ID: 679204
Sample Name: rZ3LaKxraF
Cookbook: default.jbs
Time: 12:01:06
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report rZ3LaKxraF 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Remcos 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Boot Survival 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 11
Public IPs 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rZ3LaKxraF.exe.log 13
C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp 14
C:\Users\user\AppData\Roaming\ohnfNTVBamkg.exe 14
C:\Users\user\AppData\Roaming\vbmcdsb\logs.dat 14
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 17
Sections 18
Resources 18
Imports 18
Network Behavior 18
Snort IDS Alerts 18
TCP Packets 18
Statistics 19
Behavior 19

System Behavior 19
Analysis Process: rZ3LaKxraF.exePID: 6412, Parent PID: 2816 19
General 19
File Activities 20
File Created 20
File Deleted 20
File Written 20
File Read 22
Analysis Process: schtasks.exePID: 6684, Parent PID: 6412 22
General 22
File Activities 23
File Read 23
Analysis Process: conhost.exePID: 6716, Parent PID: 6684 23
General 23
Analysis Process: rZ3LaKxraF.exePID: 6800, Parent PID: 6412 23
General 23
Analysis Process: rZ3LaKxraF.exePID: 6856, Parent PID: 6412 23
General 23
File Activities 24
File Created 24
Registry Activities 24
Key Created 24
Key Value Created 24
Disassembly 24

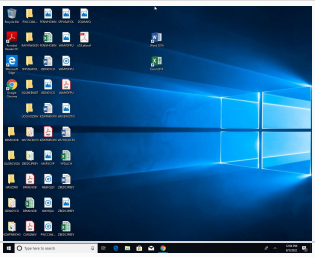
Windows Analysis Report

rZ3LaKxraF

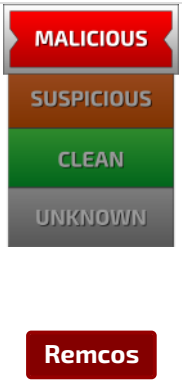
Overview

General Information

Sample Name:	rZ3LaKxraF (renamed file extension from none to exe)
Analysis ID:	679204
MD5:	f8b7ccfaa25ad75..
SHA1:	aae29f7ef62d532.
SHA256:	42638e51cd3eff4..
Tags:	exe RemcosRAT
Infos:	



Detection



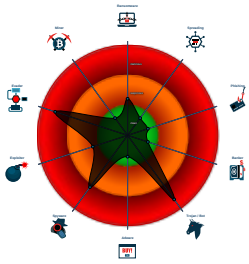
Remcos

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AntiVM3
- Yara detected Remcos RAT
- Antivirus / Scanner detection for sub…
- Detected Remcos RAT
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- rZ3LaKxraF.exe (PID: 6412 cmdline: "C:\Users\user\Desktop\rZ3LaKxraF.exe" MD5: F8B7CCFAA25AD7547501496C248C178E)
  - schtasks.exe (PID: 6684 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ohnfNTVBamkg" /XML "C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - rZ3LaKxraF.exe (PID: 6800 cmdline: {path} MD5: F8B7CCFAA25AD7547501496C248C178E)
  - rZ3LaKxraF.exe (PID: 6856 cmdline: {path} MD5: F8B7CCFAA25AD7547501496C248C178E)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "37.120.210.219:3398:kehinde#2020|",
  "Assigned name": "jd",
  "Connect interval": "5",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "remcos",
  "Hide file": "Disable",
  "Mutex": "remcos_enhatfsgar",
  "Keylog flag": "1",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "1",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screens",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "audio",
  "Connect delay": "0",
  "Copy folder": "remcos",
  "Keylog folder": "vbmcdsb"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.614442968.0000000002AB0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.407920965.0000000004329000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.407920965.0000000004329000.00000004.00000800.00020000.00000000.sdmp	Remcos	detect Remcos in memory	JPCERT/CC Incident Response Group	• 0xb7c8c:$remcos: Remcos • 0xb8500:$remcos: Remcos • 0xb8538:$url: Breaking-Security.Net • 0xbcd42:$resource: SETTINGS
00000007.00000000.399658714.0000000000410000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.404558787.0000000003405000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.rZ3LaKxraF.exe.43cfc58.2.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
0.2.rZ3LaKxraF.exe.43cfc58.2.unpack	INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer	detects Windows exceutables potentially bypassing UAC using eventvwr.exe	ditekSHen	• 0x10738:$s1: \Classes\mscfile\shell\open\command • 0x10720:$s2: eventvwr.exe
0.2.rZ3LaKxraF.exe.43cfc58.2.unpack	Remcos_1	Remcos Payload	kevoreilly	• 0x11034:$name: Remcos • 0x118a8:$name: Remcos • 0x118fb:$name: REMCOS • 0x10688:$time: %02i:%02i:%02i:%03i • 0x11320:$time: %02i:%02i:%02i:%03i • 0x29fc:$crypto: 0F B6 96 08 04 00 00 89 10 8B 45 08 8D 34 07 8B 01 03 C2 8B CB 99 F7 F9 8A 84 95 F4 FB FF F F 30 06 47 3B 7D 0C 72
0.2.rZ3LaKxraF.exe.43cfc58.2.unpack	Remcos	detect Remcos in memory	JPCERT/CC Incident Response Group	• 0x11034:$remcos: Remcos • 0x118a8:$remcos: Remcos • 0x118e0:$url: Breaking-Security.Net • 0x160ea:$resource: SETTINGS

Source	Rule	Description	Author	Strings
0.2.rZ3LaKxraF.exe.43cfc58.2.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x114dc:$funcs1: autogetofflinelogs • 0x114c0:$funcs2: clearlogins • 0x114f0:$funcs3: getofflinelogs • 0x11578:$funcs4: execcom • 0x114cc:$funcs5: deletekeylog • 0x11798:$funcs6: remscriptexecd • 0x115bc:$funcs7: getwindows • 0x10da0:$funcs8: fundlldata • 0x10d78:$funcs9: getfunlib • 0x107ec:$funcs10: autofflinelogs • 0x113b8:$funcs11: getclipboard • 0x114b4:$funcs12: getscrslist • 0x107e0:$funcs13: offlinelogs • 0x105c8:$funcs14: getcamsingleframe • 0x116e4:$funcs15: listfiles • 0x115e0:$funcs16: getproclist • 0x10828:$funcs17: onlinelogs • 0x11700:$funcs18: getdrives • 0x11784:$funcs19: remscriptsuccess • 0x10600:$funcs20: getcamframe • 0x1115c:$str_a1: C:\Windows\System32\cmd.exe
Click to see the 16 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/Remcos RAT Checkin 348 - Source IP: 192.168.2.7 - Destination IP: 37.120.210.219

Timestamp:	192.168.2.737.120.210.2194977433982841134 08/05/22-12:03:58.881678
SID:	2841134
Source Port:	49774
Destination Port:	3398
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Remcos RAT

Remote Access Functionality

Yara detected Remcos RAT

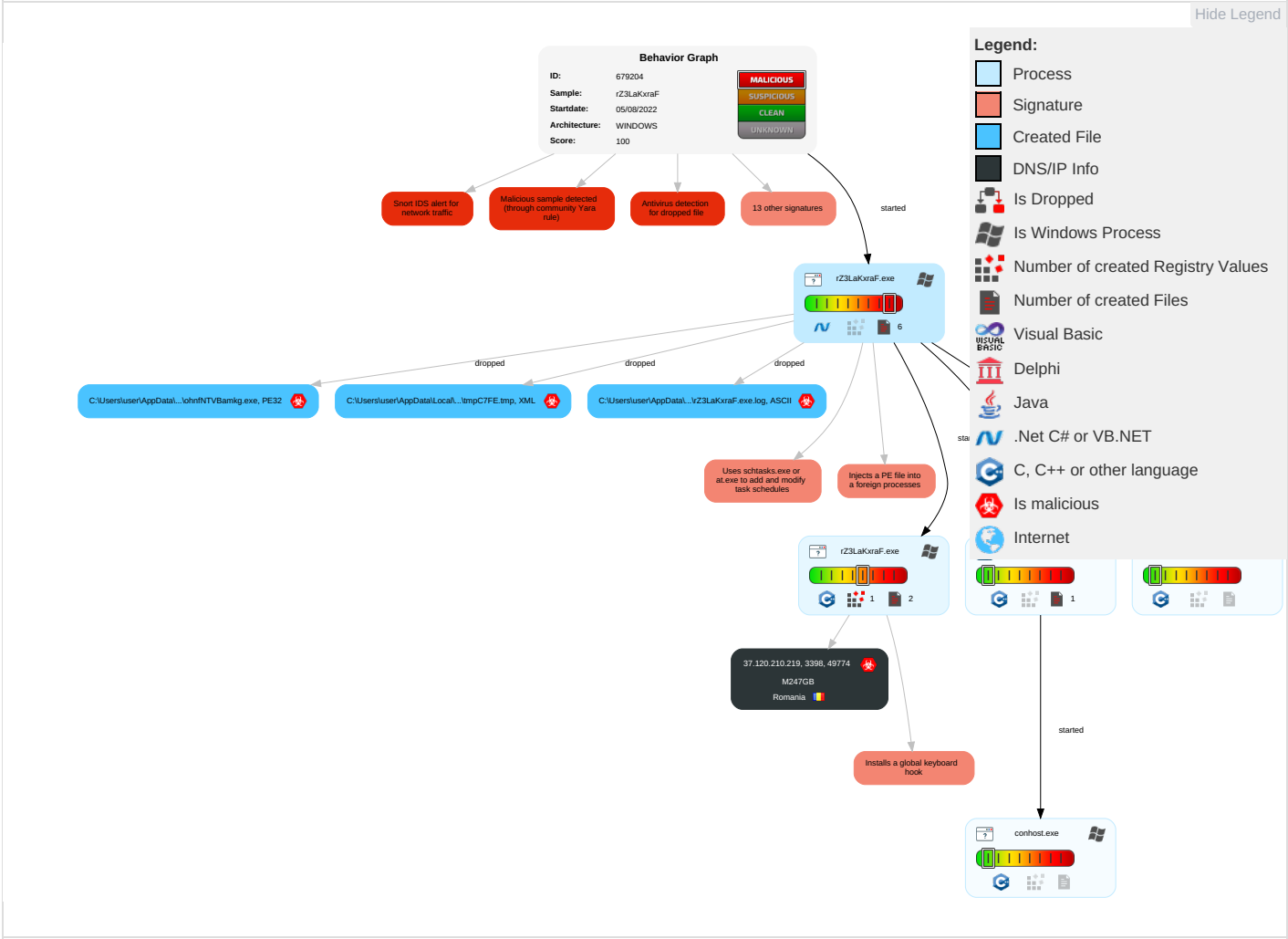
Detected Remcos RAT

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	1 Masquerading	1 1 1 Input Capture	1 Query Registry	Remote Services	1 1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Software Packing	Cached Domain Credentials	1 File and Directory 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 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

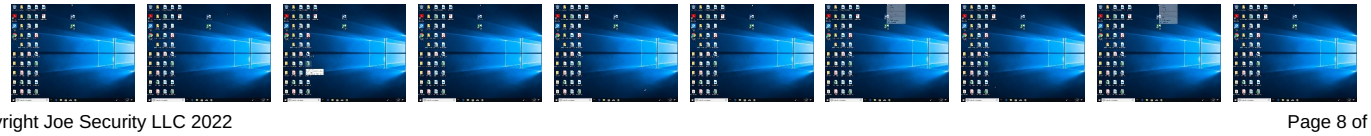
Behavior Graph

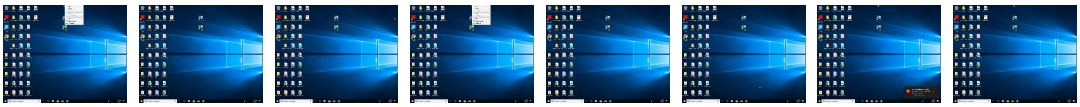


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
rZ3LaKxraF.exe	48%	ReversingLabs	ByteCode-MSIL.Spyware.SnakeLogger	
rZ3LaKxraF.exe	100%	Avira	HEUR/AGEN.1208404	
rZ3LaKxraF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ohnfNTVBamkg.exe	100%	Avira	HEUR/AGEN.1208404	
C:\Users\user\AppData\Roaming\ohnfNTVBamkg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ohnfNTVBamkg.exe	48%	ReversingLabs	ByteCode-MSIL.Spyware.SnakeLogger	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.rZ3LaKxraF.exe.f00000.0.unpack	100%	Avira	HEUR/AGEN.1208404		Download File
7.0.rZ3LaKxraF.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1219514		Download File
0.2.rZ3LaKxraF.exe.43cfc58.2.unpack	100%	Avira	HEUR/AGEN.1219514		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
37.120.210.219	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
37.120.210.219	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	rZ3LaKxraF.exe, 00000000.00000002.404143465.0000000003321000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	rZ3LaKxraF.exe, 00000000.00000002.410661170.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.120.210.219	unknown	Romania		9009	M247GB	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679204
Start date and time: 05/08/202212:01:06	2022-08-05 12:01:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rZ3LaKxraF (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
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@8/4@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.82.210.154
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, arc.trafficmanager.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target rZ3LaKxraF.exe, PID 6856 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: rZ3LaKxraF.exe

Simulations

Behavior and APIs

Time	Type	Description
12:03:08	API Interceptor	808x Sleep call for process: rZ3LaKxraF.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\rZ3LaKxraF.exe.log

Process:	C:\Users\user\Desktop\rZ3LaKxraF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF

SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp

Process:	C:\Users\user\Desktop\rZ3LaKxraF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1661
Entropy (8bit):	5.174023600988245
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1Ntn:cbhH7MlNQ8/rydbz9l3YODOLNdq3v
MD5:	221CE6A07FB67113112AED2562CBF3B3
SHA1:	39FEC1C7C72BB5C740C24412537B4F429486708F
SHA-256:	6B98B72DA3B6BDBDBF83DE716C1D1F8F50D43E71FA28FB262391111289O0F414
SHA-512:	73EB9B348394B3BCB36AC00EC6CC7F636EB45EDB3DDA29682A0A7D943D1BF9BC99B641706DF93C59E61C73EE80C5E7B871956F7AD179C8B8E15964C9D4594 6B
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\ohnfNTVBamkg.exe

Process:	C:\Users\user\Desktop\rZ3LaKxraF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	703488
Entropy (8bit):	6.9630413774878415
Encrypted:	false
SSDEEP:	12288:2u82iNDXR0NSqCGCHw1jZIvNds4mcGrONHhbP7r9r/+pppppppppppppppppppppZ:E1rvqCGCQJZIvoYGoHhb1qH
MD5:	F8B7CCFAA25AD7547501496C248C178E
SHA1:	AAE29F7EF62D5329C27C2040ED573D0DDC9A522E
SHA-256:	42638E51CD3EFF415CE751E700D233596988FD51FFBA584B18DD2E78EC07BC2B
SHA-512:	CBFEC11BA74137DF8A56D8C6CA74A04F3773D52C097AD78A5413733AD8DE540CE8F0BE54A9DCF2A708BBB56A0DAEA69F247BA7255485DE2406ED310B07D91 E44
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 48%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....9.b.....P..\...^.....z.. .....@.. .....@.....@z..O.....h[..... .....H.....text....Z... ...\..... ..`.rsrc...h[.....\...^.....@..@.reloc.....@..B.....tz.....H.....Q..,.....B...HE...4.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+.*.0.....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....,!r...p.....(-...o....s/.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r=..p~....o0...(1.....t$....+..*...0..&.....(....rI..p~....o0...(1.....

C:\Users\user\AppData\Roaming\vbmcdsb\logs.dat

Process:	C:\Users\user\Desktop\rZ3LaKxraF.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	25
Entropy (8bit):	3.593269689515108

Encrypted:	false
SSDEEP:	3:M1XKe3n:0aS
MD5:	89B5667E995FBEB88EDDA0BAC2FD47C4
SHA1:	76FB3FE1E77B0F1A5C6014437515F1DB8EAAEC37
SHA-256:	EE321AE724EA998CADB15526D3573191C892653D28A8AA7DE43413AE2DCE5E79
SHA-512:	F542FC946C29FAECC5D660548B43B1F59C909955FDF162F150426DBB23FDD3CDEFED435254884DBCDACA82529249A7C2C07DC9DC8C5073156056F8A92B28AS F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	...[Program Manager]...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.9630413774878415
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:	rZ3LaKxraF.exe
File size:	703488
MD5:	f8b7ccfaa25ad7547501496c248c178e
SHA1:	aae29f7ef62d5329c27c2040ed573d0ddc9a522e
SHA256:	42638e51cd3eff415ce751e700d233596988fd51ffba584b18dd2e78ec07bc2b
SHA512:	cbfec11ba74137df8a56d8c6ca74a04f3773d52c097ad78a5413733ad8de540ce8f0be54a9dcf2a708bbb56a0daea69f247ba7255485de2406ed310b07d91e44
SSDEEP:	12288:2u82iNDXR0NSqCGCHw1jZIvNds4mcGrONHhbP7r9r/+pppppppppppppppppppppZ:E1rvqCGCQJZIvoYGoHhb1qH
TLSH:	33E48E80E586B664DE19D7745BFACC754533BD6AE838952C28DD3F37BBB7AA20011023
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....9.b.....P..\...^.....z... .....@.. .....@.....

File Icon

Icon Hash:	c4c4c4c8ccd4d0c4

Static PE Info

General

Entrypoint:	0x477a92
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:	0x62DF39AA [Tue Jul 26 00:47:38 2022 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]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x77a40	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x35b68	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
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	0x75a98	0x75c00	False	0.814691563826964	data	7.651863680261729	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x35b68	0x35c00	False	0.21262263808139534	data	4.520503418212817	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	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	0x78460	0x668	data		
RT_ICON	0x78ac8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294965391, next used block 7403512		
RT_ICON	0x78db0	0x1e8	data		
RT_ICON	0x78f98	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x790c0	0x35e0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x7c6a0	0xea8	data		
RT_ICON	0x7d548	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x7ddf0	0x6c8	data		
RT_ICON	0x7e4b8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x7ea20	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x8f248	0x94a8	data		
RT_ICON	0x986f0	0x67e8	data		
RT_ICON	0x9eed8	0x5488	data		
RT_ICON	0xa4360	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 2130706432		
RT_ICON	0xa8588	0x25a8	data		
RT_ICON	0xaab30	0x10a8	data		
RT_ICON	0xabbd8	0x988	data		
RT_ICON	0xac560	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xac9c8	0x102	data		
RT_VERSION	0xacacc	0x354	data		
RT_MANIFEST	0xace20	0xd48	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

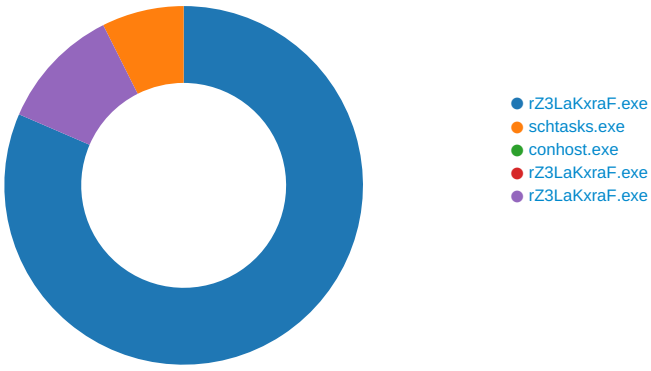
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.737.120.210.2194977433982841134 08/05/22-12:03:58.881678	TCP	2841134	ETPRO TROJAN Win32/Remcos RAT Checkin 348	49774	3398	192.168.2.7	37.120.210.219

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:02:43.141547918 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:02:43.615458965 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:02:43.615602016 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:02:43.616734028 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:02:44.114769936 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:02:44.131412029 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:02:44.652451038 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:02:58.748060942 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:02:58.758995056 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:02:59.282506943 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:03:18.786052942 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:03:18.789299011 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:03:19.304574966 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:03:38.821558952 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:03:38.824368954 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:03:39.342868090 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:03:58.876553059 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:03:58.881678104 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:03:59.401487112 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:04:18.985163927 CEST	3398	49774	37.120.210.219	192.168.2.7
Aug 5, 2022 12:04:18.986965895 CEST	49774	3398	192.168.2.7	37.120.210.219
Aug 5, 2022 12:04:19.506959915 CEST	3398	49774	37.120.210.219	192.168.2.7

Statistics

Behavior



System Behavior

Analysis Process: rZ3LaKxraF.exe PID: **6412**, Parent PID: **2816**

General

Target ID:	0
Start time:	12:02:56
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\rZ3LaKxraF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\rZ3LaKxraF.exe"

Imagebase:	0xf00000
File size:	703488 bytes
MD5 hash:	F8B7CCFAA25AD7547501496C248C178E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.407920965.0000000004329000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Remcos, Description: detect Remcos in memory, Source: 00000000.00000002.407920965.0000000004329000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.404558787.0000000003405000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Remcos, Description: detect Remcos in memory, Source: 00000000.00000002.404558787.0000000003405000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.404143465.0000000003321000.00000004.00000800.00020000.00000000.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	6D03CF06	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	6D03CF06	unknown
C:\Users\user\AppData\Roaming\ohnfNTVBamkg.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BE81E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BE87038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rZ3LaKxraF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D34C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp	success or wait	1	6BE86A95	DeleteFileW

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\Roaming\ohnfNTVBamkg.exe	0	703488	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 39 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 5c 07 00 00 5e 03 00 00 00 00 00 fd 7a 07 00 00 20 00 00 00 fd 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL9bP\^z @ @	success or wait	1	6BE81B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp	0	1661	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </Registrati	success or wait	1	6BE81B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rZ3LaKxraF.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	6D34C907	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	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D015705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CF703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D01CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CF703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CF703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D015705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BE81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BE81B4F	ReadFile
C:\Users\user\Desktop\rZ3LaKxraF.exe	unknown	703488	success or wait	1	6BE81B4F	ReadFile

Analysis Process: schtasks.exe PID: **6684**, Parent PID: **6412**

General

Target ID:	3
Start time:	12:03:16
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ohnfNTVBamkg" /XML "C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp
Imagebase:	0xef0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp	unknown	2	success or wait	1	EFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC7FE.tmp	unknown	1662	success or wait	1	EFABD9	ReadFile

Analysis Process: conhost.exe PID: **6716**, Parent PID: **6684**

General

Target ID:	5
Start time:	12:03:17
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rZ3LaKxraF.exe PID: **6800**, Parent PID: **6412**

General

Target ID:	6
Start time:	12:03:18
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\rZ3LaKxraF.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x290000
File size:	703488 bytes
MD5 hash:	F8B7CCFAA25AD7547501496C248C178E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: rZ3LaKxraF.exe PID: **6856**, Parent PID: **6412**

General

Target ID:	7
Start time:	12:03:19
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\rZ3LaKxraF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x870000
File size:	703488 bytes

MD5 hash:	F8B7CCFAA25AD7547501496C248C178E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000002.614442968.0000000002AB0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000007.00000000.399658714.0000000000410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vbmcdsb	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	407A7F	CreateDirectoryA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\remcos_enhatfsgar\	success or wait	1	408FED	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\remcos_enhatfsgar	EXEpath	unicode	~n.j?..].w.+..."9...*.....b.Gh....w.	success or wait	1	409019	RegSetValueExA

Disassembly

No disassembly