ID: 876163
Sample Name: qu0t4ukLoN.exe
Cookbook: default.jbs
Time: 11:39:25
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

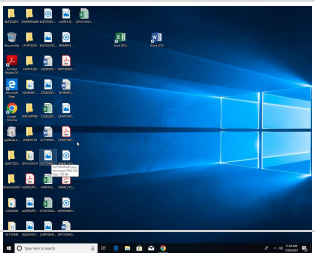
Windows Analysis Report

qu0t4ukLoN.exe

Overview

General Information

Sample Name:	qu0t4ukLoN.exe
Original Sample Name:	1df346c349b9b..
Analysis ID:	876163
MD5:	1df346c349b9b..
SHA1:	13df3b1666b67..
SHA256:	8e96ef86e327d..
Tags:	exe RedLineStealer
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

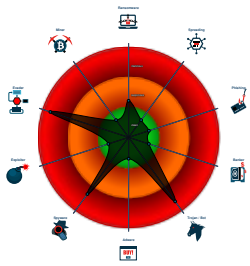
Amadey, RedLine

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for drop…
- Disable Windows Defender real time…
- Connects to many ports of the same…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- qu0t4ukLoN.exe (PID: 4908 cmdline: C:\Users\user\Desktop\qu0t4ukLoN.exe MD5: 1DF346C349B9B71B11825690BE73E635)
  - v7020033.exe (PID: 5988 cmdline: C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe MD5: A9A0FDF699EB764206C59FF3CA3FAC53)
    - v6434086.exe (PID: 2336 cmdline: C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe MD5: 4D67FD4D3D62A45215D1FBDF9CA87397)
      - a4758283.exe (PID: 6988 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe MD5: 1BE37E0816A88025F557178CA7FC03C8)
        - conhost.exe (PID: 6104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - AppLaunch.exe (PID: 6072 cmdline: C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - b7687179.exe (PID: 3320 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe MD5: 927C5B1DEF98D855184A0ED56D8A2787)
- rundll32.exe (PID: 5760 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: 5116 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: 5296 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.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.cyble.com/2023/01/25/the-rise-of-amadey-bot-a-growing-concern-for-internet-security/https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-become	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.avast.com/adobe-acrobat-sign-malware	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "77.91.68.62/wings/game/index.php",
  "Version": "3.83"
}
```


Threatname: RedLine


```
{
  "C2 url": "83.97.73.122:19062",
  "Bot Id": "misa",
  "Authorization Header": "9e79529a6bdb4962f44d12b0d6d62d32"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd00:$pat14: , CommandLine: • 0x140e6:$v2_1: ListOfProcesses • 0x13e9a:$v4_3: base64str • 0x14b69:$v4_4: stringKey • 0x1269c:$v4_5: BytesToStringConverted • 0x113ef:$v4_6: FromBase64 • 0x12bd4:$v4_8: procName
C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.357315003.0000000004D41000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
00000006.00000000.361157707.0000000000E82000.00000002.00000001.01000000.00000008.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000006.00000002.426987259.000000000325F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000002.00000003.358780202.0000000004C12000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: b7687179.exe PID: 3320	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.v7020033.exe.4d85c20.0.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
2.3.v6434086.exe.4c3f81e.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.3.v6434086.exe.4c3f81e.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0xd00:$pat14: , CommandLine: • 0x140e6:$v2_1: ListOfProcesses • 0x13e9a:$v4_3: base64str • 0x14b69:$v4_4: stringKey • 0x1269c:$v4_5: BytesToStringConverted • 0x113ef:$v4_6: FromBase64 • 0x12bd4:$v4_8: procName
1.3.v7020033.exe.4d85c20.0.raw.unpack	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
2.3.v6434086.exe.4c3f81e.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 83.97.73.122

Timestamp:	192.168.2.383.97.73.12249697190622043231 05/26/23-11:40:50.159297
SID:	2043231
Source Port:	49697
Destination Port:	19062
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 83.97.73.122

Timestamp:	192.168.2.383.97.73.12249697190622043233 05/26/23-11:40:32.455619
SID:	2043233
Source Port:	49697
Destination Port:	19062
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 83.97.73.122 - Destination IP: 192.168.2.3

Timestamp:	83.97.73.122192.168.2.319062496972043234 05/26/23-11:40:36.975680
SID:	2043234
Source Port:	19062
Destination Port:	49697
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Sample uses string decryption to hide its real strings
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- Connects to many ports of the same IP (likely port scanning)
- C2 URLs / IPs found in malware configuration

System Summary

- Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Writes to foreign memory regions
- .NET source code references suspicious native API functions

