

ID: 694562
Sample Name:
W445hIpF47.exe
Cookbook: default.jbs
Time: 23:52:14
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report W445hIpF47.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Initial Sample 4
Dropped Files 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Spam, unwanted Advertisements and Ransom Demands 6
System Summary 6
Data Obfuscation 6
Boot Survival 7
Malware Analysis System Evasion 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 11
World Map of Contacted 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 14
Created / dropped Files 14
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe 14
Static File Info 14
General 14
File Icon 14
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 16
Data Directories 16
Sections 16
Resources 17
Imports 17
Exports 17
Possible Origin 17
Network Behavior 17
UDP Packets 17
DNS Queries 18
Statistics 18
Behavior 18
System Behavior 19
Analysis Process: W445hIpF47.exePID: 4984, Parent PID: 4180 19
General 19
File Activities 19
File Created 19
File Written 19
File Read 20

Registry Activities 20
Key Value Created 20
Analysis Process: zrnips.exePID: 4940, Parent PID: 3528 20
General 20
File Activities 21
File Read 21
Registry Activities 21
Key Value Created 21
Analysis Process: zrnips.exePID: 4544, Parent PID: 3528 21
General 21
File Activities 22
File Read 22
Registry Activities 22
Key Value Created 22
Analysis Process: zrnips.exePID: 5896, Parent PID: 3528 22
General 22
File Activities 23
File Read 23
Registry Activities 23
Key Value Created 23
Analysis Process: zrnips.exePID: 5612, Parent PID: 3528 23
General 23
File Activities 23
File Read 23
Registry Activities 23
Key Value Created 23
Analysis Process: zrnips.exePID: 6132, Parent PID: 3528 24
General 24
File Activities 24
File Read 24
Registry Activities 24
Key Value Created 24
Analysis Process: zrnips.exePID: 5684, Parent PID: 3528 24
General 24
File Activities 25
File Read 25
Registry Activities 25
Key Value Created 25
Analysis Process: zrnips.exePID: 1792, Parent PID: 3528 25
General 25
File Activities 26
File Read 26
Registry Activities 26
Key Value Created 26
Analysis Process: zrnips.exePID: 4736, Parent PID: 3528 26
General 26
Analysis Process: zrnips.exePID: 856, Parent PID: 3528 26
General 26
File Activities 27
File Read 27
Registry Activities 27
Key Value Created 27
Analysis Process: zrnips.exePID: 4888, Parent PID: 3528 27
General 27
Analysis Process: zrnips.exePID: 5408, Parent PID: 3528 28
General 28
Analysis Process: zrnips.exePID: 4724, Parent PID: 3528 28
General 28
Disassembly 29

Copyright Joe Security LLC 2022

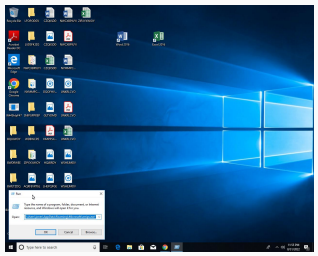
Windows Analysis Report

W445hIpF47.exe

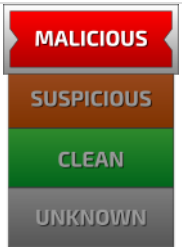
Overview

General Information

Sample Name:	W445hIpF47.exe
Analysis ID:	694562
MD5:	379af253605407..
SHA1:	ca8717ffb9b80a9..
SHA256:	15bfead5bee24b..
Tags:	exe
Infos:	



Detection



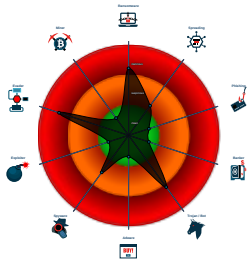
Gandcrab, ReflectiveLoader

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

Signatures

- Yara detected Gandcrab
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected ReflectiveLoader
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Creates multiple autostart registry k…
- Found evasive API chain (may stop…
- Contains functionality to determine t…
- Found Tor onion address
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- W445hIpF47.exe (PID: 4984 cmdline: "C:\Users\user\Desktop\W445hIpF47.exe" MD5: 379AF2536054073F63E7F45D80963BB4)
- zrnips.exe (PID: 4940 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 4544 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 5896 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 5612 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 6132 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 5684 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 1792 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 4736 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 856 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 4888 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 5408 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- zrnips.exe (PID: 4724 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe" MD5: 9560C1D27C69870E70DD78A19C8FE473)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
W445hIpF47.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
W445hIpF47.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
W445hIpF47.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
W445hIpF47.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
W445hIpF47.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.462969629.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000007.00000002.409239995.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000005.00000002.385384409.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000014.00000000.533542900.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000011.00000002.488096195.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
Click to see the 125 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.zrnips.exe.3960000.0.raw.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
5.3.zrnips.exe.3960000.0.raw.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
5.3.zrnips.exe.3960000.0.raw.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
5.3.zrnips.exe.3960000.0.raw.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
5.3.zrnips.exe.3960000.0.raw.unpack	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
Click to see the 294 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Contains functionality to determine the online IP of the system

Found Tor onion address

May check the online IP address of the machine

Spam, unwanted Advertisements and Ransom Demands



Yara detected Gandcrab

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Yara detected ReflectiveLoader

Copyright Joe Security LLC 2022

Boot Survival



Creates multiple autostart registry keys

Malware Analysis System Evasion

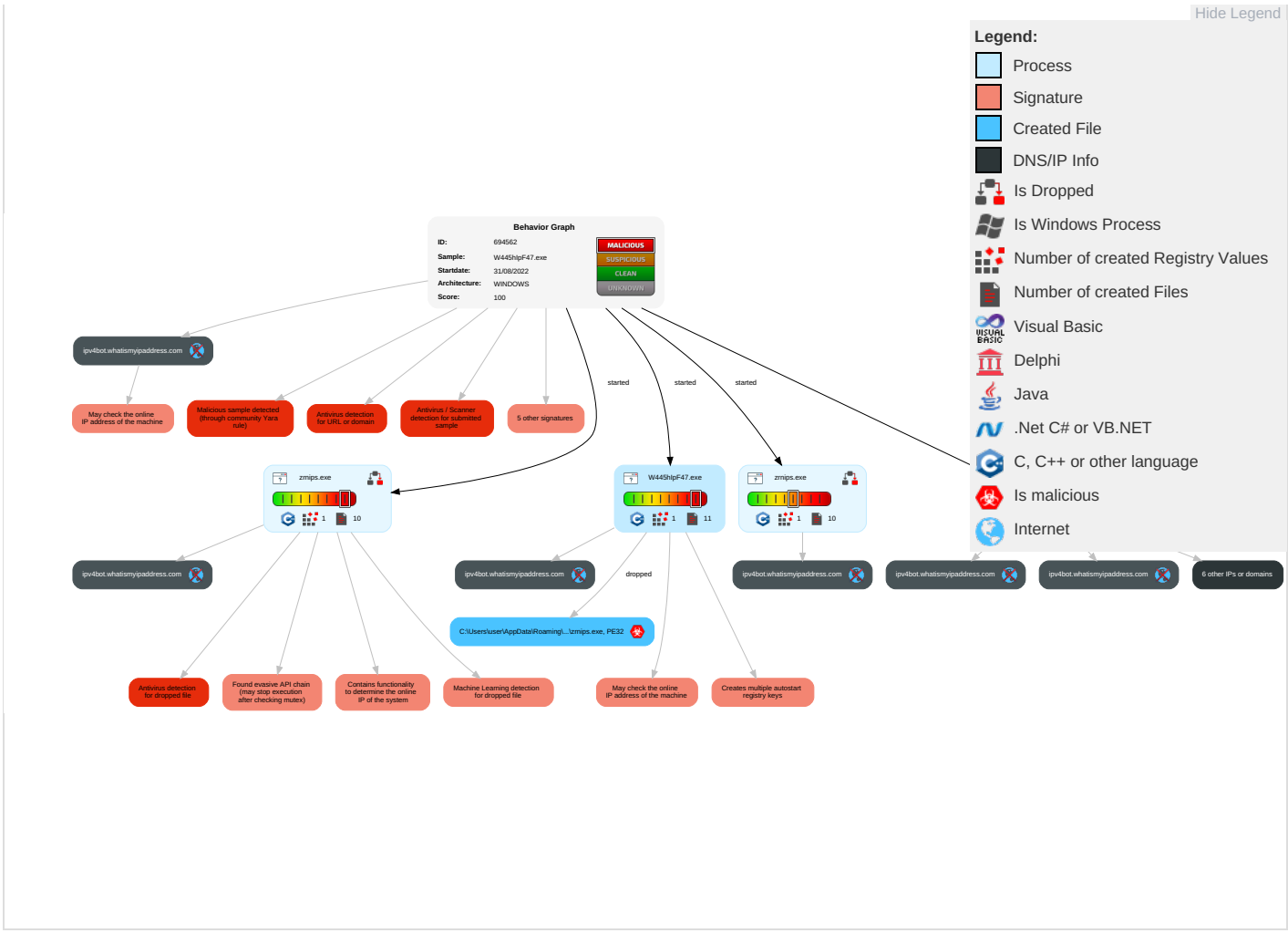


Found evasive API chain (may stop execution after checking mutex)

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
1 Replication Through Removable Media	1 1 Native API	1 1 Registry Run Keys / Startup Folder	1 Process Injection	1 Masquerading	1 Input Capture	1 Query Registry	1 Replication Through Removable Media	1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Data Encrypted for Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Process Injection	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	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)	1 Software Packing	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 1 Peripheral Device Discovery	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	Software Packing	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Proxy	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 File and Directory Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	4 4 System Information Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

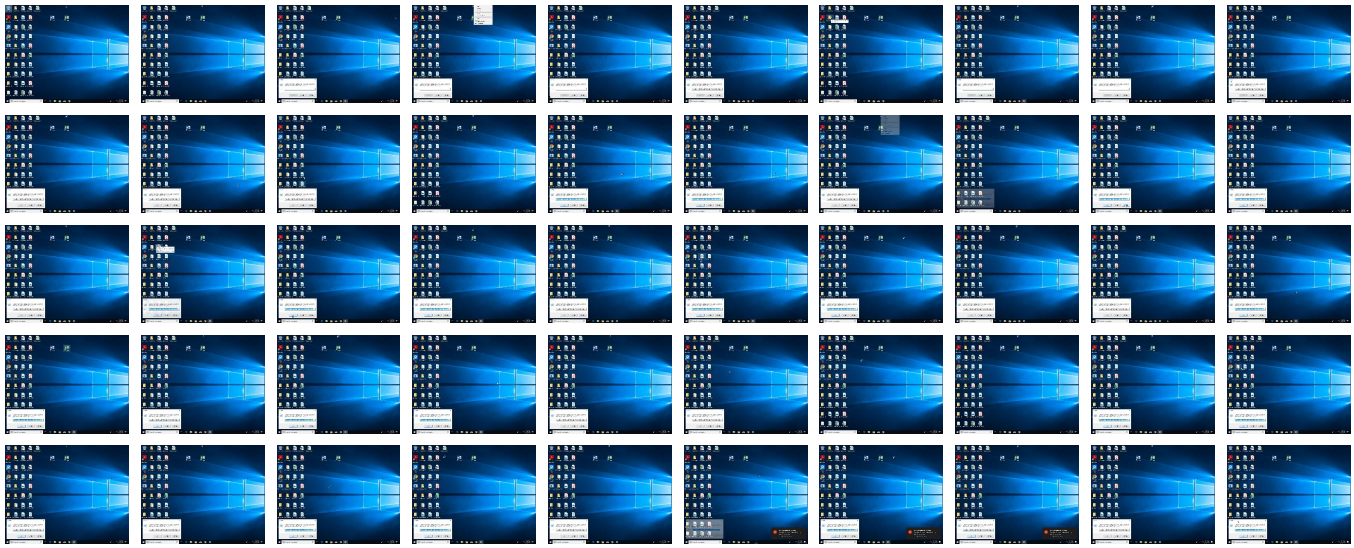
Behavior Graph



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
W445hlpF47.exe	74%	Metadefender		Browse
W445hlpF47.exe	97%	ReversingLabs	Win32.Ransomware.GandCrab	
W445hlpF47.exe	100%	Avira	TR/Dropper.Gen	
W445hlpF47.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.0.W445hlpF47.exe.fda0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.3.zrnips.exe.3240000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
5.3.zrnips.exe.3960000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
23.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.3.zrnips.exe.3ca0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
19.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.3.W445hlpF47.exe.3750000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.3.zrnips.exe.2f20000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.3.zrnips.exe.3d60000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
23.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.3.zrnips.exe.36c0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.zrnips.exe.3170000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.3.zrnips.exe.3990000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.3.zrnips.exe.34a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.2.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.2.W445hlpF47.exe.fda0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.3.zrnips.exe.3a10000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
17.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.0.zrnips.exe.fcd0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gdcbmuveqjsli57x.onion/1cd33ea6922904b9	100%	Avira URL Cloud	malware	
http://https://tox.chat/download.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipv4bot.whatismyipaddress.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://gdcbmuveqjsli57x.onion/1cd33ea6922904b9	W445hIpF47.exe, 00000001.00000002.335771276.000000000FDB2000.00000004.00000001.01000000.00000003.sdmp, zrnips.exe, 00000003.00000002.369749852.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000005.00000002.385384409.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000007.00000002.409249887.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000008.00000002.425172336.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000C.00000002.447997228.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000D.00000002.462969629.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000F.00000002.490894450.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000013.00000002.522593346.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000014.00000002.547774907.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000017.00000002.576290248.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.torproject.org/	W445hIpF47.exe, 00000001.00000002.335771276.000000000FDB2000.00000004.00000001.01000000.00000003.sdmp, zrnips.exe, 00000003.00000002.369749852.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000005.00000002.385384409.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000007.00000002.409249887.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000008.00000002.425172336.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000C.00000002.447997228.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000D.00000002.462969629.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000F.00000002.490894450.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000013.00000002.522593346.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000014.00000002.547774907.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000017.00000002.576290248.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/	zrnips.exe, 00000003.00000002.369371671.0000000000D8A000.00000004.00000020.00020000.00000000.sdmp, zrnips.exe, 0000000D.00000002.462566765.0000000000C68000.00000004.00000020.00020000.00000000.sdmp, zrnips.exe, 00000017.00000002.575488485.00000000011D4000.00000004.00000020.00020000.00000000.sdmp, zrnips.exe, 00000017.00000002.575403448.0000000001198000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/75	zrnips.exe, 00000017.00000002.575403448.0000000001198000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tox.chat/download.html	W445hIpF47.exe, 00000001.00000002.335771276.000000000FDB2000.00000004.00000001.01000000.00000003.sdmp, zrnips.exe, 00000003.00000002.369749852.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000005.00000002.385384409.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000007.00000002.409249887.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000008.00000002.425172336.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000C.00000002.447997228.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000D.00000002.462969629.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 0000000F.00000002.490894450.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000013.00000002.522593346.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000014.00000002.547774907.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, zrnips.exe, 00000017.00000002.576290248.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694562
Start date and time:	2022-08-31 23:52:14 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	W445hIpF47.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@13/1@12/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99% (good quality ratio 95.1%) • Quality average: 83.3% • Quality standard deviation: 24.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Copyright Joe Security LLC 2022

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.82.228.9
- Excluded domains from analysis (whitelisted): rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, neus2c-displaycatalog.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: W445hIpF47.exe

Simulations

Behavior and APIs

Time	Type	Description
23:53:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce oikgjamwdag "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:53:30	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce oikgjamwdag "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:53:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce vlujgxdarml "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:53:50	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce icyakbwwtkt "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:53:59	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce vcvvgrlytwo "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:54:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce fnwitigtrzg "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:54:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce jxyyakggfhw "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:54:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce pufpoqlopxk "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:54:33	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce gwocugdvyyi "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:54:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce vlujgxdarml "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:54:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce icyakbwwtkt "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:55:03	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce vcvvgrlytwo "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:55:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce fnwitigtrzg "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
23:55:20	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce jxyyakggfhw "C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"

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\Roaming\Microsoft\zrnips.exe

Process:	C:\Users\user\Desktop\W445hIpF47.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	71680
Entropy (8bit):	6.490137598305917
Encrypted:	false
SSDEEP:	1536:wZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:/d5BJHMqqDL2/Ovvdr
MD5:	9560C1D27C69870E70DD78A19C8FE473
SHA1:	6ECB41C480469733814619 95BC35D590668AAF3A
SHA-256:	FEEEAA9486096A2ECCC13C646D7FA7125D1FD7AFA7F66617037740E02BF3FAAB
SHA-512:	F4AA1DA9C32F290FB9C39831B1E8065168CF3EDFAE8A9D72D1C5BA752B80825CFC2B6B3D7A4487123756BE87E1D112BEB624B314EF2B1F2B626C2DFC8294C6DB
Malicious:	**true**
Yara Hits:	• Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This V.4.(.m cannot be run in DOS mode....$.....}.....B.....B.....1.....Y...G.....~.....y.....|....Rich..... ...PE..L....6.Z..... K.....Z..... ....@.....P...U.....@.....P..... ..text...H..... ..`.rdata..&q.....r.....@..@.data..... .....@....CRT.....0.....@..@.rsrc.....@.....@..@.reloc.....P..... .....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.490113861759907
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	W445hIpF47.exe
File size:	71680
MD5:	379af2536054073f63e7f45d80963bb4
SHA1:	ca8717ffb9b80a979116ebbb676dfecd0ec73c8f
SHA256:	15bfead5bee24b7c1d0104bb04e72bf5d735ee2a9416ba3ab43ecf296613b391
SHA512:	3046e5907f882ce472d95ac46368fc3c1243ff15fd175c32a20600ce0890225b662003a921ccc2b79bb312c3c51b48fcbdf708cca85dd9374af27fdb20412e74
SSDEEP:	1536:XZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:+d5BJHMqqDL2/Ovvdr
TLSH:	86636C1DB2D1B293F1E396B9FAB57E25445D2D103B056BEB08A369F568220F16C3B703
File Content Preview:	MZ.....@.....!..L.!This {v..p.m cannot be run in DOS mode....$.....}.....B.....B.....1.....Y.....G.....~.....y.....|.....Rich.....PE..L..

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x10004b20
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH
Time Stamp:	0x5A9C3687 [Sun Mar 4 18:10:15 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	8735e6cad23590d9b5b60978db488a28

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 4Ch
push 000003E8h
call dword ptr [1000A098h]
call 00007FCA14E9017Fh
test eax, eax
je 00007FCA14E904EAh
push 00000000h
call dword ptr [1000A168h]
push 00000000h
push 00000000h
push 00000000h
push 10002D30h
push 00000000h
push 00000000h
call dword ptr [1000A108h]
mov dword ptr [ebp-04h], eax
cmp dword ptr [ebp-04h], 00000000h
je 00007FCA14E9050Eh
push 00001388h
mov eax, dword ptr [ebp-04h]
push eax
call dword ptr [1000A080h]
cmp eax, 00000102h
jne 00007FCA14E904EEh
push 00000000h
mov ecx, dword ptr [ebp-04h]
push ecx
call dword ptr [1000A094h]
mov edx, dword ptr [ebp-04h]
push edx

Instruction
call dword ptr [1000A10Ch]
call 00007FCA14E90214h
call 00007FCA14E8FBFFh
lea ecx, dword ptr [ebp-4Ch]
call 00007FCA14E91E97h
mov dword ptr [ebp-24h], 00000000h
mov dword ptr [ebp-20h], 00000000h
mov dword ptr [ebp-18h], 00000000h
mov dword ptr [ebp-28h], 00000000h
lea eax, dword ptr [ebp-20h]
push eax
lea ecx, dword ptr [ebp-24h]
push ecx
lea edx, dword ptr [ebp-28h]
push edx
lea eax, dword ptr [ebp-18h]
push eax
lea ecx, dword ptr [ebp-4Ch]
call 00007FCA14E91E13h
mov dword ptr [ebp-2Ch], 00000000h
mov dword ptr [ebp-0Ch], 00000000h
mov ecx, dword ptr [ebp-18h]
call 00007FCA14E903FDh

Rich Headers

Programming Language:	• [C] VS2013 build 21005 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2013 build 21005 • [RES] VS2013 build 21005 • [LNK] VS2013 build 21005

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x10550	0x55	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x105a8	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x15000	0xaf4	.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	0xa000	0x200	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8448	0x8600	False	0.4546991604477612	data	6.32052618210059	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0x7126	0x7200	False	0.4776589912280701 5	data	6.1644872822657275	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x12000	0xa84	0xc00	False	0.3056640625	data	3.538638851099626	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.CRT	0x13000	0x4	0x200	False	0.033203125	data	0.04078075625387198	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1e0	0x200	False	0.52734375	data	4.7176788329467545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x15000	0xaf4	0xc00	False	0.7932942708333334	data	6.537931848954439	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x14060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	ReadFile, SetFilePointer, GetFileAttributesW, GetLastError, MoveFileW, lstrcpyW, SetFileAttributesW, CreateMutexW, GetDriveTypeW, VerSetConditionMask, WaitForSingleObject, GetTickCount, InitializeCriticalSection, OpenProcess, GetSystemDirectoryW, TerminateThread, Sleep, TerminateProcess, VerifyVersionInfoW, WaitForMultipleObjects, DeleteCriticalSection, ExpandEnvironmentStringsW, lstrlenW, SetHandleInformation, lstrcatA, MultiByteToWideChar, CreatePipe, lstrcmpiA, Process32NextW, CreateToolhelp32Snapshot, LeaveCriticalSection, EnterCriticalSection, FindFirstFileW, lstrcmpW, FindClose, FindNextFileW, GetNativeSystemInfo, GetComputerNameW, GetDiskFreeSpaceW, GetWindowsDirectoryW, GetVolumeInformationW, LoadLibraryA, lstrcmpiW, VirtualFree, CreateThread, CloseHandle, lstrcatW, CreateFileMappingW, ExitThread, CreateFileW, GetModuleFileNameW, WriteFile, GetModuleHandleW, UnmapViewOfFile, MapViewOfFile, GetFileSize, GetEnvironmentVariableW, lstrcpyA, GetModuleHandleA, VirtualAlloc, GetProcAddress, Process32FirstW, GetTempPathW, GetProcessHeap, HeapFree, HeapAlloc, lstrlenA, CreateProcessW, ExitProcess, IsProcessorFeaturePresent
USER32.dll	BeginPaint, wsprintfW, TranslateMessage, LoadCursorW, LoadIconW, MessageBoxA, GetMessageW, EndPaint, DestroyWindow, RegisterClassExW, ShowWindow, CreateWindowExW, SendMessageW, DispatchMessageW, DefWindowProcW, UpdateWindow, wsprintfA, GetForegroundWindow, SetWindowLongW
GDI32.dll	TextOutW
ADVAPI32.dll	FreeSid, RegSetValueExW, RegCreateKeyExW, RegCloseKey, CryptExportKey, CryptAcquireContextW, CryptGetKeyParam, CryptReleaseContext, CryptImportKey, CryptEncrypt, CryptGenKey, CryptDestroyKey, GetUserNameW, RegQueryValueExW, RegOpenKeyExW, AllocateAndInitializeSid
SHELL32.dll	ShellExecuteW, SHGetSpecialFolderPathW, ShellExecuteExW
CRYPT32.dll	CryptStringToBinaryA, CryptBinaryToStringA
WININET.dll	InternetCloseHandle, HttpAddRequestHeadersW, HttpSendRequestW, InternetConnectW, HttpOpenRequestW, InternetOpenW, InternetReadFile
PSAPI.DLL	EnumDeviceDrivers, GetDeviceDriverBaseNameW

Exports

Name	Ordinal	Address
_ReflectiveLoader@0	1	0x10005ff0

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:53:23.396292925 CEST	56807	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:53:23.415654898 CEST	53	56807	8.8.8.8	192.168.2.4
Aug 31, 2022 23:53:39.384253025 CEST	61007	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:53:39.404722929 CEST	53	61007	8.8.8.8	192.168.2.4
Aug 31, 2022 23:53:46.596919060 CEST	61124	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:53:46.616827965 CEST	53	61124	8.8.8.8	192.168.2.4
Aug 31, 2022 23:53:57.822163105 CEST	59444	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:53:57.841733932 CEST	53	59444	8.8.8.8	192.168.2.4
Aug 31, 2022 23:54:05.162791014 CEST	59446	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:54:05.180521011 CEST	53	59446	8.8.8.8	192.168.2.4
Aug 31, 2022 23:54:15.519988060 CEST	61088	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:54:15.537431955 CEST	53	61088	8.8.8.8	192.168.2.4
Aug 31, 2022 23:54:22.834369898 CEST	58729	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:54:22.852421045 CEST	53	58729	8.8.8.8	192.168.2.4
Aug 31, 2022 23:54:35.832240105 CEST	64700	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:54:35.849760056 CEST	53	64700	8.8.8.8	192.168.2.4
Aug 31, 2022 23:54:50.327919006 CEST	56022	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:54:50.345698118 CEST	53	56022	8.8.8.8	192.168.2.4
Aug 31, 2022 23:55:02.226505995 CEST	60822	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:55:02.256041050 CEST	53	60822	8.8.8.8	192.168.2.4
Aug 31, 2022 23:55:15.291393042 CEST	49750	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:55:15.310765982 CEST	53	49750	8.8.8.8	192.168.2.4
Aug 31, 2022 23:55:23.649331093 CEST	51054	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:55:23.666527033 CEST	53	51054	8.8.8.8	192.168.2.4

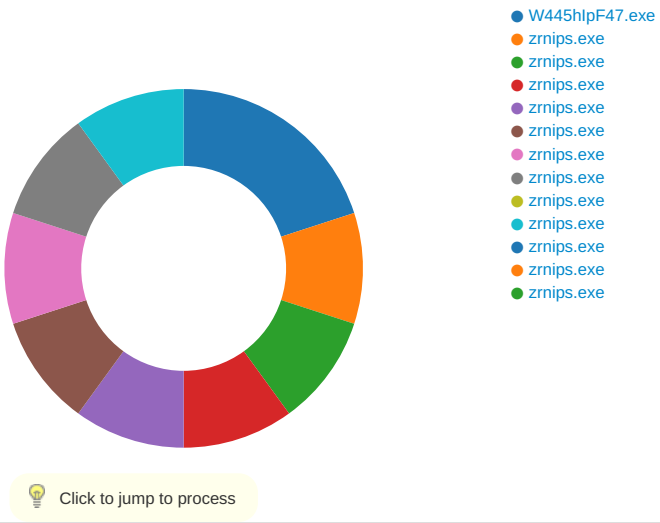
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:53:23.396292925 CEST	192.168.2.4	8.8.8.8	0x3a9b	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:39.384253025 CEST	192.168.2.4	8.8.8.8	0x9d16	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:46.596919060 CEST	192.168.2.4	8.8.8.8	0xc9d3	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:53:57.822163105 CEST	192.168.2.4	8.8.8.8	0xc391	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:05.162791014 CEST	192.168.2.4	8.8.8.8	0x1496	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:15.519988060 CEST	192.168.2.4	8.8.8.8	0xc381	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:22.834369898 CEST	192.168.2.4	8.8.8.8	0x3ae	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:35.832240105 CEST	192.168.2.4	8.8.8.8	0x2d2	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:54:50.327919006 CEST	192.168.2.4	8.8.8.8	0xfbe8	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:55:02.226505995 CEST	192.168.2.4	8.8.8.8	0x70e7	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:55:15.291393042 CEST	192.168.2.4	8.8.8.8	0x7f1	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:55:23.649331093 CEST	192.168.2.4	8.8.8.8	0x765a	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)

Statistics

Behavior

Copyright Joe Security LLC 2022



System Behavior

Analysis Process: W445hIpF47.exe PID: 4984, Parent PID: 4180

General

Target ID:	1
Start time:	23:53:14
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\W445hIpF47.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\W445hIpF47.exe"
Imagebase:	0xfda0000
File size:	71680 bytes
MD5 hash:	379AF2536054073F63E7F45D80963BB4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000001.00000002.335771276.000000000FDB2000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000001.00000000.316448392.000000000FDAA000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000001.00000003.334801749.0000000003750000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000001.00000003.334801749.0000000003750000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000001.00000003.334801749.0000000003750000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000001.00000003.334801749.0000000003750000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000001.00000003.334801749.0000000003750000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000001.00000003.334801749.0000000003750000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000001.00000002.335764679.000000000FDAA000.00000002.00000001.01000000.00000003.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\Microsoft\zrnips.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	FDA2852	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe	0	71680	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

Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000002.369680264.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000000.355052836.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000003.00000002.369749852.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000003.00000003.369063842.00000000034A0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000003.00000003.369063842.00000000034A0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000003.00000003.369063842.00000000034A0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000003.00000003.369063842.00000000034A0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000003.00000003.369063842.00000000034A0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000003.00000003.369063842.00000000034A0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe, Author: ReversingLabs
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	vlujgxdarml	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **4544**, Parent PID: **3528**

General

Target ID:	5
Start time:	23:53:41
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000005.00000002.385384409.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000005.00000003.384531740.0000000003960000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000005.00000003.384531740.0000000003960000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000005.00000003.384531740.0000000003960000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000005.00000003.384531740.0000000003960000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000005.00000003.384531740.0000000003960000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000005.00000003.384531740.0000000003960000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000005.00000000.373648417.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000005.00000002.385364580.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	icyakbwwtkt	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **5896**, Parent PID: **3528**

General

Target ID:	7
Start time:	23:53:50
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000007.00000002.409239995.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000007.00000003.408576390.0000000003990000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000007.00000003.408576390.0000000003990000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000007.00000003.408576390.0000000003990000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000007.00000003.408576390.0000000003990000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000007.00000003.408576390.0000000003990000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000007.00000003.408576390.0000000003990000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000007.00000002.409249887.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000007.00000000.394503180.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	vcvvgrlytwo	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **5612**, Parent PID: **3528**

General

Target ID:	8
Start time:	23:53:59
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000008.00000002.425162740.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000008.00000003.424307564.0000000003CA0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000008.00000003.424307564.0000000003CA0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000008.00000003.424307564.0000000003CA0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000008.00000003.424307564.0000000003CA0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000008.00000003.424307564.0000000003CA0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000008.00000003.424307564.0000000003CA0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000008.00000000.412718126.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000008.00000002.425172336.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	fnwitigtrzg	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **6132**, Parent PID: **3528**

General

Target ID:	12
Start time:	23:54:07
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000002.447982065.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000C.00000002.447997228.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000000.432379853.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000000C.00000003.446505391.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000C.00000003.446505391.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000003.446505391.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000C.00000003.446505391.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000C.00000003.446505391.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000C.00000003.446505391.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	jxyyakggfhw	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **5684**, Parent PID: **3528**

General

Target ID:	13
Start time:	23:54:16
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000D.00000002.462969629.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000D.00000000.449764265.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000000D.00000003.462209860.0000000003240000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000D.00000003.462209860.0000000003240000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000D.00000003.462209860.0000000003240000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000D.00000003.462209860.0000000003240000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000D.00000003.462209860.0000000003240000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000D.00000003.462209860.0000000003240000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000D.00000002.462959628.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	pufpoqlopxk	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **1792**, Parent PID: **3528**

General

Target ID:	15
Start time:	23:54:24
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000002.490875423.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 0000000F.00000003.490038612.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000F.00000003.490038612.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000003.490038612.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000F.00000003.490038612.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000F.00000003.490038612.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000F.00000003.490038612.0000000002F20000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000F.00000002.490894450.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000000.467464358.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	gwocugdvyyi	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **4736**, Parent PID: **3528**

General

Target ID:	17
Start time:	23:54:33
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000011.00000002.488096195.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000011.00000000.485191831.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: zrnips.exe PID: **856**, Parent PID: **3528**

General

Target ID:	19
Start time:	23:54:41
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000013.00000003.521241668.00000000036C0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000013.00000003.521241668.00000000036C0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000003.521241668.00000000036C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000013.00000003.521241668.00000000036C0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000013.00000003.521241668.00000000036C0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000013.00000003.521241668.00000000036C0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000000.503181846.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000013.00000002.522593346.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000002.522576271.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

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\Roaming\Microsoft\zrnips.exe	unknown	71680	success or wait	1	FCD3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	ldtrmpohtby	unicode	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"	success or wait	1	FCD2AAA	RegSetValueExW

Analysis Process: zrnips.exe PID: **4888**, Parent PID: **3528**

General

Target ID:	20
Start time:	23:54:55
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000014.00000000.533542900.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000014.00000003.546628326.0000000003D60000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000014.00000003.546628326.0000000003D60000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000014.00000003.546628326.0000000003D60000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000014.00000003.546628326.0000000003D60000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000014.00000003.546628326.0000000003D60000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000014.00000003.546628326.0000000003D60000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000014.00000002.547763801.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000014.00000002.547774907.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: zrnips.exe PID: **5408**, Parent PID: **3528**

General

Target ID:	23
Start time:	23:55:03
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000017.00000002.576268980.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000017.00000000.551633083.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: ReflectiveLoader, Description: Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended, Source: 00000017.00000003.574625963.0000000003A10000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000017.00000003.574625963.0000000003A10000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000017.00000003.574625963.0000000003A10000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000017.00000003.574625963.0000000003A10000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000017.00000003.574625963.0000000003A10000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000017.00000003.574625963.0000000003A10000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000017.00000002.576290248.000000000FCE2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: zrnips.exe PID: **4724**, Parent PID: **3528**

General

Target ID:	25
Start time:	23:55:12
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\zrnips.exe"
Imagebase:	0xfcd0000
File size:	71680 bytes
MD5 hash:	9560C1D27C69870E70DD78A19C8FE473
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000002.573322590.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000000.568967780.000000000FCDA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly