ID: 831157
Sample Name: aeICl0Aabv.exe
Cookbook: default.jbs
Time: 07:06:10
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

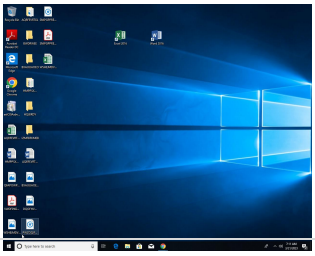
Windows Analysis Report

aeICl0Aabv.exe

Overview

General Information

Sample Name:	aeICl0Aabv.exe
Original Sample Name:	0192d35c916b…
Analysis ID:	831157
MD5:	0192d35c916b…
SHA1:	9480935bca8e…
SHA256:	06736e8c8a3d…
Tags:	exe RedLineStealer
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

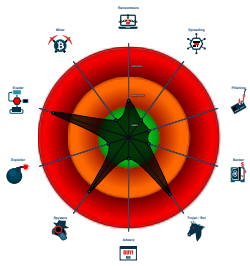
Amadey, RedLine

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Disable Windows Defender real time…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- aeICl0Aabv.exe (PID: 2948 cmdline: C:\Users\user\Desktop\aeICl0Aabv.exe MD5: 0192D35C916B3A26132CEF7DD09DBABE)
  - zap9052.exe (PID: 1392 cmdline: C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe MD5: 099A593A4B3A2B670832798FFFEF0987)
    - zap9953.exe (PID: 3324 cmdline: C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe MD5: FCE6A8713A6F6A9B3B40FB5A6F39D51F)
      - zap8476.exe (PID: 5416 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe MD5: FB7A56568450CF705F26C6C9FD80CCE2)
        - tz5602.exe (PID: 5396 cmdline: C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe MD5: 7E93BACBBC33E6652E147E7FE07572A0)
        - v7930id.exe (PID: 5852 cmdline: C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe MD5: 293C64D08567381D93D7CC071C4F0B3A)
- rundll32.exe (PID: 5868 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\ MD5: 73C519F050C20580F8A62C849D49215A)
- rundll32.exe (PID: 2140 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP001.TMP\ MD5: 73C519F050C20580F8A62C849D49215A)
- rundll32.exe (PID: 5104 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\ MD5: 73C519F050C20580F8A62C849D49215A)
- rundll32.exe (PID: 5044 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP003.TMP\ MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Amadey	Amadey is a botnet that appeared around October 2018 and is being sold for about 500$ on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.	No Attribution	**http://** https://asec.ahnlab.com/en/36634/https://asec.ahnlab.com/en/41450/https://asec.ahnlab.com/en/44504/https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-becomehttps://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.html	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey

Name	Description	Attribution	Blogpost URLs	Link
RedLine Stealer	RedLine Stealer is a malware available on underground forums for sale apparently as standalone ($100/$150 depending on the version) or also on a subscription basis ($100/month). This malware harvests information from browsers such as saved credentials, autocomplete data, and credit card information. A system inventory is also taken when running on a target machine, to include details such as the username, location data, hardware configuration, and information regarding installed security software. More recent versions of RedLine added the ability to steal cryptocurrency. FTP and IM clients are also apparently targeted by this family, and this malware has the ability to upload and download files, execute commands, and periodically send back information about the infected computer.	No Attribution	**http://** https://asec.ahnlab.com/en/30445/https://asec.ahnlab.com/en/35981/https://asec.ahnlab.com/ko/25837/https://bartblaze.blogspot.com/2021/06/digital-artists-targeted-in-redline.htmlhttps://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "62.204.41.87/joomla/index.php",
  "Version": "3.68"
}
```


Threatname: RedLine


```
{
  "C2 url": "193.233.20.30:4125",
  "Bot Id": "vint",
  "Authorization Header": "fb8811912f8370b3d23bffda092d88d0"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a440:$pat14: , CommandLine: • 0x134ad:$v2_1: ListOfProcesses • 0x1328c:$v4_3: base64str • 0x13e05:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12814:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
C:\Users\user\AppData\Local\Temp\IXP000.TMP\y89Te35.exe	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.306492758.0000000000400000.00000040.00000001.01000000.0000000A.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000006.00000002.306492758.0000000000400000.00000040.00000001.01000000.0000000A.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x1300:$s3: 83 EC 38 53 B0 C4 88 44 24 2B 88 44 24 2F B0 3F 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.

Source	Rule	Description	Author	Strings
00000006.00000002.306673569.00000000004F0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000006.00000002.306673569.00000000004F0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000006.00000002.306894968.00000000006A6000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x1690:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.zap9052.exe.10eda20.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.3.zap9052.exe.10eda20.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x18840:$pat14: , CommandLine: • 0x118ad:$v2_1: ListOfProcesses • 0x1168c:$v4_3: base64str • 0x12205:$v4_4: stringKey • 0xff63:$v4_5: BytesToStringConverted • 0xf176:$v4_6: FromBase64 • 0x10498:$v4_8: procName • 0x10c14:$v5_5: FileScanning • 0x1016c:$v5_7: RecordHeaderField • 0xfe34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
6.2.v7930id.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
6.2.v7930id.exe.400000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x1300:$s3: 83 EC 38 53 B0 C4 88 44 24 2B 88 44 24 2F B0 3F 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
6.2.v7930id.exe.4f0e67.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 9 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

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Lowering of HIPS / PFW / Operating System Security Settings

Disable Windows Defender real time protection (registry)

Disable Windows Defender notifications (registry)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Remote Access Functionality

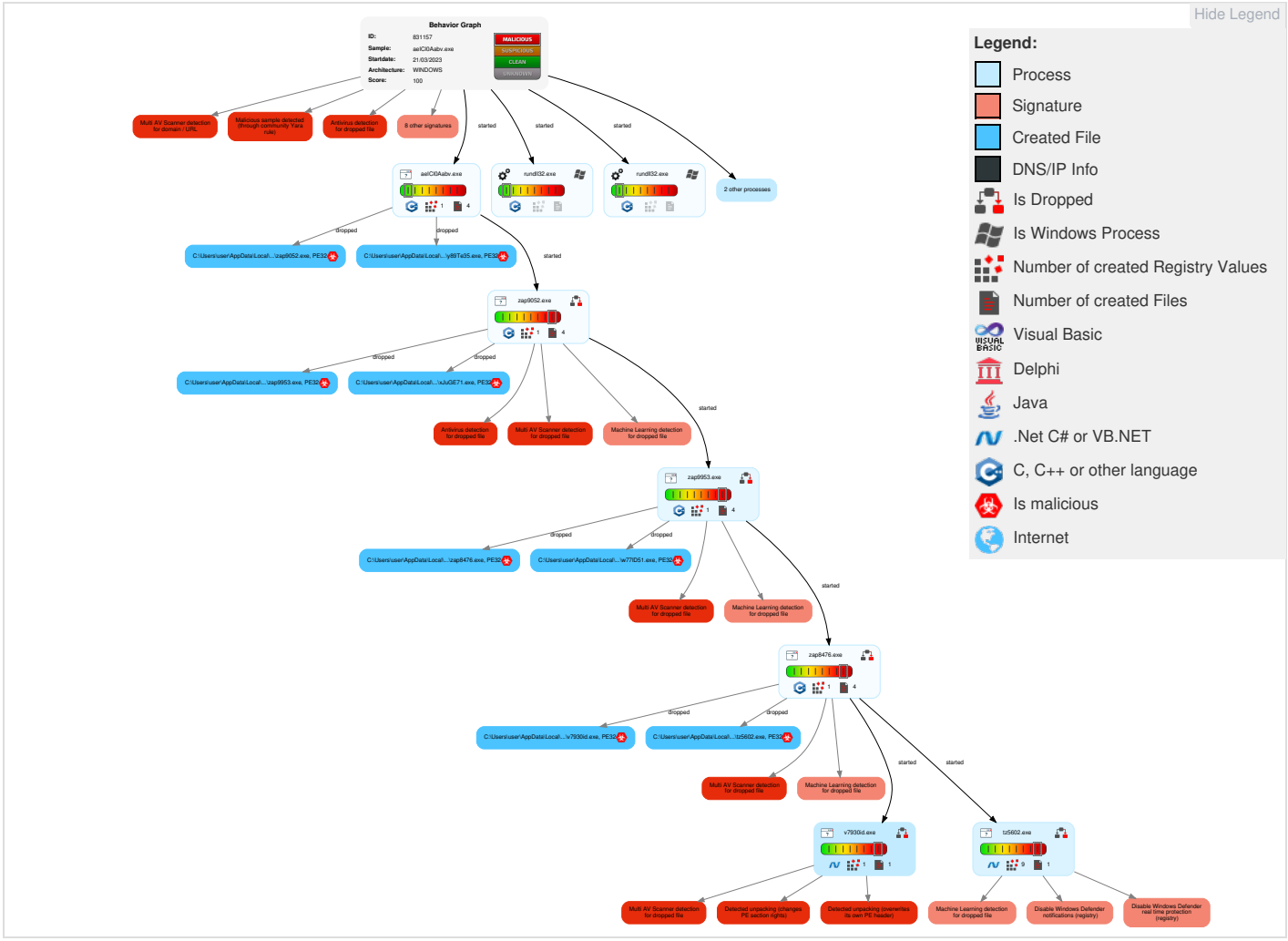
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 Windows Service	2 Bypass User Access Control	2 1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Service Execution	Logon Script (Windows)	1 Windows Service	2 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Process Injection	2 Software Packing	NTDS	2 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 3 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Bypass User Access Control	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	2 Process 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	2 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 System Owner/User 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)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
aeICl0Aabv.exe	62%	ReversingLabs	Win32.Trojan.Plugx	
aeICl0Aabv.exe	58%	Virustotal		Browse
aeICl0Aabv.exe	100%	Avira	HEUR/AGEN.1252166	
aeICl0Aabv.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\y89Te35.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\w77ID51.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\y89Te35.exe	92%	ReversingLabs	Win32.Spyware.RedLine	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\y89Te35.exe	85%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe	67%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe	61%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	88%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	78%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe	54%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe	56%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP002.TMP\w77ID51.exe	43%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\w77ID51.exe	46%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe	67%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe	88%	ReversingLabs	ByteCode-MSIL.Trojan.Casdet	
C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe	49%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.aeICl0Aabv.exe.50000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
2.3.zap9953.exe.47be620.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.aeICl0Aabv.exe.50000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
3.3.zap8476.exe.4f27c20.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.zap9052.exe.12e0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
1.0.zap9052.exe.12e0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
193.233.20.30:4125	0%	URL Reputation	safe	
62.204.41.87/joomla/index.php	0%	Avira URL Cloud	safe	
62.204.41.87/joomla/index.php	13%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
62.204.41.87/joomla/index.php	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	low

Name	Malicious	Antivirus Detection	Reputation
193.233.20.30:4125	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	zap9052.exe, 00000001.00000003.247343724.000000000104F000.00000004.00000020.00020000.00000000.sdmp, xJuGE71.exe.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831157
Start date and time:	2023-03-21 07:06:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	22
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
Sample file name:	aeICl0Aabv.exe
Original Sample Name:	0192d35c916b3a26132cef7dd09dbabe.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@15/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 47.5% (good quality ratio 45.5%) • Quality average: 85.1% • Quality standard deviation: 23.9%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.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 NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\tz5602.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZilv:Q3La/KDLI4MWuPTxAlv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\v7930id.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.355221377978991
Encrypted:	false
SSDEEP:	6:Q3La/xwchM3RJoDLIP12MUAvvR+uCqDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21v
MD5:	03C5BA5FCE7124B503EA65EF522177C3
SHA1:	F76B1F538D5EA66664355901E927B2F870ACCDD8
SHA-256:	8128CE419BBE0419F1A0BDE97C3A14E3377C0184DC1D7AF61AA01AAB756B625B

SHA-512:	151A974DDABA852144EC4BC18C548227A32E5261736F186A3920F2497434AEE9DBB0E0AB77E0E52A84A9FBC4529A158882B7549763400DDC2082D384B1135141
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Temp\IXP000.TMP\y89Te35.exe

Process:	C:\Users\user\Desktop\aeICl0Aabv.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	241152
Entropy (8bit):	6.346560230971658
Encrypted:	false
SSDEEP:	6144:f36hrz456we4lz7zzZ5my2IuViMqJnyJQ:Pxpz7LmeuVi3nN
MD5:	5086DB99DE54FCA268169A1C6CF26122
SHA1:	003F768FFCC99BDA5CDA1FB966FDA8625A8FDC3E
SHA-256:	42873B0C5899F64B5F3205A4F3146210CC63152E529C69D6292B037844C81EC4
SHA-512:	90531B1B984B21CE62290B713FFC07917BBD766EEF7D5E6F4C1C68B2FC7D29495CDD5F05FD71FE5107F1614BBB30922DCFB730F50599E44AEAFF52C50F46B8E5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\y89Te35.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 92% • Antivirus: Virustotal, Detection: 85%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]..M.o...o...o..B....o..B....o..B....o.....o.....o.....5o..B....o...o...o.....o....m..o.....o..Rich.o.....PE..L...:[.d.....Ut.....@.....@.....xp..d.....(..pC..p.....D.....C..@.....text..... ..`.rdata.. .....@..@.data...H'.....j.....@....rsrc.....@..@.reloc...(.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe

Process:	C:\Users\user\Desktop\aeICl0Aabv.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	795648
Entropy (8bit):	7.906970785388822
Encrypted:	false
SSDEEP:	12288:KMrfy90y7gnSzY55gb3+JoD+m8Ln0kDdoFLZS7pNBFoDztlS3SX/DZIRdqxwk/SH:ly77gqOJo20kSnSVpOtlZS3ZtH
MD5:	099A593A4B3A2B670832798FFFEF0987
SHA1:	D55750831158F1E72B65678CFA53C021EE34E7C5
SHA-256:	886CFA4C68A576CBEB743EFD8C00D97E720D45BCE4A4195D591D2A274ACAB905
SHA-512:	F9BD1AEF78395FC91C1E368C01E747BBACE5E701588A614EF2CC0F7DF64D19C2CF8CA4C3FE88968E44A3288910E7E7579068A5A7B3F7FCC96385F1245FA0484
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67% • Antivirus: Virustotal, Detection: 61%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...K..K..K...N..K...H..K...O..K...J..K..J...K...C..K.....K...I..K.Rich..K.....PE..L....`.b.....d.....`j.....@.....p.....B#....@..... .....`.....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	179200
Entropy (8bit):	4.95425936878501
Encrypted:	false
SSDEEP:	3072:VxqZWjfa8oty3QqECU8eUcFShTnxNn2pU9f2MKTV/wi4lr55R9TxlnsPsUw0jOuu:fqZCQqElPSh
MD5:	3389637C0D072121BF1B127629736D37

SHA1:	300E915EFDF2479BFD0D3699C0A6BC51260F9655
SHA-256:	2B74C4CE2674A8FC0C78FFFA39C5DE5E43AE28B8BF425349A5F97C6A61135153
SHA-512:	A32CC060D2600F6CA94FFDCE07C95EA5E2F56C0B418260456B568CB41E5F55DB0C4FC97C35CA4103C674E61A17300D834D2C0DA5A78B7084B6BC342FD23A7F B4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Virustotal, Detection: 78%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. ....@.....8...O.....,..... ....H.....text..... ....`.rsrc...,.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	649728
Entropy (8bit):	7.874818956122623
Encrypted:	false
SSDEEP:	12288:PMr9y90bUgLn0gDd24VYenpgByx2/JaB3oXTDZIydQxwkrn:Wy80gApepTx2XSKf4
MD5:	FCE6A8713A6F6A9B3B40FB5A6F39D51F
SHA1:	21952BFB7DC453FD83179492C5D13558567BF0D4
SHA-256:	AFD3690658BC11279995363D35C734C086F6AA3B6944912C78E261115D6ADF21
SHA-512:	99CCE86C86C7462651011FA8F84DFEC744ED9FA9ED8119A431FAFB37A215602A6AD8958029370EE2EBB568B88869AFF502C3CE4D1F3356B63F9BB4AE2125621 B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 54% • Antivirus: Virustotal, Detection: 56%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...K..K..K...N..K...H..K...O..K...J..K..J...K...C..K.....K...I..K.Ric h..K.....PE..L....`.b.....d.....`j.....@.....@.....h....@..... .....b.....0.....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc....p.....d...|.....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\w77lD51.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	294912
Entropy (8bit):	7.399210694110962
Encrypted:	false
SSDEEP:	6144:i4nHaV3pMKs+tDZIydWSC1xwkIyHZJe1:i4nHaV3jBtDZIydMxwkIMe
MD5:	CBE7F23A5F54722AACC67EBD9085397F
SHA1:	48713739E12BA90E5ECA13DE33640B05AA16F8DE
SHA-256:	2AC363ABD934EF9ADCA77D685F60A74E10808FAA1AE801090F0486EF6E5B4794
SHA-512:	CA853FDE313ECB3FA83BC55B89444470699A0C44BB9BF4C01F142C616125606AA21B02422E63C7A56BA8FA11479E81878CBF81FA64439DC38327E61F248F3D82
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43% • Antivirus: Virustotal, Detection: 46%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f.Q.f.Q.f.Q...Q.f.Q..4Q.f.Q...Q.f.Q..9Q.f.Q.f.Q.f.Q...Q.f.Q..0Q.f.Q ..7Q.f.QRich.f.Q.....PE..L...96eb...../.....@.....I.....<.....*..@..... .....text..... ..`.data...,.....@....vazaweh.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	321024
Entropy (8bit):	7.65025522410403
Encrypted:	false
SSDEEP:	6144:KVy+bnr+vp0yN90QEvVfTM8huv7p3pJwtWs5BenWxDp3BK1x2p:DMrTy90BVIOGpUrHeqp3Byx2p
MD5:	FB7A56568450CF705F26C6C9FD80CCE2
SHA1:	85528F8E87BEF1973DB70F835D10D968A0715B2D
SHA-256:	2D1CB286FA2471168CA6F6305F41272B781BEB0FB872B16F15427EE6967B4249
SHA-512:	1103044E07EFAF98E1F12BF1044A606A1ACA460446C42E8FBDF03B03B936E0D5B7EB4BF0018BA2A12735723DFCCBC8E5FE85BE17FD391FED25F1ED5F08523DD5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...K..K..K...N..K...H..K...O..K...J..K..J...K...C..K.....K...I..K.Rich..K.....PE..L....`.b.....d...~.....`j.....@.....0.....z....@..... .....l_..... .....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc....`.....`...|.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	4.97029807367379
Encrypted:	false
SSDEEP:	96:yA/vMth9sDLibql3A44P9QL4fwmPImg+A03PvXLOzk+gqWYV4J6oP/zNt:yw+wGWt94+iANiCkc4Jhp
MD5:	7E93BACBBC33E6652E147E7FE07572A0
SHA1:	421A7167DA01C8DA4DC4D5234CA3DD84E319E762
SHA-256:	850CD190AAEEBCF1505674D97F51756F325E650320EAF76785D954223A9BEE38
SHA-512:	250169D7B6FCEBFF400BE89EDAE8340F14130CED70C340BA9DA9F225F62B52B35F6645BFB510962EFB866F988688CB42392561D3E6B72194BC89D310EA43AA91
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..".....@... ...`....@.. ..... .@.....@..O....`.....@..8..... ....H.....text.... ... ..."..... ..`.rsrc.....`.....$.....@..@.relo c.....*.....@..B.....@.....H.....T$.....0.....@s.....@...(....&*..0..K..... ?...(.....~....(.....*r...p.....(....%..(....& ....(....(....&.(....&*..0..e.....(....~.....+G.....o....r#..p(....,-.o.... .....(....-.*.(....&(.....o....(....&..X....i2..(....&*....0..`.....(....~.....+B.....o....r...p(....,(.o.... .....(....-.*.(....&.o....(....&..X....i2..(....&*.0..c..... ?...(.....~....(.....,*....(.....%...(...

C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	235520
Entropy (8bit):	7.1650349685088575
Encrypted:	false
SSDEEP:	3072:oWaA4/Oci2WX3TqCGDbYQ9/IfB8KrYytJl6aRn3YIiiIrbnILLKXJl9U35Z:T42VmCGDbz9BB87yte6qn7NnEWDy
MD5:	293C64D08567381D93D7CC071C4F0B3A
SHA1:	59AA22EE71B37B4B264B979DA0A56B03563593EB
SHA-256:	0A06D02AF688F2E7F1057969489E302867FAB3FCABD5ABB909E1F30212EDBC22
SHA-512:	BAC16DD74BDB4591D29E1A3163642C793403A9BBF082B3E16FB7EF6632AF9327AE0123290892279D915DE8F0897B6456DEB7597011B53A168374575856C7908D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 49%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f.Q.f.Q.f.Q...Q.f.Q..4Q.f.Q...Q.f.Q..9Q.f.Q.f.Q.f.Q...Q.f.Q..0Q.f.Q..7Q.f.QRich.f.Q.....PE..L.....a...../.....@.....<.....*..@..... .....text..... ..`.data...,.....@....nakulor.....@....rsrc.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.931003449191294
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:	aeICl0Aabv.exe
File size:	974848
MD5:	0192d35c916b3a26132cef7dd09dbabe
SHA1:	9480935bca8e7c22c379e894633ad59acae0c871
SHA256:	06736e8c8a3dafb02d3ce28f9917f7e79e37b6a0d998c375b91d7029ef356da5
SHA512:	614d1a0159834c7d8ca086455366912beba7398d9764fa21d6f4e05015d31abf4d4d9ffe289379848858e12a09cf4ae4cf17348d8182336aab3e9965679ba03b
SSDEEP:	24576:syFzLdzags/31Oqoj83ZR2hJzSknQBlL13M64C:bhFaXOqoj83ZVT5MF
TLSH:	7D252246AAFA9077E5B817706AF742930E367EE15CF4836723C6990A0DB33C46975323
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...K...K...K...N...K...H...K...O...K...J...K...J...K...C...K.....K...I...K.Rich..K.....PE..L....`.b.....d.

File Icon

Icon Hash:	f8e0e4e8ecccc870

Static PE Info

General

Entrypoint:	0x406a60
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x628D60E2 [Tue May 24 22:49:06 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	10
OS Version Minor:	0
File Version Major:	10
File Version Minor:	0
Subsystem Version Major:	10
Subsystem Version Minor:	0
Import Hash:	646167cce332c1c252cdcb1839e0cf48

Entrypoint Preview

Instruction
call 00007F4C18BDAAA5h
jmp 00007F4C18BDA3B5h
push 00000058h
push 004072B8h
call 00007F4C18BDAB47h
xor ebx, ebx
mov dword ptr [ebp-20h], ebx
lea eax, dword ptr [ebp-68h]
push eax
call dword ptr [0040A184h]
mov dword ptr [ebp-04h], ebx
mov eax, dword ptr fs:[00000018h]

Instruction
mov esi, dword ptr [eax+04h]
mov edi, ebx
mov edx, 004088ACh
mov ecx, esi
xor eax, eax
lock cmpxchg dword ptr [edx], ecx
test eax, eax
je 00007F4C18BDA3CAh
cmp eax, esi
jne 00007F4C18BDA3B9h
xor esi, esi
inc esi
mov edi, esi
jmp 00007F4C18BDA3C2h
push 000003E8h
call dword ptr [0040A188h]
jmp 00007F4C18BDA389h
xor esi, esi
inc esi
cmp dword ptr [004088B0h], esi
jne 00007F4C18BDA3BCh
push 0000001Fh
call 00007F4C18BDA8DBh
pop ecx
jmp 00007F4C18BDA3ECh
cmp dword ptr [004088B0h], ebx
jne 00007F4C18BDA3DEh
mov dword ptr [004088B0h], esi
push 004010C4h
push 004010B8h
call 00007F4C18BDA506h
pop ecx
pop ecx
test eax, eax
je 00007F4C18BDA3C9h
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, 000000FFh
jmp 00007F4C18BDA4E9h
mov dword ptr [004081E4h], esi
cmp dword ptr [004088B0h], esi
jne 00007F4C18BDA3CDh
push 004010B4h
push 004010ACh
call 00007F4C18BDAA95h
pop ecx
pop ecx
mov dword ptr [000088B0h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa28c	0xb4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0xe5824	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf2000	0x888	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1410	0x54	.text
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	0x1008	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa000	0x288	.idata
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	0x6314	0x6400	False	0.5744140625	data	6.314163792045976	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x8000	0x1a48	0x200	False	0.609375	data	4.970639543960129	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xa000	0x1052	0x1200	False	0.4140625	data	5.025949912909207	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0xe6000	0xe5a00	False	0.9672242872210125	data	7.95183138593728	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf2000	0x888	0xa00	False	0.746484375	data	6.222637930812128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AVI	0xc9f8	0x2e1a	RIFF (little-endian) data, AVI, 272 x 60, 10.00 fps, video: RLE 8bpp	English	United States
RT_ICON	0xf814	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0xfe7c	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x10164	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	English	United States
RT_ICON	0x1034c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_ICON	0x10474	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x1131c	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x11bc4	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	English	United States
RT_ICON	0x1228c	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x127f4	0xd9d2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x201c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x22770	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x23818	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x241a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x24608	0x2f2	data	English	United States
RT_DIALOG	0x248fc	0x1b0	data	English	United States
RT_DIALOG	0x24aac	0x166	data	English	United States
RT_DIALOG	0x24c14	0x1c0	data	English	United States
RT_DIALOG	0x24dd4	0x130	data	English	United States
RT_DIALOG	0x24f04	0x120	data	English	United States
RT_STRING	0x25024	0x8c	Matlab v4 mat-file (little endian) l, numeric, rows 0, columns 0	English	United States
RT_STRING	0x250b0	0x520	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x255d0	0x5cc	data	English	United States
RT_STRING	0x25b9c	0x4b0	data	English	United States
RT_STRING	0x2604c	0x44a	data	English	United States
RT_STRING	0x26498	0x3ce	data	English	United States
RT_RCDATA	0x26868	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0x26870	0xca296	Microsoft Cabinet archive data, many, 828054 bytes, 2 files, at 0x2c +A "zap9052.exe" +A "y89Te35.exe", ID 1798, number 1, 32 datablocks, 0x1503 compression	English	United States
RT_RCDATA	0xf0b08	0x4	data	English	United States
RT_RCDATA	0xf0b0c	0x24	data	English	United States
RT_RCDATA	0xf0b30	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xf0b38	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xf0b40	0x4	data	English	United States
RT_RCDATA	0xf0b44	0xc	data	English	United States
RT_RCDATA	0xf0b50	0x4	data	English	United States
RT_RCDATA	0xf0b54	0xc	data	English	United States
RT_RCDATA	0xf0b60	0x4	data	English	United States
RT_RCDATA	0xf0b64	0x5	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xf0b6c	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xf0b74	0x7	ASCII text, with no line terminators	English	United States
RT_GROUP_ICON	0xf0b7c	0xbc	data	English	United States
RT_VERSION	0xf0c38	0x408	data	English	United States
RT_MANIFEST	0xf1040	0x7e2	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	GetTokenInformation, RegDeleteValueA, RegOpenKeyExA, RegQueryInfoKeyA, FreeSid, OpenProcessToken, RegSetValueExA, RegCreateKeyExA, LookupPrivilegeValueA, AllocateAndInitializeSid, RegQueryValueExA, EqualSid, RegCloseKey, AdjustTokenPrivileges
KERNEL32.dll	_lopen, _llseek, CompareStringA, GetLastError, GetFileAttributesA, GetSystemDirectoryA, LoadLibraryA, DeleteFileA, GlobalAlloc, GlobalFree, CloseHandle, WritePrivateProfileStringA, IsDBCSLeadByte, GetWindowsDirectoryA, SetFileAttributesA, GetProcAddress, GlobalLock, LocalFree, RemoveDirectoryA, FreeLibrary, _lclose, CreateDirectoryA, GetPrivateProfileIntA, GetPrivateProfileStringA, GlobalUnlock, ReadFile, SizeofResource, WriteFile, GetDriveTypeA, lstrcmpA, SetFileTime, SetFilePointer, FindResourceA, CreateMutexA, GetVolumeInformationA, ExpandEnvironmentStringsA, GetCurrentDirectoryA, FreeResource, GetVersion, SetCurrentDirectoryA, GetTempPathA, LocalFileTimeToFileTime, CreateFileA, SetEvent, TerminateThread, GetVersionExA, LockResource, GetSystemInfo, CreateThread, ResetEvent, LoadResource, ExitProcess, GetModuleHandleW, CreateProcessA, FormatMessageA, GetTempFileNameA, DosDateTimeToFileTime, CreateEventA, GetExitCodeProcess, FindNextFileA, LocalAlloc, GetShortPathNameA, MulDiv, GetDiskFreeSpaceA, EnumResourceLanguagesA, GetTickCount, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, QueryPerformanceCounter, TerminateProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, GetStartupInfoW, Sleep, FindClose, GetCurrentProcess, FindFirstFileA, WaitForSingleObject, GetModuleFileNameA, LoadLibraryExA
GDI32.dll	GetDeviceCaps
USER32.dll	SetWindowLongA, GetDlgItemTextA, DialogBoxIndirectParamA, ShowWindow, MsgWaitForMultipleObjects, SetWindowPos, GetDC, GetWindowRect, DispatchMessageA, GetDesktopWindow, CharUpperA, SetDlgItemTextA, ExitWindowsEx, MessageBeep, EndDialog, CharPrevA, LoadStringA, CharNextA, EnableWindow, ReleaseDC, SetForegroundWindow, PeekMessageA, GetDlgItem, SendMessageA, SendDlgItemMessageA, MessageBoxA, SetWindowTextA, GetWindowLongA, CallWindowProcA, GetSystemMetrics
msvcrt.dll	_controlfp, ?terminate@@YAXXZ, _acmdln, _initterm, __setusermatherr, _except_handler4_common, memcpy, _ismbblead, __p__fmode, _cexit, _exit, exit, __set_app_type, __getmainargs, _amsg_exit, __p__commode, _XcptFilter, memcpy_s, _vsnprintf, memset
COMCTL32.dll	
Cabinet.dll	
VERSION.dll	GetFileVersionInfoA, VerQueryValueA, GetFileVersionInfoSizeA

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior

System Behavior

Analysis Process: aeICl0Aabv.exe PID: **2948**, Parent PID: **3452**

General

Target ID:	0
Start time:	07:07:02
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\aeICl0Aabv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\aeICl0Aabv.exe
Imagebase:	0x50000
File size:	974848 bytes
MD5 hash:	0192D35C916B3A26132CEF7DD09DBABE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000003.246587631.000000000464E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup0	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\"	success or wait	1	52243	RegSetValueExA

Analysis Process: zap9052.exe PID: **1392**, Parent PID: **2948**

General

Target ID:	1
Start time:	07:07:03
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\zap9052.exe
Imagebase:	0x12e0000
File size:	795648 bytes
MD5 hash:	099A593A4B3A2B670832798FFFEF0987
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000003.247343724.000000000104F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs • Detection: 61%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12E5458	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\TMP4351$.TMP	read attributes | delete | synchronize | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	12E5949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	12E48E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	12E48E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe	success or wait	1	12E5300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 25 fd fd fd 4b 13 fd 4b 13 fd 4b fd fd fd 4e 52 fd 4b fd fd fd 48 52 fd 4b fd fd fd 4f 47 fd 4b fd fd fd 4a 42 fd 4b 13 fd 4a fd 0d fd 4b fd fd fd 43 5a fd 4b fd fd fd 12 fd 4b fd fd fd 49 52 fd 4b fd 52 69 63 68 fd fd 4b fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 60 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0e 0d 00 64 00	MZ@!L!This program cannot be run in DOS mode.$%KKKNKHKOKJKJKCKKIKRichKPEL`bd	success or wait	20	12E4B0B	WriteFile
C:\Users\user\AppData\Local\Temp\IXP001.TMP\xJuGE71.exe	0	5632	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 16 fd fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 01 00 00 14 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 04 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 03 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL0 @ @	success or wait	7	12E4B0B	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup1	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP001.TMP\"	success or wait	1	12E2243	RegSetValueExA

Analysis Process: zap9953.exe PID: **3324**, Parent PID: **1392**

General

Target ID:	2

Start time:	07:07:03
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\zap9953.exe
Imagebase:	0xde0000
File size:	649728 bytes
MD5 hash:	FCE6A8713A6F6A9B3B40FB5A6F39D51F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 54%, ReversingLabs • Detection: 56%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	DE5458	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\TMP4351$.TMP	read attributes | delete | synchronize | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	DE5949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DE48E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\w77lD51.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	DE48E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe	success or wait	1	DE5300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 25 fd fd fd 4b 13 fd 4b 13 fd 4b fd fd fd 4e 52 fd 4b fd fd fd 48 52 fd 4b fd fd fd 4f 47 fd 4b fd fd fd 4a 42 fd 4b 13 fd 4a fd 0d fd 4b fd fd fd 43 5a fd 4b fd fd fd 12 fd 4b fd fd fd 49 52 fd 4b fd 52 69 63 68 fd fd 4b fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 60 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0e 0d 00 64 00	MZ@!L!This program cannot be run in DOS mode.$%KKKNKHKOKJKJKCKKIKRichKPEL`bd	success or wait	10	DE4B0B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\w77ID51.exe	0	6656	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 07 fd 02 fd 66 fd 51 fd 66 fd 51 fd 66 fd 51 fd 10 01 51 fd 66 fd 51 fd 10 34 51 fd 66 fd 51 fd 10 00 51 fd 66 fd 51 fd 1e 39 51 fd 66 fd 51 fd 66 fd 51 fd 66 fd 51 fd 10 05 51 fd 66 fd 51 fd 10 30 51 fd 66 fd 51 fd 10 37 51 fd 66 fd 51 52 69 63 68 fd 66 fd 51 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 39 36 65 62 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$fQfQfQQfQ4QfQQfQ9QfQfQfQQfQ0QfQ7QffQRichfQPEL96eb	success or wait	10	DE4B0B	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup2	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\"	success or wait	1	DE2243	RegSetValueExA

Analysis Process: zap8476.exe PID: **5416**, Parent PID: **3324**

General

Target ID:	3
Start time:	07:07:04
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\zap8476.exe
Imagebase:	0xa10000
File size:	321024 bytes
MD5 hash:	FB7A56568450CF705F26C6C9FD80CCE2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	A15458	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\TMP4351$.TMP	read attributes | delete | synchronize | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	A15949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A148E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A148E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe	success or wait	1	A15300	DeleteFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe	success or wait	1	A15300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe	0	11264	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 01 02 fd 00 00 00 00 00 00 00 00 fd 00 22 00 0b 01 30 00 00 22 00 00 00 08 00 00 00 00 00 00 fd 40 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL"0"@ `@ @	success or wait	1	A14B0B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe	0	21504	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 07 fd 02 fd 66 fd 51 fd 66 fd 51 fd 66 fd 51 fd 10 01 51 fd 66 fd 51 fd 10 34 51 fd 66 fd 51 fd 10 00 51 fd 66 fd 51 fd 1e 39 51 fd 66 fd 51 fd 66 fd 51 fd 66 fd 51 fd 10 05 51 fd 66 fd 51 fd 10 30 51 fd 66 fd 51 fd 10 37 51 fd 66 fd 51 52 69 63 68 fd 66 fd 51 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 12 fd fd 61 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$fQfQfQQfQ4QfQ Q fQ9QfQfQfQQfQ0QfQ7QfQRichfQPELa	success or wait	8	A14B0B	WriteFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup3	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP003.TMP\"	success or wait	1	A12243	RegSetValueExA

Analysis Process: tz5602.exe PID: **5396**, Parent PID: **5416**

General

Target ID:	4
Start time:	07:07:04
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\tz5602.exe
Imagebase:	0xad0000
File size:	11264 bytes
MD5 hash:	7E93BACBBC33E6652E147E7FE07572A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 88%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\tz5602.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0CB586ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\tz5602.exe.log	0	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0	success or wait	1	7FFC0CB58769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C5BB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0C5BB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0C6912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C5C2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0C6912E7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center	success or wait	1	7FFC0B41E75B	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	success or wait	1	7FFC0B41E75B	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableIOAVProtection	dword	1	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	DisableNotifications	dword	1	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AUOptions	dword	2	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AutoInstallMinorUpdates	dword	0	success or wait	1	7FFC0BAFA911	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers	dword	1	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	UseWUServer	dword	1	success or wait	1	7FFC0BAFA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate	DoNotConnectToWindowsUpdateInternetLocations	dword	1	success or wait	1	7FFC0BAFA911	RegSetValueExW

Analysis Process: rundll32.exe PID: **5868**, Parent PID: **3452**

General

Target ID:	5
Start time:	07:07:12
Start date:	21/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\
Imagebase:	0x7ff632c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Analysis Process: v7930id.exe PID: **5852**, Parent PID: **5416**

General

Target ID:	6
Start time:	07:07:15
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\v7930id.exe
Imagebase:	0x400000
File size:	235520 bytes
MD5 hash:	293C64D08567381D93D7CC071C4F0B3A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000006.00000002.306492758.0000000000400000.00000040.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000006.00000002.306492758.0000000000400000.00000040.00000001.01000000.0000000A.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000006.00000002.306673569.00000000004F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000006.00000002.306673569.00000000004F0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000006.00000002.306894968.00000000006A6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000006.00000003.282735795.0000000000520000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000006.00000003.282735795.0000000000520000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 49%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\v7930id.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\v7930id.exe.log	0	321	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	717E5F3C	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	717E5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	717EC075	RegSetValueExW

Analysis Process: rundll32.exe PID: **2140**, Parent PID: **3452**

General

Target ID:	11
Start time:	07:07:21
Start date:	21/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP001.TMP\
Imagebase:	0x7ff632c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5104**, Parent PID: **3452**

General

Target ID:	17
Start time:	07:07:29
Start date:	21/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\
Imagebase:	0x7ff632c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5044**, Parent PID: **3452**

General	
Target ID:	18
Start time:	07:07:42
Start date:	21/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP003.TMP\
Imagebase:	0x7ff632c30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly