ID: 694565
Sample Name:
wThN5MTIsw.exe
Cookbook: default.jbs
Time: 23:55:56
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

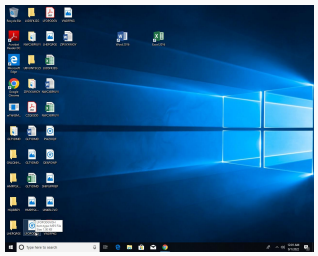
Windows Analysis Report

wThN5MTIsw.exe

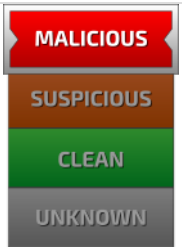
Overview

General Information

Sample Name:	wThN5MTIsw.exe
Analysis ID:	694565
MD5:	1813521f3884de..
SHA1:	874f4efd9b2ba64.
SHA256:	4e705159b6c3a7..
Tags:	exe GandCrab
Infos:	



Detection



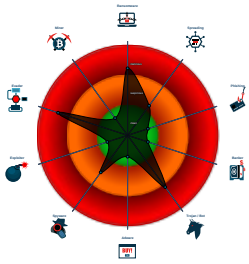
Gandcrab, ReflectiveLoader

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…
- 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**
- wThN5MTIsw.exe (PID: 6388 cmdline: "C:\Users\user\Desktop\wThN5MTIsw.exe" MD5: 1813521F3884DE8427728B54B5C9A391)
- ssapst.exe (PID: 6592 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 6840 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 7028 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 5668 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 6104 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 4292 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 1416 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 3588 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 3248 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 6228 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 5016 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 7020 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 7108 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 204 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 4804 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 5952 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 1784 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 5076 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 5700 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- ssapst.exe (PID: 972 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe" MD5: C99BAB5FEA91C0938D1D5B6684158B24)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
wThN5MTIsw.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
wThN5MTIsw.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
wThN5MTIsw.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
wThN5MTIsw.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
wThN5MTIsw.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$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\ssapst.exe	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xef91:$s1: _ReflectiveLoader@ • 0xef92:$s2: ReflectiveLoader@
C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe	Gandcrab	Gandcrab Payload	kevoreilly	• 0xe5c8:$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
00000000.00000002.335673365.000000000F4EA000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000008.00000002.421043250.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xef92:$x1: ReflectiveLoader
00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xe8fe:$: DECRYPT.txt • 0xe964:$: DECRYPT.txt
00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
Click to see the 199 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
34.3.ssapst.exe.32a0000.0.unpack	ReflectiveLoader	Detects a unspecified hack tool, crack or malware using a reflective loader - no hard match - further investigation recommended	Florian Roth	• 0xd992:$x1: ReflectiveLoader
34.3.ssapst.exe.32a0000.0.unpack	SUSP_RANSOMWARE_Indicator_Jul20	Detects ransomware indicator	Florian Roth	• 0xd2fe:$: DECRYPT.txt • 0xd364:$: DECRYPT.txt
34.3.ssapst.exe.32a0000.0.unpack	JoeSecurity_ReflectiveLoader	Yara detected ReflectiveLoader	Joe Security	
34.3.ssapst.exe.32a0000.0.unpack	INDICATOR_SUSPICIOUS_ReflectiveLoader	detects Reflective DLL injection artifacts	ditekSHen	• 0xd991:$s1: _ReflectiveLoader@ • 0xd992:$s2: ReflectiveLoader@
34.3.ssapst.exe.32a0000.0.unpack	Gandcrab	Gandcrab Payload	kevoreilly	• 0xcfc8:$string3: action=result&e_files=%d&e_size=%I64u&e_time=%d&
Click to see the 468 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

Boot Survival

Creates multiple autostart registry keys

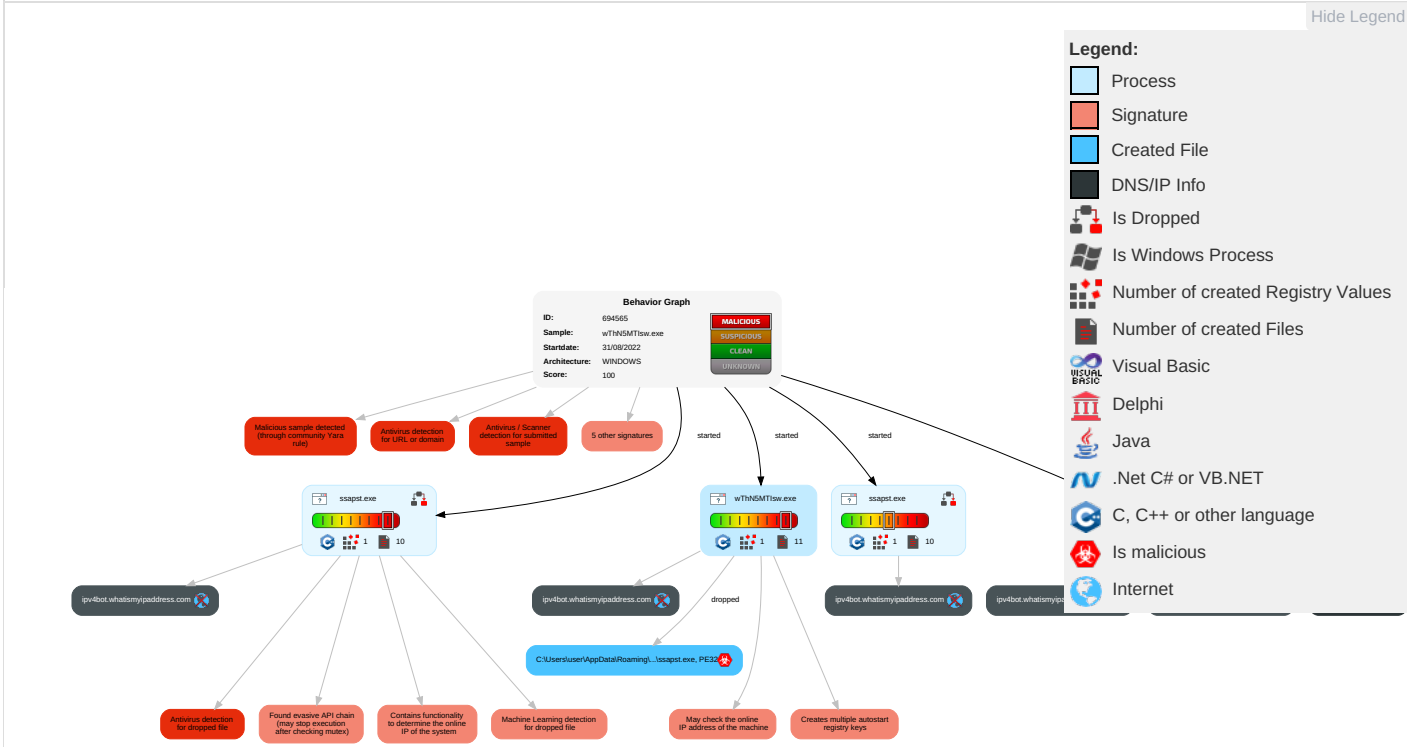
Malware Analysis System Evasion

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 1 Security Software Discovery	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 Process 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 1 Peripheral Device 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 Account 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 System Owner/User 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 Remote System 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 System Network Configuration 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 Connections 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 File and Directory 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	4 4 System Information Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

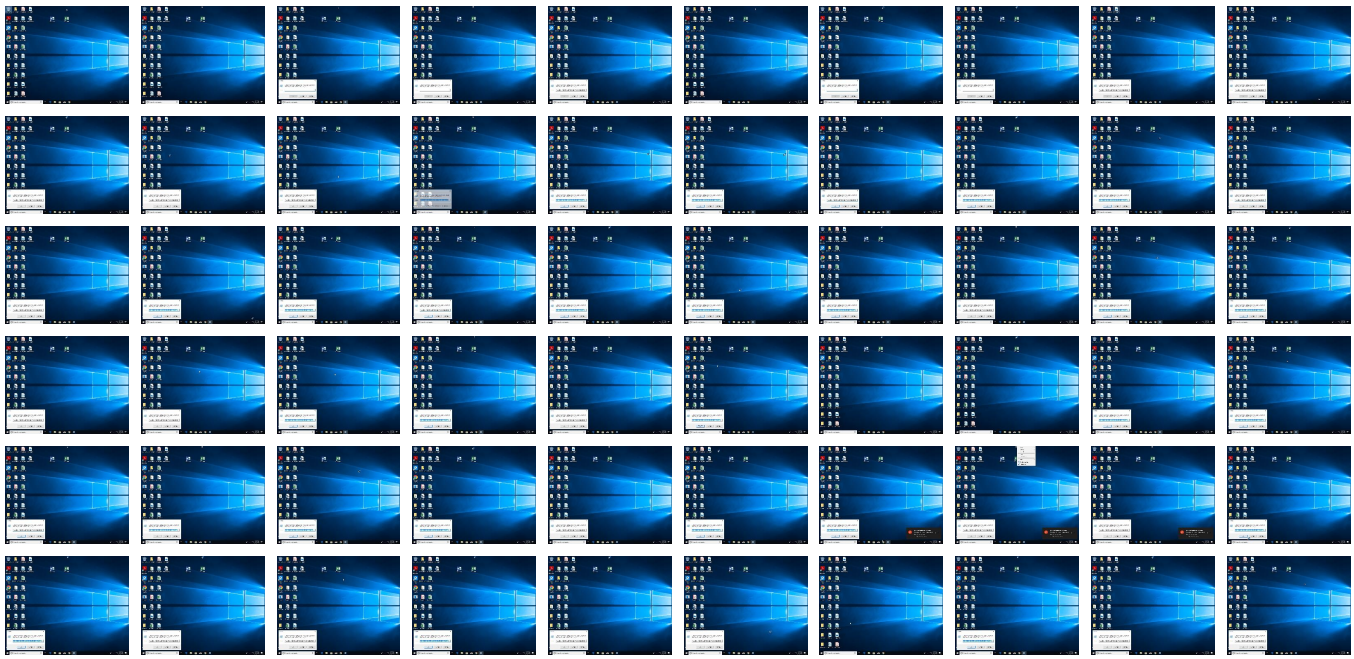
Behavior Graph

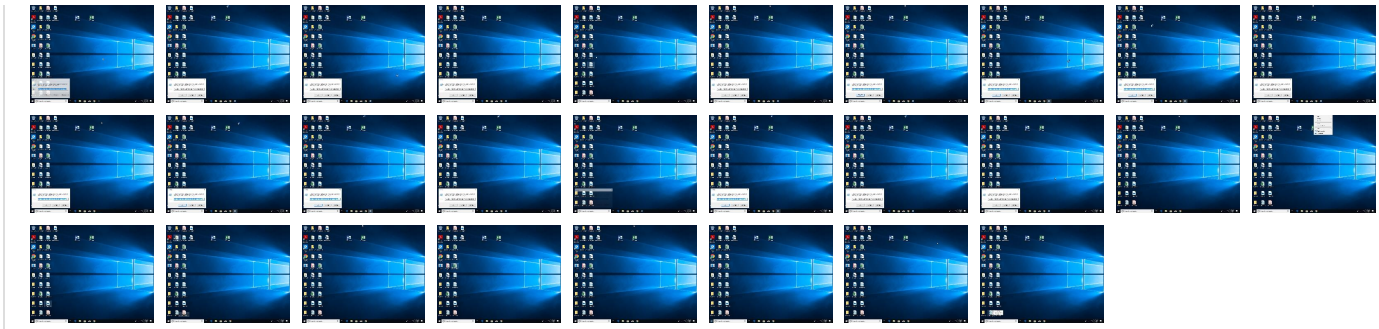


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
wThN5MTIsw.exe	90%	Virustotal		Browse
wThN5MTIsw.exe	93%	ReversingLabs	Win32.Ransomware.GandCrab	
wThN5MTIsw.exe	100%	Avira	TR/Dropper.Gen	
wThN5MTIsw.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
34.3.ssapst.exe.32a0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.wThN5MTIsw.exe.3170000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
32.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.wThN5MTIsw.exe.f4e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
24.3.ssapst.exe.3b60000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
24.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.3.ssapst.exe.2f70000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
35.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
30.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.3.ssapst.exe.3830000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.3.ssapst.exe.36d0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
15.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.3.ssapst.exe.3300000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
35.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.3.ssapst.exe.3730000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
33.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.3.ssapst.exe.3230000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
22.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
24.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
19.3.ssapst.exe.3520000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
25.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.3.ssapst.exe.30f0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.3.ssapst.exe.38c0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
30.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.3.ssapst.exe.3730000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
34.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
14.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
25.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
30.3.ssapst.exe.2fc0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
33.3.ssapst.exe.3d30000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.3.ssapst.exe.3640000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.wThN5MTIsw.exe.f4e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
33.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
34.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
31.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
32.3.ssapst.exe.3790000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.2.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
32.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
18.0.ssapst.exe.fe60000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gdcbmuveqjsli57x.onion/cec3c1ad6b0ea08f	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/2	wThN5MTIsw.exe, 00000000.00000002.335452470.00000000008D9000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/5	ssapst.exe, 00000018.00000002.585108554.00000000012E8000.00000004.00000020.00020000.00000000.sdmp, ssapst.exe, 00000019.00000002.605561331.0000000000EF8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/S	ssapst.exe, 00000004.00000002.382761696.0000000001018000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/)	ssapst.exe, 00000002.00000002.369878312.0000000000DCA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/I	ssapst.exe, 00000004.00000002.382761696.0000000001018000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/QL	ssapst.exe, 00000004.00000002.382761696.0000000001018000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/g	ssapst.exe, 00000019.00000002.607798154.0000000000F31000.00000004.00000020.00020000.00000000.sdmp, ssapst.exe, 00000019.00000003.601906375.0000000000F31000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://gdcbmuveqjsli57x.onion/cec3c1ad6b0ea08f	wThN5MTIsw.exe, 00000000.00000002.335680061.000000000F4F2000.00000004.00000001.01000000.00000003.sdmp, ssapst.exe, 00000002.00000002.370333139.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000004.00000002.383047915.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000006.00000002.406483395.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000008.00000002.421052694.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000C.00000002.445300926.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000E.00000002.457737689.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000F.00000002.485790617.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000012.00000002.521001527.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000013.00000002.556559672.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000018.00000002.585820146.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000019.00000002.608758289.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000001A.00000002.628251824.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000001E.00000002.654951583.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000020.00000002.682007928.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000021.00000002.703365325.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000022.00000002.734737605.000000000FE72000.00000004.00000001.01000000.00000004.sdmp	true	• Avira URL Cloud: malware	unknown
http://ipv4bot.whatismyipaddress.com/l;	ssapst.exe, 00000002.00000002.369878312.0000000000DCA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/&	ssapst.exe, 00000018.00000002.585108554.00000000012E8000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.torproject.org/	wThN5MTIsw.exe, 00000000.00000002.335680061.000000000F4F2000.00000004.00000001.01000000.00000003.sdmp, ssapst.exe, 00000002.00000002.370333139.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000004.00000002.383047915.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000006.00000002.406483395.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000008.00000002.421052694.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000C.00000002.445300926.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000E.00000002.457737689.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000F.00000002.485790617.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000012.00000002.521001527.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000013.00000002.556559672.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000018.00000002.585820146.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000019.00000002.608758289.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000001A.00000002.628251824.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000001E.00000002.654951583.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000020.00000002.682007928.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000021.00000002.703365325.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000022.00000002.734737605.000000000FE72000.00000004.00000001.01000000.00000004.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/G%b	ssapst.exe, 00000002.00000002.369878312.0000000000DCA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/x	ssapst.exe, 00000018.00000002.585108554.00000000012E8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://ipv4bot.whatismyipaddress.com/	ssapst.exe, 00000019.00000003.601906375.0000000000F31000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://tox.chat/download.html	wThN5MTIsw.exe, 00000000.00000002.335680061.000000000F4F2000.00000004.00000001.01000000.00000003.sdmp, ssapst.exe, 00000002.00000002.370333139.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000004.00000002.383047915.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000006.00000002.406483395.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000008.00000002.421052694.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000C.00000002.445300926.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000E.00000002.457737689.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000000F.00000002.485790617.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000012.00000002.521001527.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000013.00000002.556559672.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000018.00000002.585820146.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000019.00000002.608758289.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000001A.00000002.628251824.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 0000001E.00000002.654951583.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000020.00000002.682007928.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000021.00000002.703365325.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, ssapst.exe, 00000022.00000002.734737605.000000000FE72000.00000004.00000001.01000000.00000004.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:	694565
Start date and time:	2022-08-31 23:55:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wThN5MTIsw.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:	37
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@21/1@17/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99% (good quality ratio 95.1%) • Quality average: 83.3% • Quality standard deviation: 24.4%
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, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.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
23:57:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce qxcdehgjaib "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:57:14	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce qxcdehgjaib "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:57:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce ocipuxittak "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:57:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce trtwjkdvbrs "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:57:40	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce ftylkauykkg "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:57:48	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce biktigczvpq "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:57:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce rjjumyjxpew "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:58:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce ypcrxwqpxuk "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:58:14	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce qtytdguwutr "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:58:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ocipuxittak "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:58:37	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce trtwjkdvbrs "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:58:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ftylkauykkg "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:58:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce biktigczvpq "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce rjjumyjxpew "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce ypcrxwqpxuk "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:21	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce qtytdguwutr "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce hdwqlmoiwuh "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce hedsypabrrz "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce hdwqlmoiwuh "C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
23:59:58	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce hedsypabrrz "C:\Users\user\AppData\Roaming\Microsoft\ssapst.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\ssapst.exe

Process:	C:\Users\user\Desktop\wThN5MTIsw.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	71680
Entropy (8bit):	6.4901994599792285
Encrypted:	false
SSDEEP:	1536:eZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:9d5BJHMqqDL2/Ovvdr
MD5:	C99BAB5FEA91C0938D1D5B6684158B24
SHA1:	ECD22F94099A54544BA148AE4F53B6B52FB61573
SHA-256:	48BB3CA46BEF3D18611DCD134BAE27C277FF007E2D486CC46B17ECBDA3981429
SHA-512:	76FE6196B411FDBD88053502CCE6494B9F995277FEF67406BE5143B72E1832D039E1B90D15E9490BC238DD7EF3DF3C37D7C62B71E495811437AA3C5ECB5D300
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\ssapst.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This .....Ym 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):	6.4900942221998115
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:	wThN5MTIsw.exe
File size:	71680
MD5:	1813521f3884de8427728b54b5c9a391
SHA1:	874f4efd9b2ba64fa3bcb6ae87b116bd526b85c3
SHA256:	4e705159b6c3a72b2b160486b9d582f05e34cd89a767428ef47ff6562b39619e
SHA512:	d640a17b59a7a23d9353339a97a174c4de4fdc7f96e813f30d0d3f687f5e67df933d90f1c7de614ce82686eb6d0dad37680cf6d1b314a04c49de0802b8329705
SSDEEP:	1536:oZZZZZZZZZZZZpXzzzzzzzzzzzzADypczUk+lkZJngWMqqU+2bbbAV2/S2OvvdZl:nd5BJHMqqDL2/Ovvdr
TLSH:	FC636C1DB2D1B293F1E396B9FAB57E25445D2D103B056BEB08A369F568220F16C3B703
File Content Preview:	MZ.....@.....!..L.!This :.@i.hm 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 00007FF6F49E256Fh
test eax, eax
je 00007FF6F49E28DAh
push 00000000h
call dword ptr [1000A168h]
push 00000000h
push 00000000h
push 00000000h
push 10002D30h

Instruction
push 00000000h
push 00000000h
call dword ptr [1000A108h]
mov dword ptr [ebp-04h], eax
cmp dword ptr [ebp-04h], 00000000h
je 00007FF6F49E28FEh
push 00001388h
mov eax, dword ptr [ebp-04h]
push eax
call dword ptr [1000A080h]
cmp eax, 00000102h
jne 00007FF6F49E28DEh
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 00007FF6F49E2604h
call 00007FF6F49E1FEFh
lea ecx, dword ptr [ebp-4Ch]
call 00007FF6F49E4287h
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 00007FF6F49E4203h
mov dword ptr [ebp-2Ch], 00000000h
mov dword ptr [ebp-0Ch], 00000000h
mov ecx, dword ptr [ebp-18h]
call 00007FF6F49E27EDh

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	

Name	Virtual Address	Virtual Size	Is in Section
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
Aug 31, 2022 23:57:06.129142046 CEST	59683	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:57:06.148230076 CEST	53	59683	8.8.8.8	192.168.2.4
Aug 31, 2022 23:57:22.315282106 CEST	64167	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:57:22.333259106 CEST	53	64167	8.8.8.8	192.168.2.4
Aug 31, 2022 23:57:28.340138912 CEST	52239	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:57:28.359524012 CEST	53	52239	8.8.8.8	192.168.2.4
Aug 31, 2022 23:57:38.929553032 CEST	56807	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:57:38.949150085 CEST	53	56807	8.8.8.8	192.168.2.4
Aug 31, 2022 23:57:45.791605949 CEST	59444	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:57:45.811317921 CEST	53	59444	8.8.8.8	192.168.2.4
Aug 31, 2022 23:57:56.947793007 CEST	55570	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:57:56.965518951 CEST	53	55570	8.8.8.8	192.168.2.4
Aug 31, 2022 23:58:02.928319931 CEST	64906	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:58:02.947957039 CEST	53	64906	8.8.8.8	192.168.2.4
Aug 31, 2022 23:58:15.867604971 CEST	59446	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:58:15.885432959 CEST	53	59446	8.8.8.8	192.168.2.4
Aug 31, 2022 23:58:29.536561966 CEST	50861	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:58:29.558046103 CEST	53	50861	8.8.8.8	192.168.2.4
Aug 31, 2022 23:58:46.581418991 CEST	61088	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:58:46.599021912 CEST	53	61088	8.8.8.8	192.168.2.4
Aug 31, 2022 23:59:02.684118986 CEST	58729	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:59:02.701252937 CEST	53	58729	8.8.8.8	192.168.2.4
Aug 31, 2022 23:59:10.632801056 CEST	64700	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:59:10.652909040 CEST	53	64700	8.8.8.8	192.168.2.4
Aug 31, 2022 23:59:21.689377069 CEST	60550	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:59:21.708925962 CEST	53	60550	8.8.8.8	192.168.2.4
Aug 31, 2022 23:59:34.749181032 CEST	55673	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:59:34.769097090 CEST	53	55673	8.8.8.8	192.168.2.4
Aug 31, 2022 23:59:46.759083986 CEST	52437	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:59:46.777046919 CEST	53	52437	8.8.8.8	192.168.2.4
Aug 31, 2022 23:59:57.148920059 CEST	52825	53	192.168.2.4	8.8.8.8
Aug 31, 2022 23:59:57.168656111 CEST	53	52825	8.8.8.8	192.168.2.4
Sep 1, 2022 00:00:11.293533087 CEST	58530	53	192.168.2.4	8.8.8.8
Sep 1, 2022 00:00:11.310962915 CEST	53	58530	8.8.8.8	192.168.2.4

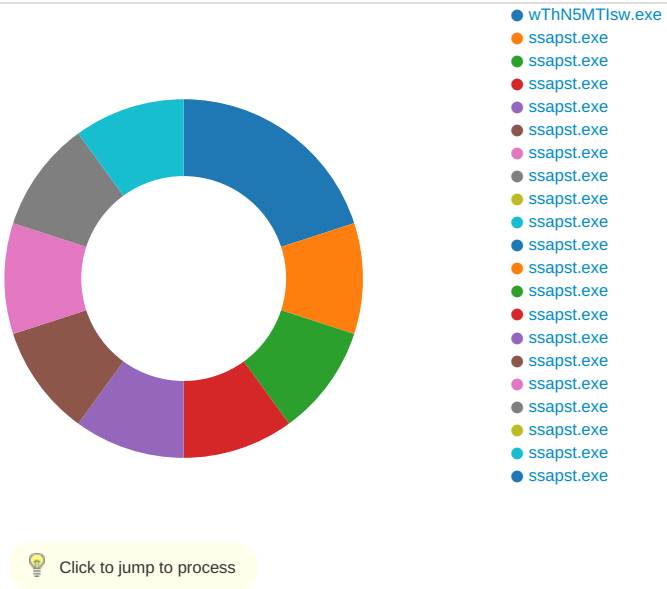
DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:57:06.129142046 CEST	192.168.2.4	8.8.8.8	0xb918	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:57:22.315282106 CEST	192.168.2.4	8.8.8.8	0x3c2b	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:57:28.340138912 CEST	192.168.2.4	8.8.8.8	0xcc0e	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:57:38.929553032 CEST	192.168.2.4	8.8.8.8	0xd15d	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:57:45.791605949 CEST	192.168.2.4	8.8.8.8	0xc4ea	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:57:56.947793007 CEST	192.168.2.4	8.8.8.8	0x5ef8	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:02.928319931 CEST	192.168.2.4	8.8.8.8	0x9f47	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:15.867604971 CEST	192.168.2.4	8.8.8.8	0x93a8	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:29.536561966 CEST	192.168.2.4	8.8.8.8	0x2a7d	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:58:46.581418991 CEST	192.168.2.4	8.8.8.8	0x5d70	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:02.684118986 CEST	192.168.2.4	8.8.8.8	0x97b6	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:10.632801056 CEST	192.168.2.4	8.8.8.8	0x4d06	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:21.689377069 CEST	192.168.2.4	8.8.8.8	0xf04e	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:34.749181032 CEST	192.168.2.4	8.8.8.8	0x670d	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:46.759083986 CEST	192.168.2.4	8.8.8.8	0x8f79	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:59:57.148920059 CEST	192.168.2.4	8.8.8.8	0x52d6	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)
Sep 1, 2022 00:00:11.293533087 CEST	192.168.2.4	8.8.8.8	0x25b0	Standard query (0)	ipv4bot.whatismyipaddress.com	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: wThN5MTIsw.exe PID: 6388, Parent PID: 4180

General

Target ID:	0
Start time:	23:56:59
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\wThN5MTIsw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\wThN5MTIsw.exe"
Imagebase:	0xf4e0000
File size:	71680 bytes
MD5 hash:	1813521F3884DE8427728B54B5C9A391
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: 00000000.00000002.335673365.000000000F4EA000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000000.00000002.335680061.000000000F4F2000.00000004.00000001.01000000.00000003.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: 00000000.00000003.334936467.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000000.00000003.334936467.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000003.334936467.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000000.00000003.334936467.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000000.00000003.334936467.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000000.00000003.334936467.0000000003170000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000000.00000000.321170731.000000000F4EA000.00000002.00000001.01000000.00000003.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\ssapst.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F4E2852	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\ssapst.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 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 fd fd fd fd 59 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 b0 42 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 00 50 45 00 00 4c 01 06	MZ@!L!This Ym cannot be run in DOS mode.$}BB1YG~y|RichP EL	success or wait	1	F4E286F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\wThN5MTIsw.exe	unknown	71680	success or wait	1	F4E3652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	qxcdehgjaib	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	F4E2AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **6592**, Parent PID: **3528**

General

Target ID:	2
Start time:	23:57:13
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000002.00000002.370323598.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000000.354396039.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000002.00000002.370333139.000000000FE72000.00000004.00000001.01000000.00000004.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: 00000002.00000003.369602233.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000002.00000003.369602233.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000002.00000003.369602233.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000002.00000003.369602233.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000002.00000003.369602233.0000000003640000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000002.00000003.369602233.0000000003640000.00000004.00001000.00020000.00000000.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\ssapst.exe, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: C:\Users\user\AppData\Roaming\Microsoft\ssapst.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	ocipuxittak	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **6840**, Parent PID: **3528**

General

Target ID:	4
Start time:	23:57:24
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000004.00000003.382524367.00000000038C0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000004.00000002.383041261.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000004.00000000.373713609.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000004.00000002.383047915.000000000FE72000.00000004.00000001.01000000.00000004.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	trtwjkdvbrs	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **7028**, Parent PID: **3528**

General

Target ID:	6
Start time:	23:57:32
Start date:	31/08/2022

Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000006.00000002.406382399.000000000FE6A000.00000002.00000001.01000000.00000004.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: 00000006.00000003.405218158.0000000002F70000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000006.00000003.405218158.0000000002F70000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000006.00000003.405218158.0000000002F70000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000006.00000003.405218158.0000000002F70000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000006.00000003.405218158.0000000002F70000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000006.00000003.405218158.0000000002F70000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000006.00000000.391649222.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000006.00000002.406483395.000000000FE72000.00000004.00000001.01000000.00000004.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	ftylkauykkg	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: 5668, Parent PID: 3528

General

Target ID:	8
Start time:	23:57:40
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000008.00000002.421043250.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000008.00000002.421052694.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000008.00000000.408927489.000000000FE6A000.00000002.00000001.01000000.00000004.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: 00000008.00000003.419920296.00000000030F0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000008.00000003.419920296.00000000030F0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000008.00000003.419920296.00000000030F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000008.00000003.419920296.00000000030F0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000008.00000003.419920296.00000000030F0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000008.00000003.419920296.00000000030F0000.00000004.00001000.00020000.00000000.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	biktigczvpq	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **6104**, Parent PID: **3528**

General

Target ID:	12
Start time:	23:57:48
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 0000000C.00000002.445300926.000000000FE72000.00000004.00000001.01000000.00000004.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: 0000000C.00000003.444009772.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000C.00000003.444009772.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000003.444009772.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000C.00000003.444009772.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000C.00000003.444009772.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000C.00000003.444009772.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000000.426845599.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000C.00000002.445271222.000000000FE6A000.00000002.00000001.01000000.00000004.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	rjjumyjxpew	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **4292**, Parent PID: **3528**

General

Target ID:	14
Start time:	23:57:57
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 0000000E.00000000.444554151.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000E.00000002.457737689.000000000FE72000.00000004.00000001.01000000.00000004.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: 0000000E.00000003.456730321.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000E.00000003.456730321.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000003.456730321.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000E.00000003.456730321.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000E.00000003.456730321.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000E.00000003.456730321.0000000003730000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000E.00000002.457728648.000000000FE6A000.00000002.00000001.01000000.00000004.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	ypcrxwqpxuk	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **1416**, Parent PID: **3528**

General

Target ID:	15
Start time:	23:58:05
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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.00000002.485778645.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000000.462423463.000000000FE6A000.00000002.00000001.01000000.00000004.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.00000003.484382333.0000000003300000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000000F.00000003.484382333.0000000003300000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000000F.00000003.484382333.0000000003300000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000000F.00000003.484382333.0000000003300000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000000F.00000003.484382333.0000000003300000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000000F.00000003.484382333.0000000003300000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000000F.00000002.485790617.000000000FE72000.00000004.00000001.01000000.00000004.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	qtytdguwutr	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **3588**, Parent PID: **3528**

General

Target ID:	17
Start time:	23:58:14
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000011.00000002.485870462.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000011.00000000.482554766.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **3248**, Parent PID: **3528**

General

Target ID:	18
Start time:	23:58:23
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000012.00000000.500809556.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000012.00000002.520951774.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000012.00000002.521001527.000000000FE72000.00000004.00000001.01000000.00000004.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: 00000012.00000003.513687059.0000000003230000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000012.00000003.513687059.0000000003230000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000012.00000003.513687059.0000000003230000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000012.00000003.513687059.0000000003230000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000012.00000003.513687059.0000000003230000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000012.00000003.513687059.0000000003230000.00000004.00001000.00020000.00000000.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\ssapst.exe	unknown	71680	success or wait	1	FE63652	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	hdwqlmoiwuh	unicode	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"	success or wait	1	FE62AAA	RegSetValueExW

Analysis Process: ssapst.exe PID: **6228**, Parent PID: **3528**

General	
Target ID:	19
Start time:	23:58:37
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000013.00000002.556440908.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000000.531056963.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000013.00000002.556559672.000000000FE72000.00000004.00000001.01000000.00000004.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: 00000013.00000003.550407327.0000000003520000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000013.00000003.550407327.0000000003520000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000013.00000003.550407327.0000000003520000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000013.00000003.550407327.0000000003520000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000013.00000003.550407327.0000000003520000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000013.00000003.550407327.0000000003520000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Analysis Process: ssapst.exe PID: **5016**, Parent PID: **3528**

General	
Target ID:	22
Start time:	23:58:45
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000016.00000000.548829843.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000016.00000002.553896559.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **7020**, Parent PID: **3528**

General	
Target ID:	24
Start time:	23:58:55
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000018.00000002.585820146.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000018.00000000.570376945.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000018.00000002.585796532.000000000FE6A000.00000002.00000001.01000000.00000004.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: 00000018.00000003.584737437.0000000003B60000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000018.00000003.584737437.0000000003B60000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000018.00000003.584737437.0000000003B60000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000018.00000003.584737437.0000000003B60000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000018.00000003.584737437.0000000003B60000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000018.00000003.584737437.0000000003B60000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Analysis Process: ssapst.exe PID: **7108**, Parent PID: **3528**

General

Target ID:	25
Start time:	23:59:04
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000019.00000000.588245655.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000019.00000002.608758289.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000002.608744037.000000000FE6A000.00000002.00000001.01000000.00000004.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: 00000019.00000003.601841912.00000000036D0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000019.00000003.601841912.00000000036D0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000019.00000003.601841912.00000000036D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000019.00000003.601841912.00000000036D0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000019.00000003.601841912.00000000036D0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000019.00000003.601841912.00000000036D0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs
Reputation:	low

Analysis Process: ssapst.exe PID: **204**, Parent PID: **3528**

General

Target ID:	26
Start time:	23:59:13
Start date:	31/08/2022

Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 0000001A.00000003.625461976.0000000003830000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001A.00000003.625461976.0000000003830000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001A.00000003.625461976.0000000003830000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001A.00000003.625461976.0000000003830000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001A.00000003.625461976.0000000003830000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001A.00000003.625461976.0000000003830000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001A.00000002.628240997.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 0000001A.00000002.628251824.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001A.00000000.608029027.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **4804**, Parent PID: **3528**

General

Target ID:	30
Start time:	23:59:21
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 0000001E.00000002.654951583.000000000FE72000.00000004.00000001.01000000.00000004.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: 0000001E.00000003.653635490.0000000002FC0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 0000001E.00000003.653635490.0000000002FC0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000003.653635490.0000000002FC0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 0000001E.00000003.653635490.0000000002FC0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 0000001E.00000003.653635490.0000000002FC0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 0000001E.00000003.653635490.0000000002FC0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000000.626543672.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001E.00000002.654935793.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **5952**, Parent PID: **3528**

General

Target ID:	31
Start time:	23:59:31

Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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.00000000.648211037.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 0000001F.00000002.651985737.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **1784**, Parent PID: **3528**

General

Target ID:	32
Start time:	23:59:40
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000020.00000003.679180879.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000020.00000003.679180879.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000020.00000003.679180879.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000020.00000003.679180879.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000020.00000003.679180879.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000020.00000003.679180879.0000000003790000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000020.00000002.681984770.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000020.00000000.666637056.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000020.00000002.682007928.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **5076**, Parent PID: **3528**

General

Target ID:	33
Start time:	23:59:49
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000021.00000003.701450302.0000000003D30000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000021.00000003.701450302.0000000003D30000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000021.00000003.701450302.0000000003D30000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000021.00000003.701450302.0000000003D30000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000021.00000003.701450302.0000000003D30000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000021.00000003.701450302.0000000003D30000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000021.00000002.703365325.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000021.00000000.688032587.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000021.00000002.703345921.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **5700**, Parent PID: **3528**

General

Target ID:	34
Start time:	23:59:58
Start date:	31/08/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24
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: 00000022.00000002.734717569.000000000FE6A000.00000002.00000001.01000000.00000004.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: 00000022.00000003.731764683.00000000032A0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_RANSOMWARE_Indicator_Jul20, Description: Detects ransomware indicator, Source: 00000022.00000003.731764683.00000000032A0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000022.00000003.731764683.00000000032A0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_ReflectiveLoader, Description: detects Reflective DLL injection artifacts, Source: 00000022.00000003.731764683.00000000032A0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Gandcrab, Description: Gandcrab Payload, Source: 00000022.00000003.731764683.00000000032A0000.00000004.00001000.00020000.00000000.sdmp, Author: kevoreilly • Rule: Win32_Ransomware_GandCrab, Description: unknown, Source: 00000022.00000003.731764683.00000000032A0000.00000004.00001000.00020000.00000000.sdmp, Author: ReversingLabs • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000022.00000000.705195952.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_Gandcrab, Description: Yara detected Gandcrab, Source: 00000022.00000002.734737605.000000000FE72000.00000004.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ssapst.exe PID: **972**, Parent PID: **3528**

General

Target ID:	35
Start time:	00:00:07
Start date:	01/09/2022
Path:	C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ssapst.exe"
Imagebase:	0xfe60000
File size:	71680 bytes
MD5 hash:	C99BAB5FEA91C0938D1D5B6684158B24

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: 00000023.00000000.730367046.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_ReflectiveLoader, Description: Yara detected ReflectiveLoader, Source: 00000023.00000002.734163456.000000000FE6A000.00000002.00000001.01000000.00000004.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly