ID: 694572
Sample Name: mPNVrHIpyt.exe
Cookbook: default.jbs
Time: 00:06:24
Date: 01/09/2022
Version: 35.0.0 Citrine

Table of Contents

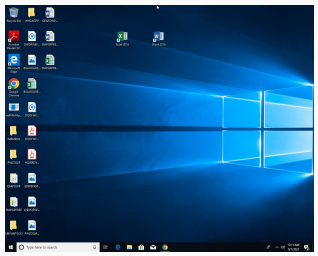
Windows Analysis Report

mPNVrHIpyt.exe

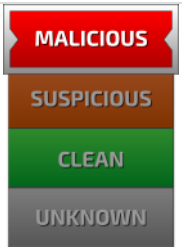
Overview

General Information

Sample Name:	mPNVrHIpyt.exe
Analysis ID:	694572
MD5:	cc7ae6e4c86f60…
SHA1:	8c7c23c91ccecf…
SHA256:	95427e787bb623.
Tags:	exe GandCrab
Infos:	



Detection



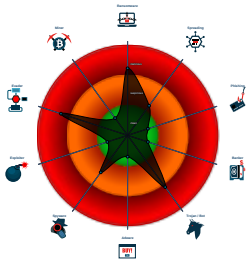
Gandcrab, ReflectiveLoader

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…
- Contains functionality to determine t…
- Found Tor onion address
- Machine Learning detection for sam…
- May check the online IP address of…

Classification



Process Tree

- **System is w10x64**
- mPNVrHIpyt.exe (PID: 3592 cmdline: "C:\Users\user\Desktop\mPNVrHIpyt.exe" MD5: CC7AE6E4C86F605AAB66FBD04EEF7997)
- wzltxa.exe (PID: 1276 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 1920 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 4616 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 6136 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 1356 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 2996 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 6016 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 5520 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 2228 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 6128 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 5752 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 2156 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 5248 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 4920 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 1200 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- wzltxa.exe (PID: 5280 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe" MD5: EAC223A7EC1CF2E33BE569DB14A87A63)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
mPNVrHIpyt.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
mPNVrHIpyt.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
mPNVrHIpyt.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
mPNVrHIpyt.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
mPNVrHIpyt.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$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\wzltxa.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$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
0000001F.00000000.523518226.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000012.00000002.407272016.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
0000000B.00000000.302743243.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000019.00000002.471339306.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
00000022.00000000.561698093.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
Click to see the 150 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
33.2.wzltxa.exe.fbb0000.0.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

Source	Rule	Description	Author	Strings
33.2.wzltxa.exe.fbb0000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
33.2.wzltxa.exe.fbb0000.0.unpack	JoeSecurity_Gandcrab	Yara detected Gandcrab	Joe Security	
33.2.wzltxa.exe.fbb0000.0.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
33.2.wzltxa.exe.fbb0000.0.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
Click to see the 355 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

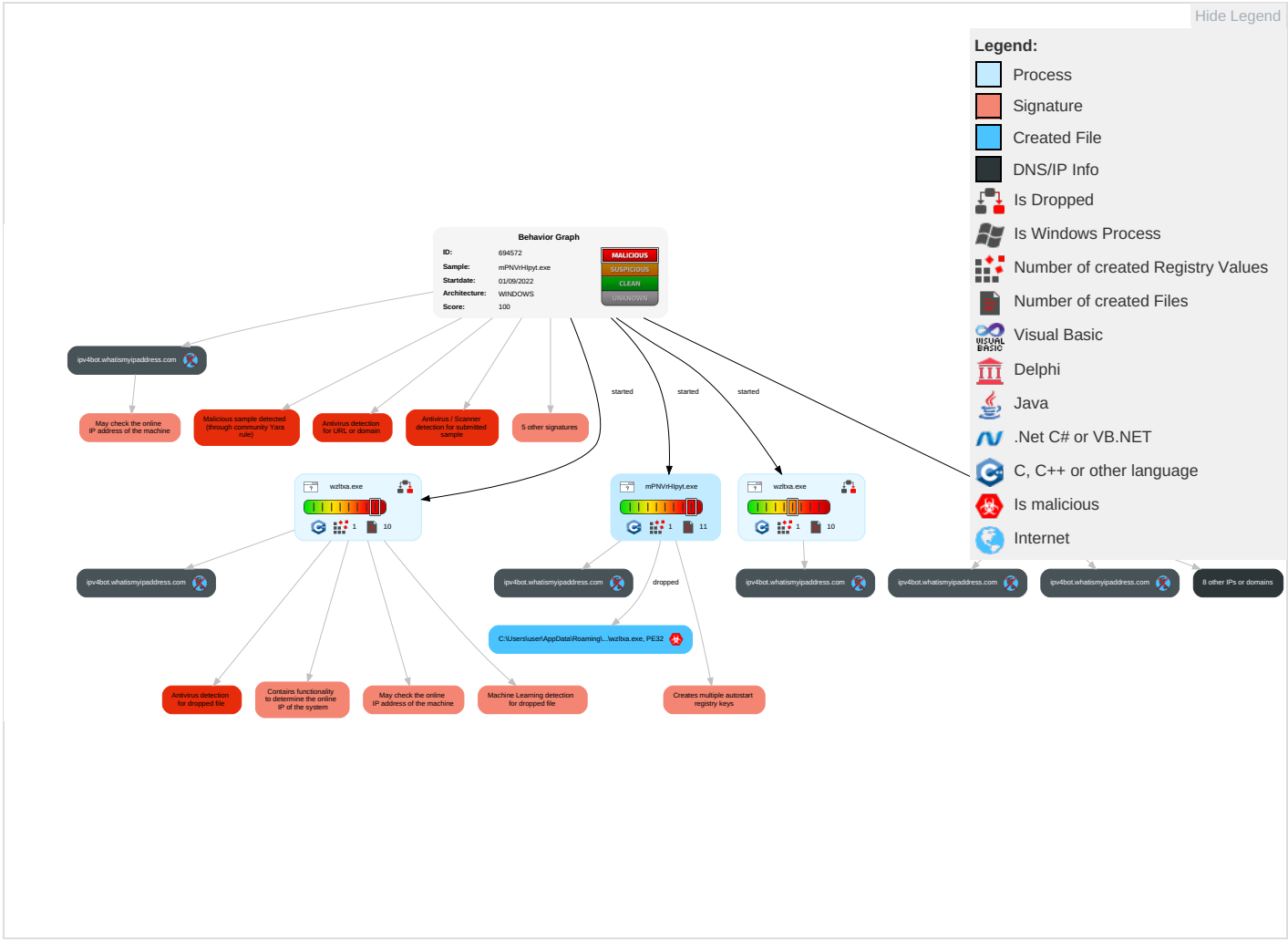
Yara detected ReflectiveLoader

Creates multiple autostart registry keys

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 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	2 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

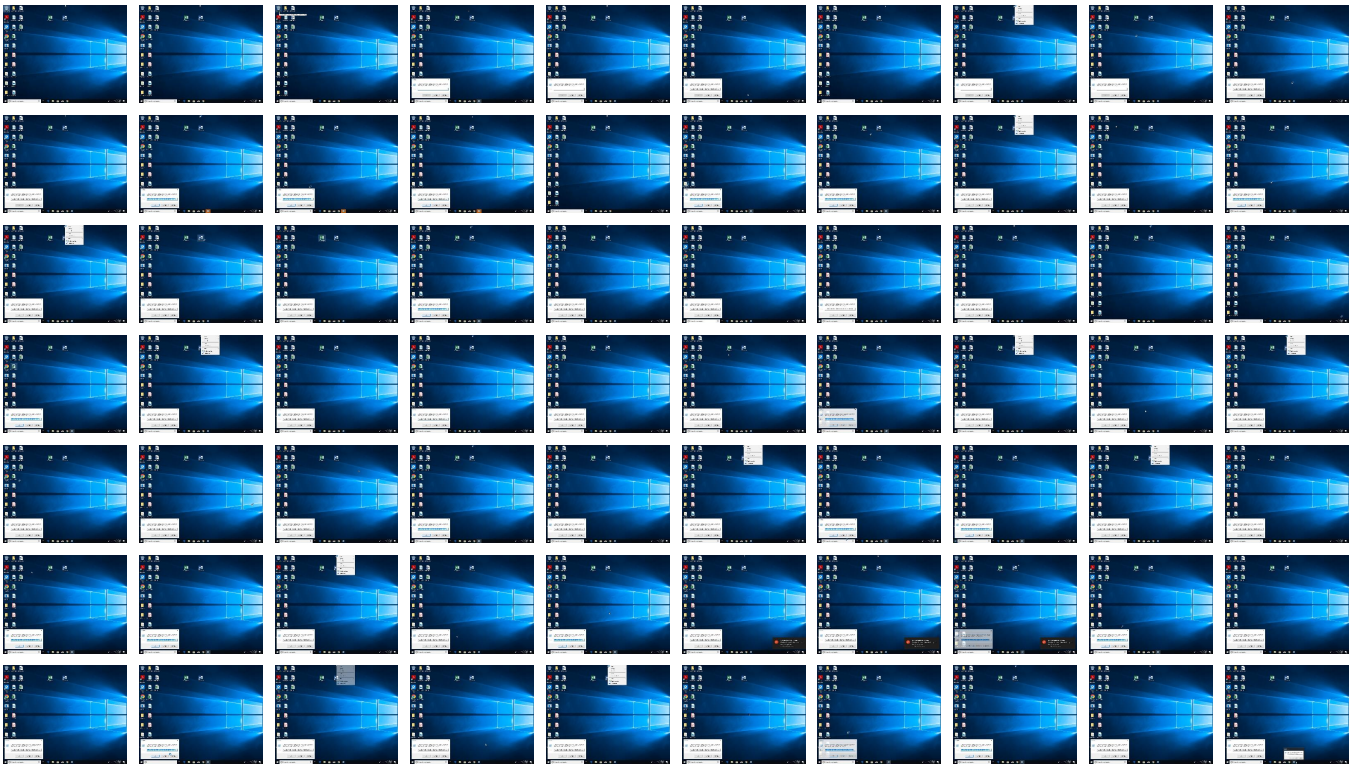
Behavior Graph

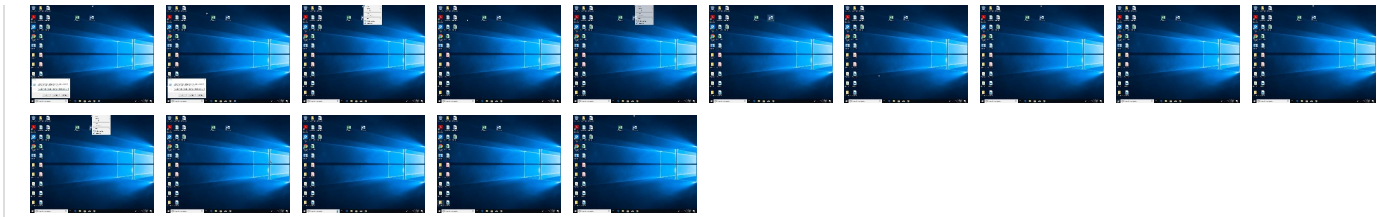


Screenshots

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
mPNVrHIpyt.exe	84%	Virustotal		Browse
mPNVrHIpyt.exe	78%	Metadefender		Browse
mPNVrHIpyt.exe	97%	ReversingLabs	Win32.Ransomware.GandCrab	
mPNVrHIpyt.exe	100%	Avira	TR/Dropper.Gen	
mPNVrHIpyt.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.mPNVrHIpyt.exe.3e00000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
27.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
27.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.3.wzltxa.exe.3940000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.mPNVrHIpyt.exe.f690000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.3.wzltxa.exe.2fa0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
13.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
31.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
40.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
34.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.3.wzltxa.exe.3270000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
39.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
34.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
30.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
33.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
39.3.wzltxa.exe.4010000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.3.wzltxa.exe.3b90000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.wzltxa.exe.3b20000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
39.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
22.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.3.wzltxa.exe.3a80000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
33.3.wzltxa.exe.2f00000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.wzltxa.exe.3640000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
33.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
31.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
28.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
28.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
28.3.wzltxa.exe.38a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
30.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.mPNVrHIpyt.exe.f690000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
40.0.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.3.wzltxa.exe.3a00000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.2.wzltxa.exe.fbb0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gdcbmuveqjsli57x.onion/cd05fa18e84d425b	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

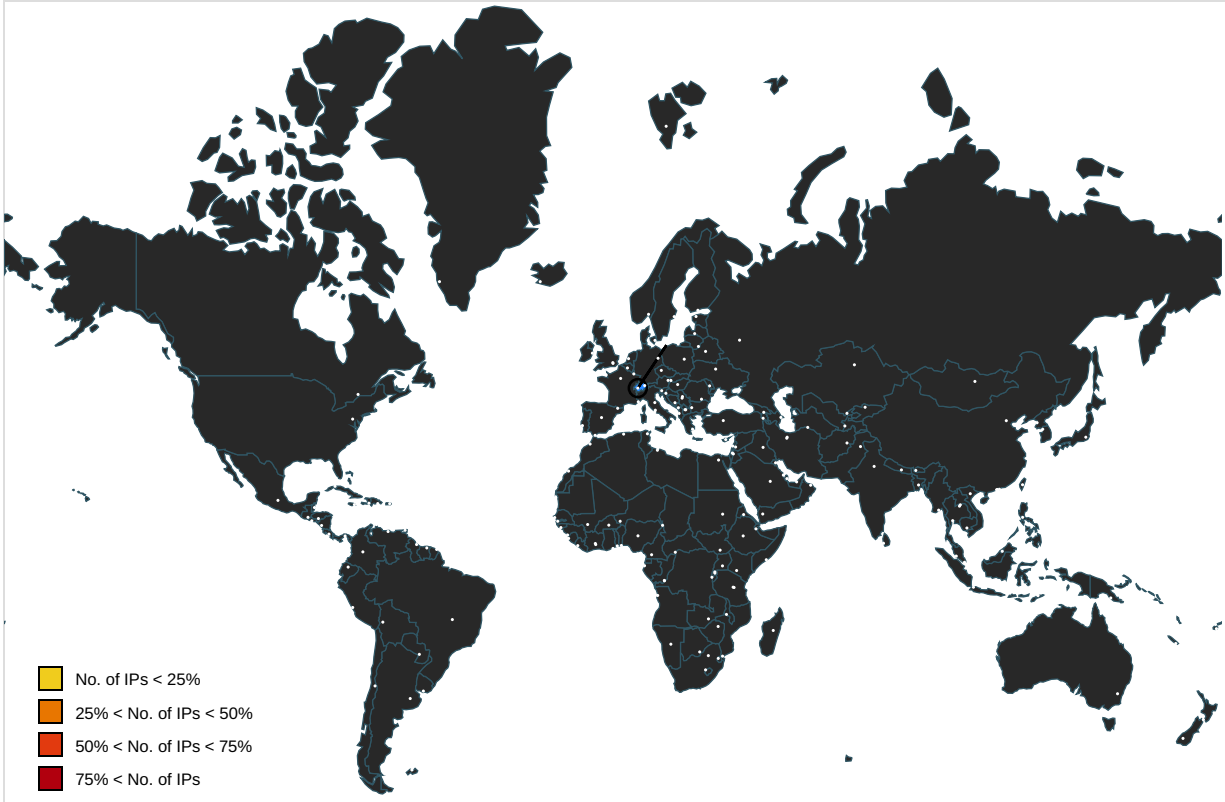
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ipv4bot.whatismyipaddress.com/r	wzltxa.exe, 0000000B.00000002.319600520.00000000010EA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/0	wzltxa.exe, 00000012.00000002.406611615.00000000012A8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/6	wzltxa.exe, 0000000D.00000002.356925187.0000000000D13000.00000004.00000020.00020000.00000000.sdmp, wzltxa.exe, 00000027.00000002.605442747.00000000016F3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/5	wzltxa.exe, 0000001F.00000002.546253684.0000000001488000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/u	mPNVrHIpyt.exe, 00000000.00000002.280964753.0000000001549000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/T	wzltxa.exe, 00000021.00000002.566573715.0000000000758000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/3	wzltxa.exe, 0000000D.00000002.356865636.0000000000CD8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/S	wzltxa.exe, 0000000B.00000002.319600520.00000000010EA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/)	wzltxa.exe, 0000001C.00000002.510519508.0000000001098000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/pxV	wzltxa.exe, 00000016.00000002.443945557.0000000000E78000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/.	wzltxa.exe, 0000001C.00000003.509113143.00000000010D4000.00000004.00000020.00020000.00000000.sdmp, wzltxa.exe, 0000001C.00000002.510669459.00000000010D4000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://gdcbmuveqjsli57x.onion/cd05fa18e84d425b	mPNVrHIpyt.exe, 00000000.00000002.281255332.000000000F6A2000.00000004.00000001.01000000.00000003.sdmp, wzltxa.exe, 0000000B.00000002.320303150.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000C.00000002.344617824.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000D.00000002.357333770.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000F.00000002.385057695.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000012.00000002.407272016.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000016.00000002.444732494.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000019.00000002.471339306.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000001C.00000002.511353636.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000001F.00000002.547100256.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000021.00000002.567450621.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000027.00000002.606206614.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp	true	• Avira URL Cloud: malware	unknown
http://ipv4bot.whatismyipaddress.com/K	mPNVrHIpyt.exe, 00000000.00000002.280964753.0000000001549000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/a	wzltxa.exe, 0000001F.00000002.546253684.0000000001488000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/E:	wzltxa.exe, 0000000F.00000002.384119850.000000000084F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/%	wzltxa.exe, 0000000D.00000002.356865636.0000000000CD8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.torproject.org/	mPNVrHIpyt.exe, 00000000.00000002.281255332.000000000F6A2000.00000004.00000001.01000000.00000003.sdmp, wzltxa.exe, 0000000B.00000002.320303150.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000C.00000002.344617824.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000D.00000002.357333770.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000F.00000002.385057695.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000012.00000002.407272016.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000016.00000002.444732494.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000019.00000002.471339306.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000001C.00000002.511353636.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000001F.00000002.547100256.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000021.00000002.567450621.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000027.00000002.606206614.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/Z	mPNVrHIpyt.exe, 00000000.00000002.280964753.0000000001549000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/Y	wzltxa.exe, 00000012.00000002.406711705.00000000012E5000.00000004.00000020.00020000.00000000.sdmp, wzltxa.exe, 00000012.00000003.405938163.00000000012E5000.00000004.00000020.00020000.00000000.sdmp, wzltxa.exe, 0000001F.00000002.546525436.000000014C6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/	wzltxa.exe, 00000027.00000002.605442747.00000000016F3000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tox.chat/download.html	mPNVrHIpyt.exe, 00000000.00000002.281255332.000000000F6A2000.00000004.00000001.01000000.00000003.sdmp, wzltxa.exe, 0000000B.00000002.320303150.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000C.00000002.344617824.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000D.00000002.357333770.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000000F.00000002.385057695.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000012.00000002.407272016.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000016.00000002.444732494.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000019.00000002.471339306.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000001C.00000002.511353636.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 0000001F.00000002.547100256.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000021.00000002.567450621.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, wzltxa.exe, 00000027.00000002.606206614.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp	false	• URL Reputation: safe	unknown
http://ipv4bot.whatismyipaddress.com/nxD	wzltxa.exe, 00000016.00000002.443945557.0000000000E78000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694572
Start date and time:	2022-09-01 00:06:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mPNVrHIpyt.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:	41
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@17/1@16/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99% (good quality ratio 95.1%) • Quality average: 83.2% • Quality standard deviation: 24.5%
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 • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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.

Simulations

Behavior and APIs

Time	Type	Description
00:07:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce imsihyxywip "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:07:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce imsihyxywip "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:07:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce lwxsmttcgib "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:08:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce rbpjrvqzmfp "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:08:11	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce lldeowbcwli "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:08:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce mvsrloqetvq "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"

Time	Type	Description
00:08:29	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce pkxyauwkvet "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:08:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce lwxsmttcgib "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:08:51	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce rbpjrvqzmfp "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:00	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce lldeowbcwli "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce mvsrloqetvq "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce pkxyauwkvet "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce axlnhkgixlf "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:36	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce xjlfhrnjhfo "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:44	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ovikprhtlzq "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:09:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce jmfyvzwgtay "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:10:01	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce axlnhkgixlf "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:10:09	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce xjlfhrnjhfo "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:10:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce ovikprhtlzq "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
00:10:26	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce jmfyvzwgtay "C:\Users\user\AppData\Roaming\Microsoft\wzltxa.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\wzltxa.exe

Process:	C:\Users\user\Desktop\mPNVrHIpyt.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	71680
Entropy (8bit):	6.49012841585642

Encrypted:	false
SSDEEP:	1536:fZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:2d5BJHMqqDL2/Ovvdr
MD5:	EAC223A7EC1CF2E33BE569DB14A87A63
SHA1:	EEF79567F14954FC347B3AFE712C07A76AFCABE6
SHA-256:	5C516C9C18FD4D7BE54B4C2218CCCDD7EA0650E6564B782027241F7D2DF50BE9
SHA-512:	8B04471BADA08AF6A20713C13CA636FC8F5487EDDCCC15201C0E436C64D3D824C674DDD71DC9A2ECF541C731AF6C54057BE482114C2FA1FD4019FC60FB28B07
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\wzltxa.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This .=...im 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):	6.490132731956949
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:	mPNVrHIpyt.exe
File size:	71680
MD5:	cc7ae6e4c86f605aab66fbd04eef7997
SHA1:	8c7c23c91ccecf548c6f9df30b839b9b24d57095
SHA256:	95427e787bb623ba2d2ec51cb289ae579aea27a674d900f9aa239f6a034b05cc
SHA512:	767db43c1dbb486350eee49ccd58cdb4767cad3907795f24bf65f5aec52c9bee18854feeac2791c87523eea018a36b42260d0b83f9699fe332e3d5dec8a0e317
SSDEEP:	1536:0ZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:Ld5BJHMqqDL2/Ovvdr
TLSH:	82636C1DB2D1B293F1E396B9FAB57E25445D2D103B056BEB08A369F568120F16C3B703
File Content Preview:	MZ.....@.....!..L.!This Nk...xm 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 00007F8A7075054Fh
test eax, eax
je 00007F8A707508BAh
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 00007F8A707508DEh
push 00001388h
mov eax, dword ptr [ebp-04h]
push eax
call dword ptr [1000A080h]
cmp eax, 00000102h
jne 00007F8A707508BEh
push 00000000h
mov ecx, dword ptr [ebp-04h]
push ecx
call dword ptr [1000A094h]
mov edx, dword ptr [ebp-04h]
push edx
call dword ptr [1000A10Ch]
call 00007F8A707505E4h
call 00007F8A7074FFCFh
lea ecx, dword ptr [ebp-4Ch]
call 00007F8A70752267h
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]

Instruction
push eax
lea ecx, dword ptr [ebp-4Ch]
call 00007F8A707521E3h
mov dword ptr [ebp-2Ch], 00000000h
mov dword ptr [ebp-0Ch], 00000000h
mov ecx, dword ptr [ebp-18h]
call 00007F8A707507CDh

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	0.47765899122807015	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
.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
Sep 1, 2022 00:07:34.490466118 CEST	51139	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:07:34.510363102 CEST	53	51139	8.8.8.8	192.168.2.3
Sep 1, 2022 00:07:52.513761044 CEST	52955	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:07:52.533942938 CEST	53	52955	8.8.8.8	192.168.2.3
Sep 1, 2022 00:08:04.046449900 CEST	57134	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:08:04.065778017 CEST	53	57134	8.8.8.8	192.168.2.3
Sep 1, 2022 00:08:09.926047087 CEST	62050	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:08:09.944586039 CEST	53	62050	8.8.8.8	192.168.2.3
Sep 1, 2022 00:08:22.282254934 CEST	53848	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:08:22.303661108 CEST	53	53848	8.8.8.8	192.168.2.3
Sep 1, 2022 00:08:32.932132959 CEST	57571	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:08:32.951133013 CEST	53	57571	8.8.8.8	192.168.2.3
Sep 1, 2022 00:08:50.475862980 CEST	53305	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:08:50.495318890 CEST	53	53305	8.8.8.8	192.168.2.3
Sep 1, 2022 00:09:02.752767086 CEST	60749	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:09:02.773488998 CEST	53	60749	8.8.8.8	192.168.2.3
Sep 1, 2022 00:09:21.074116945 CEST	56949	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:09:21.092598915 CEST	53	56949	8.8.8.8	192.168.2.3
Sep 1, 2022 00:09:35.271372080 CEST	53844	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:09:35.293471098 CEST	53	53844	8.8.8.8	192.168.2.3
Sep 1, 2022 00:09:47.508217096 CEST	53466	53	192.168.2.3	8.8.8.8

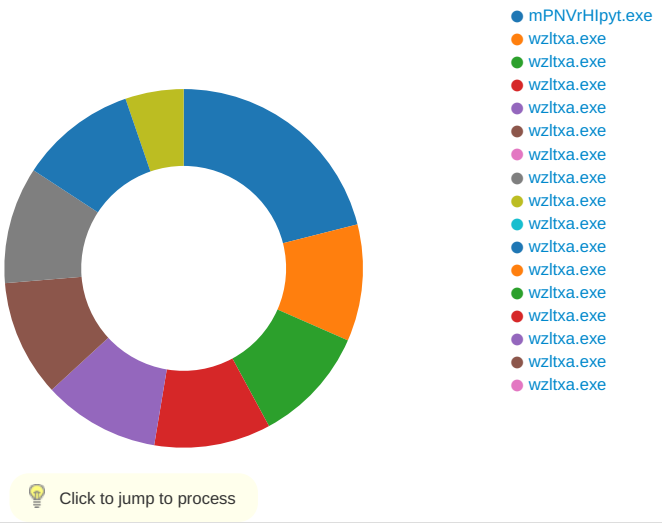
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 1, 2022 00:09:47.530179977 CEST	53	53466	8.8.8.8	192.168.2.3
Sep 1, 2022 00:10:05.653143883 CEST	53428	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:10:05.674639940 CEST	53	53428	8.8.8.8	192.168.2.3
Sep 1, 2022 00:10:13.795104980 CEST	59820	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:10:13.813121080 CEST	53	59820	8.8.8.8	192.168.2.3
Sep 1, 2022 00:10:21.883244991 CEST	64595	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:10:21.902523041 CEST	53	64595	8.8.8.8	192.168.2.3
Sep 1, 2022 00:10:29.572328091 CEST	52079	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:10:29.593041897 CEST	53	52079	8.8.8.8	192.168.2.3
Sep 1, 2022 00:10:38.119400978 CEST	64823	53	192.168.2.3	8.8.8.8
Sep 1, 2022 00:10:38.138722897 CEST	53	64823	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 1, 2022 00:07:34.490466118 CEST	192.168.2.3	8.8.8.8	0x7d52	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:07:52.513761044 CEST	192.168.2.3	8.8.8.8	0x6f58	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:08:04.046449900 CEST	192.168.2.3	8.8.8.8	0xd60e	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:08:09.926047087 CEST	192.168.2.3	8.8.8.8	0xb9a9	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:08:22.282254934 CEST	192.168.2.3	8.8.8.8	0xb7b	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:08:32.932132959 CEST	192.168.2.3	8.8.8.8	0x70c4	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:08:50.475862980 CEST	192.168.2.3	8.8.8.8	0x7a43	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:09:02.752767086 CEST	192.168.2.3	8.8.8.8	0x359e	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:09:21.074116945 CEST	192.168.2.3	8.8.8.8	0x6853	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:09:35.271372080 CEST	192.168.2.3	8.8.8.8	0x642b	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:09:47.508217096 CEST	192.168.2.3	8.8.8.8	0xe80f	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:10:05.653143883 CEST	192.168.2.3	8.8.8.8	0x2436	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:10:13.795104980 CEST	192.168.2.3	8.8.8.8	0xb939	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:10:21.883244991 CEST	192.168.2.3	8.8.8.8	0x1cb7	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:10:29.572328091 CEST	192.168.2.3	8.8.8.8	0x5c0c	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:10:38.119400978 CEST	192.168.2.3	8.8.8.8	0xefbc	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: mPNVrHIpyt.exe PID: **3592**, Parent PID: **3508**

General

Target ID:	0
Start time:	00:07:26
Start date:	01/09/2022
Path:	C:\Users\user\Desktop\mPNVrHIpyt.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\mPNVrHIpyt.exe"
Imagebase:	0xf690000
File size:	71680 bytes
MD5 hash:	CC7AE6E4C86F605AAB66FBD04EEF7997
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.264971762.000000000F69A000.00000002.00000001.01000000.00000003.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: 00000000.00000003.280650626.0000000003E00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000000.00000003.280650626.0000000003E00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000003.280650626.0000000003E00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000000.00000003.280650626.0000000003E00000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000000.00000003.280650626.0000000003E00000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000000.00000003.280650626.0000000003E00000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.281255332.000000000F6A2000.00000004.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000002.281249119.000000000F69A000.00000002.00000001.01000000.00000003.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\wzltxa.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F692852	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\wzltxa.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 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 fd 3d fd fd fd 69 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 fd fd 17 fd fd fd fd fd fd fd 19 fd 7d fd fd fd 19 fd 42 fd fd fd fd b0 42 fd fd fd fd fd fd fd fd fd fd 9a 31 fd fd fd fd fd fd 59 fd fd b0 47 fd fd fd fd b0 7e fd fd fd fd b0 79 fd fd fd fd b0 7c fd fd fd fd 52 69 63 68 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06	MZ@!L!This =im cannot be run in DOS mode.$}BB1YG~y|RichPEL	success or wait	1	F69286F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\mPNVrHIpyt.exe	unknown	71680	success or wait	1	F693652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	imsihyxywip	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	F692AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **1276**, Parent PID: **3452**

General

Target ID:	11
Start time:	00:07:42
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0x7ff651c80000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000000B.00000000.302743243.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000B.00000002.320296152.000000000FBBA000.00000002.00000001.01000000.00000004.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: 0000000B.00000003.319280593.0000000003940000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000B.00000003.319280593.0000000003940000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000B.00000003.319280593.0000000003940000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000B.00000003.319280593.0000000003940000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000B.00000003.319280593.0000000003940000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000B.00000003.319280593.0000000003940000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000B.00000002.320303150.000000000FBC2000.00000004.00000001.01000000.00000004.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: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\wzltxa.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	lwxsmttcgib	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **1920**, Parent PID: **3452**

General

Target ID:	12
Start time:	00:07:52
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000000C.00000003.343975450.0000000003B20000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000C.00000003.343975450.0000000003B20000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000003.343975450.0000000003B20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000C.00000003.343975450.0000000003B20000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000C.00000003.343975450.0000000003B20000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000C.00000003.343975450.0000000003B20000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000002.344609197.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000C.00000002.344617824.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000000.321133700.000000000FBBA000.00000002.00000001.01000000.00000004.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	rbpjrvqzmfp	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **4616**, Parent PID: **3452**

General

Target ID:	13
Start time:	00:08:00
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000000D.00000002.357323149.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000D.00000002.357333770.000000000FBC2000.00000004.00000001.01000000.00000004.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: 0000000D.00000003.356575582.0000000003270000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000D.00000003.356575582.0000000003270000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000D.00000003.356575582.0000000003270000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000D.00000003.356575582.0000000003270000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000D.00000003.356575582.0000000003270000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000D.00000003.356575582.0000000003270000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000D.00000000.343145557.000000000FBBA000.00000002.00000001.01000000.00000004.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	lldeowbcwli	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **6136**, Parent PID: **3452**

General

Target ID:	15
Start time:	00:08:12
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000000F.00000000.363985954.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000002.385026266.000000000FBBA000.00000002.00000001.01000000.00000004.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.00000003.383072637.0000000002FA0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000F.00000003.383072637.0000000002FA0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000003.383072637.0000000002FA0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000F.00000003.383072637.0000000002FA0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000F.00000003.383072637.0000000002FA0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000F.00000003.383072637.0000000002FA0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000F.00000002.385057695.000000000FBC2000.00000004.00000001.01000000.00000004.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	mvsrloqetvq	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **1356**, Parent PID: **3452**

General

Target ID:	18
Start time:	00:08:21
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000012.00000002.407272016.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000012.00000000.383675616.000000000FBBA000.00000002.00000001.01000000.00000004.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: 00000012.00000003.405995868.0000000003A80000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000012.00000003.405995868.0000000003A80000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000012.00000003.405995868.0000000003A80000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000012.00000003.405995868.0000000003A80000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000012.00000003.405995868.0000000003A80000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000012.00000003.405995868.0000000003A80000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000012.00000002.407240939.000000000FBBA000.00000002.00000001.01000000.00000004.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	pkxyauwkvet	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **2996**, Parent PID: **3452**

General

Target ID:	20
Start time:	00:08:29
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000014.00000000.401188568.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000014.00000002.405226267.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: **6016**, Parent PID: **3452**

General

Target ID:	22
Start time:	00:08:38
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000016.00000002.444732494.000000000FBC2000.00000004.00000001.01000000.00000004.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: 00000016.00000003.443479124.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000016.00000003.443479124.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000016.00000003.443479124.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000016.00000003.443479124.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000016.00000003.443479124.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000016.00000003.443479124.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000016.00000000.422070871.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000016.00000002.444710871.000000000FBBA000.00000002.00000001.01000000.00000004.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	axlnhkgixlf	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: **5520**, Parent PID: **3452**

General

Target ID:	25
Start time:	00:08:52
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000019.00000002.471339306.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000002.471324197.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000000.449352573.000000000FBBA000.00000002.00000001.01000000.00000004.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: 00000019.00000003.469796043.0000000003A00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000019.00000003.469796043.0000000003A00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000003.469796043.0000000003A00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000019.00000003.469796043.0000000003A00000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000019.00000003.469796043.0000000003A00000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000019.00000003.469796043.0000000003A00000.00000004.00001000.00020000.00000000.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Analysis Process: wzltxa.exe PID: **2228**, Parent PID: **3452**

General

Target ID:	27
Start time:	00:09:00
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000001B.00000000.467592821.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001B.00000002.470832696.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: 6128, Parent PID: 3452

General

Target ID:	28
Start time:	00:09:09
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000001C.00000000.485070318.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000001C.00000002.511353636.000000000FBC2000.00000004.00000001.01000000.00000004.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: 0000001C.00000003.509057598.00000000038A0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001C.00000003.509057598.00000000038A0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001C.00000003.509057598.00000000038A0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001C.00000003.509057598.00000000038A0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001C.00000003.509057598.00000000038A0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001C.00000003.509057598.00000000038A0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001C.00000002.511336369.000000000FBBA000.00000002.00000001.01000000.00000004.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\wzltxa.exe	unknown	71680	success or wait	1	FBB3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	xjlfhrnjhfo	unicode	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"	success or wait	1	FBB2AAA	RegSetValueExW

Analysis Process: wzltxa.exe PID: 5752, Parent PID: 3452

General

Target ID:	30
Start time:	00:09:18
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63

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: 0000001E.00000000.505234483.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000002.508822992.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: **2156**, Parent PID: **3452**

General

Target ID:	31
Start time:	00:09:27
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 0000001F.00000000.523518226.000000000FBBA000.00000002.00000001.01000000.00000004.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: 0000001F.00000003.539610642.0000000003B90000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001F.00000003.539610642.0000000003B90000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001F.00000003.539610642.0000000003B90000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001F.00000003.539610642.0000000003B90000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001F.00000003.539610642.0000000003B90000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001F.00000003.539610642.0000000003B90000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000001F.00000002.547100256.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001F.00000002.547067316.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: **5248**, Parent PID: **3452**

General

Target ID:	33
Start time:	00:09:36
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000021.00000000.547433699.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000021.00000002.567428078.000000000FBBA000.00000002.00000001.01000000.00000004.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: 00000021.00000003.565723232.0000000002F00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000021.00000003.565723232.0000000002F00000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000021.00000003.565723232.0000000002F00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000021.00000003.565723232.0000000002F00000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000021.00000003.565723232.0000000002F00000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000021.00000003.565723232.0000000002F00000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000021.00000002.567450621.000000000FBC2000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: **4920**, Parent PID: **3452**

General

Target ID:	34
Start time:	00:09:44
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000022.00000000.561698093.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000022.00000002.565428063.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: **1200**, Parent PID: **3452**

General

Target ID:	39
Start time:	00:09:53
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000027.00000002.606192732.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000027.00000002.606206614.000000000FBC2000.00000004.00000001.01000000.00000004.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: 00000027.00000003.604611550.0000000004010000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000027.00000003.604611550.0000000004010000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000027.00000003.604611550.0000000004010000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000027.00000003.604611550.0000000004010000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000027.00000003.604611550.0000000004010000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000027.00000003.604611550.0000000004010000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000027.00000000.580667243.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: wzltxa.exe PID: **5280**, Parent PID: **3452**

General

Target ID:	40
Start time:	00:10:01
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\wzltxa.exe"
Imagebase:	0xfbb0000
File size:	71680 bytes
MD5 hash:	EAC223A7EC1CF2E33BE569DB14A87A63
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: 00000028.00000000.597821532.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000028.00000002.601264865.000000000FBBA000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly