25.737855911 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:25.871424913 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:26.340863943 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:26.340910912 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:26.480662107 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:26.480782986 CET	443	49702	3.220.57.224	192.168.2.3
Nov 3, 2022 12:21:26.480864048 CET	49702	443	192.168.2.3	3.220.57.224

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:21:26.504179955 CET	49702	443	192.168.2.3	3.220.57.224
Nov 3, 2022 12:21:37.714263916 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.714333057 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.714464903 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.715651989 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.715696096 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.786349058 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.786521912 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.791690111 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.791733980 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.792078972 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.795787096 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.795840025 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.834764957 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:37.838870049 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:37.838929892 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:53.483609915 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:53.483799934 CET	443	49703	149.154.167.220	192.168.2.3
Nov 3, 2022 12:21:53.483903885 CET	49703	443	192.168.2.3	149.154.167.220
Nov 3, 2022 12:21:53.484666109 CET	49703	443	192.168.2.3	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:21:25.296978951 CET	49977	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:21:25.315884113 CET	53	49977	8.8.8.8	192.168.2.3
Nov 3, 2022 12:21:25.329701900 CET	57840	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:21:25.348983049 CET	53	57840	8.8.8.8	192.168.2.3
Nov 3, 2022 12:21:37.687520981 CET	57990	53	192.168.2.3	8.8.8.8
Nov 3, 2022 12:21:37.710592985 CET	53	57990	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
Nov 3, 2022 12:21:25.296978951 CET	192.168.2.3	8.8.8.8	0x8663	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.329701900 CET	192.168.2.3	8.8.8.8	0xa62b	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:37.687520981 CET	192.168.2.3	8.8.8.8	0xe0ee	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
Nov 3, 2022 12:21:25.315884113 CET	8.8.8.8	192.168.2.3	0x8663	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:21:25.315884113 CET	8.8.8.8	192.168.2.3	0x8663	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.315884113 CET	8.8.8.8	192.168.2.3	0x8663	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.315884113 CET	8.8.8.8	192.168.2.3	0x8663	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.315884113 CET	8.8.8.8	192.168.2.3	0x8663	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.348983049 CET	8.8.8.8	192.168.2.3	0xa62b	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)	false

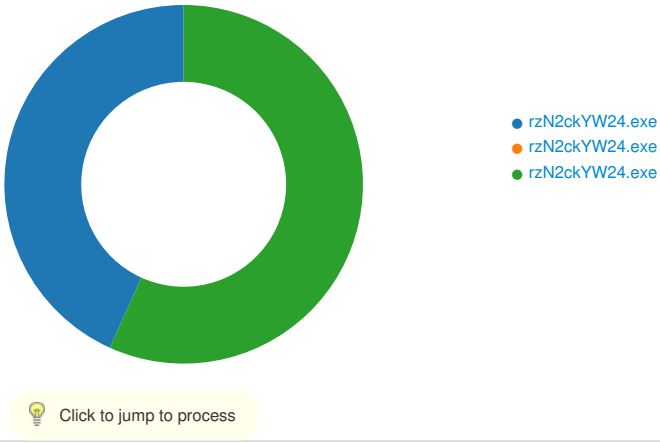
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:21:25.348983049 CET	8.8.8.8	192.168.2.3	0xa62b	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.348983049 CET	8.8.8.8	192.168.2.3	0xa62b	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.348983049 CET	8.8.8.8	192.168.2.3	0xa62b	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:25.348983049 CET	8.8.8.8	192.168.2.3	0xa62b	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:21:37.710592985 CET	8.8.8.8	192.168.2.3	0xe0ee	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: rzN2ckYW24.exe PID: **3044**, Parent PID: **3452**

General

Target ID:	0
Start time:	12:21:03
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\rzN2ckYW24.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rzN2ckYW24.exe
Imagebase:	0x9c0000
File size:	684032 bytes

MD5 hash:	44159444C9BC9980871B80B3AE071FFB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.294910636.0000000002D57000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.293830899.0000000002CB1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.299828968.0000000003D99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.299828968.0000000003D99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.299828968.0000000003D99000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D3ACF06	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	6D3ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rzN2ckYW24.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rzN2ckYW24.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	6D6BC907	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	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D38CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D385705	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

Analysis Process: rzN2ckYW24.exe PID: **6132**, Parent PID: **3044**

General

Target ID:	1
Start time:	12:21:14
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\rzN2ckYW24.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\rzN2ckYW24.exe
Imagebase:	0x170000
File size:	684032 bytes
MD5 hash:	44159444C9BC9980871B80B3AE071FFB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: rzN2ckYW24.exe PID: **6128**, Parent PID: **3044**

General

Target ID:	2
Start time:	12:21:15
Start date:	03/11/2022
Path:	C:\Users\user\Desktop\rzN2ckYW24.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\rzN2ckYW24.exe
Imagebase:	0x470000
File size:	684032 bytes
MD5 hash:	44159444C9BC9980871B80B3AE071FFB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.522788647.0000000002854000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.522788647.0000000002854000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.279572374.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.279572374.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000002.00000000.279572374.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.522385247.0000000002801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3ACF06	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	6D3ACF06	unknown
C:\Users\user\AppData\Local\Temp\tmp4B06.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1F7038	GetTempFileNameW

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	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D385705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D38CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D385705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D385705	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:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C1F1B4F	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	6C1F1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	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

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