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
- Tries to harvest and steal browser information (history, passwords, etc)

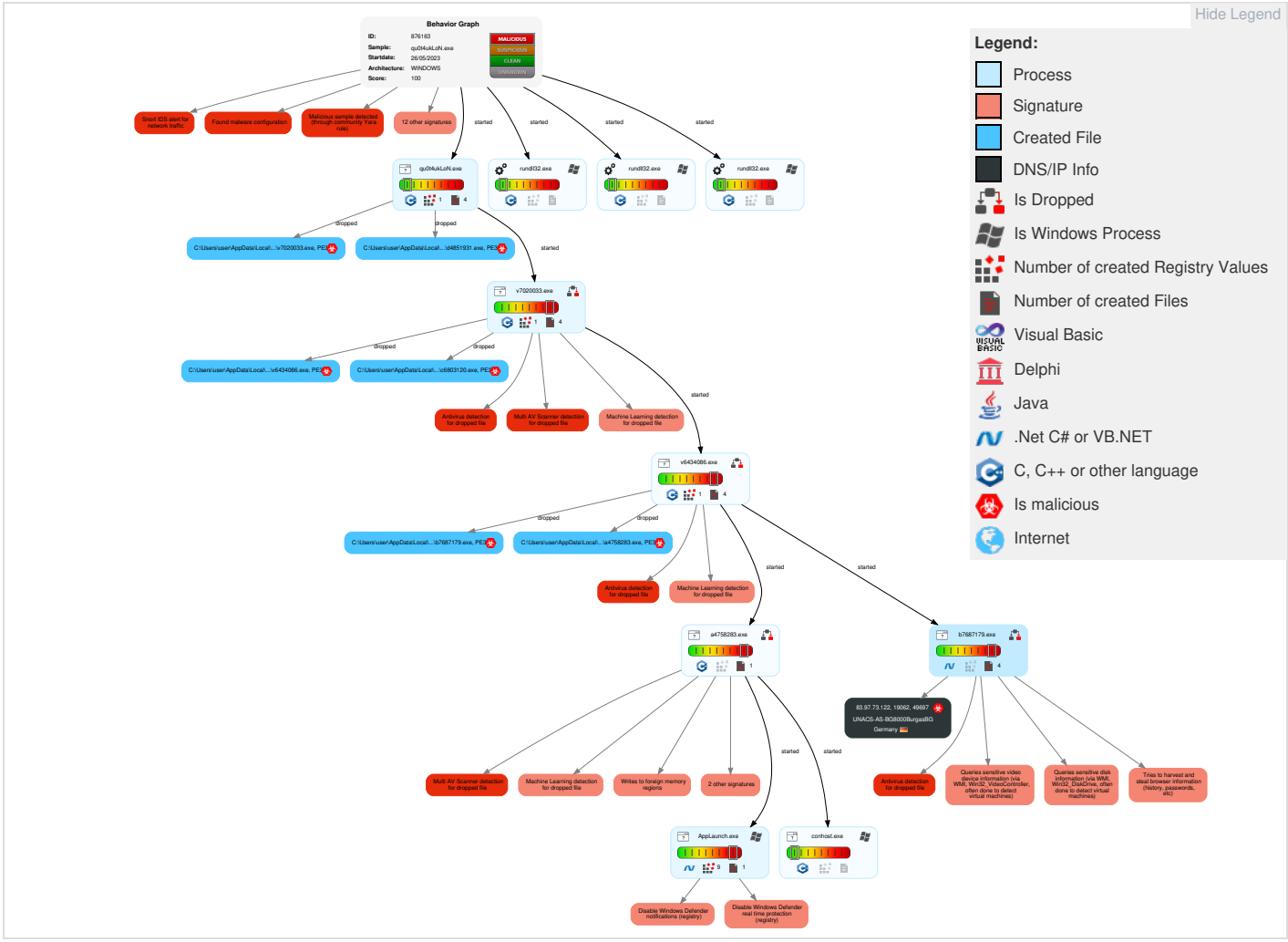
Remote Access Functionality

- 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	2 2 1 Windows Management Instrumentation	Path Interception	2 Bypass User Access Control	2 1 Disable or Modify Tools	1 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	1 3 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	3 1 1 Process Injection	2 1 Obfuscated Files or Information	Security Account Manager	1 3 7 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	1 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)	1 Timestomp	NTDS	3 4 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Bypass User Access Control	LSA Secrets	1 1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	2 3 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	2 3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window 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	1 Access Token Manipulation	Proc Filesystem	Network Service Scanning	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)	3 1 1 Process Injection	/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 Rundll32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

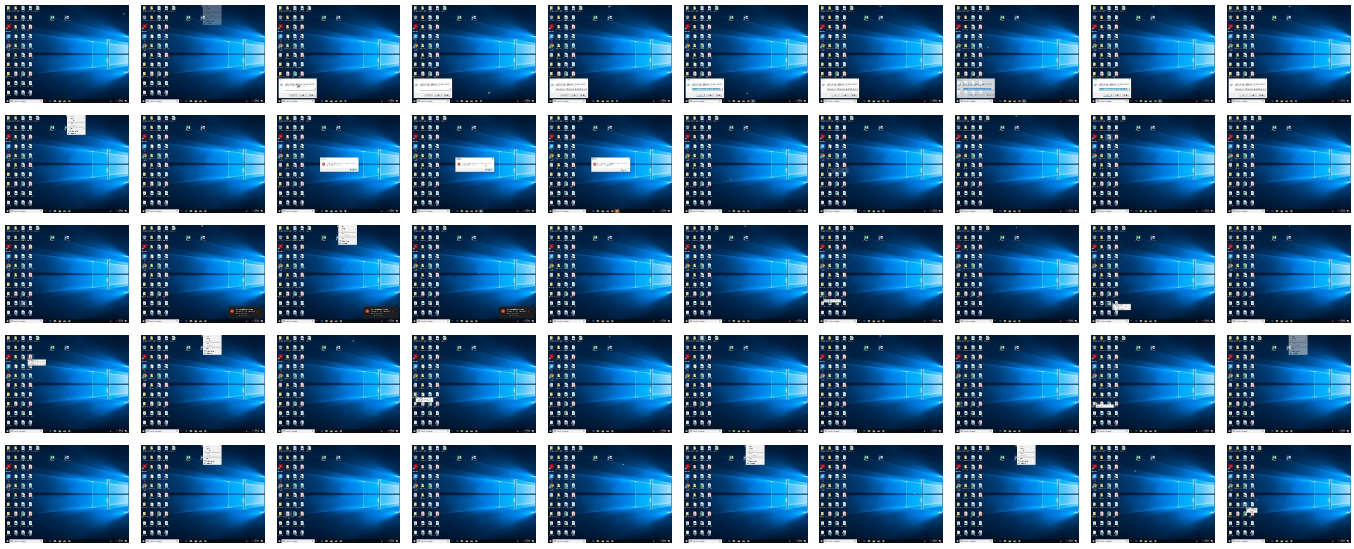
Behavior Graph



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
qu0t4ukLoN.exe	53%	ReversingLabs	ByteCode-MSIL.Trojan.RedLineStealer	
qu0t4ukLoN.exe	53%	Virustotal		Browse
qu0t4ukLoN.exe	100%	Avira	HEUR/AGEN.1307453	
qu0t4ukLoN.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\d4851931.exe	100%	Avira	HEUR/AGEN.1311185	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe	100%	Avira	HEUR/AGEN.1317762	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe	100%	Avira	HEUR/AGEN.1307453	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe	100%	Avira	HEUR/AGEN.1307453	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	100%	Avira	HEUR/AGEN.1307453	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\d4851931.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\d4851931.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.RedLineStealer	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe	50%	ReversingLabs	ByteCode-MSIL.Trojan.RedLineStealer	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe	69%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe	39%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	78%	ReversingLabs	ByteCode-MSIL.Trojan.RedLineStealer	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
83.97.73.122:19062	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id40	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
83.97.73.122:19062	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	b7687179.exe, 00000006.00000002.426987259.000000000325F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	b7687179.exe, 00000006.00000002.426987259.000000000325F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultP	b7687179.exe, 00000006.00000002.426987259.00000000031D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	b7687179.exe, 00000006.00000002.434854527.0000000004375000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.00000000043F3000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.00000000042DA000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.00000000032DF000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.0000000003488000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.00000000042F7000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.00000000044530000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.00000000043D6000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000003.422839734.0000000004482000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.00000000033FB000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.0000000004470000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.000000000336E000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.0000000003515000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.0000000004273000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.0000000004358000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000003.422839734.000000000449F000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.00000000044204000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	b7687179.exe, 00000006.00000002.43485452 7.0000000004204000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id7	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	b7687179.exe, 00000006.00000002.42698725 9.00000000032B3000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	b7687179.exe, 00000006.00000002.42698725 9.00000000032B3000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.00000000031D1000. 00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987 259.000000000325F000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	v6434086.exe, 00000002.00000003.35878020 2.0000000004C12000.00000004.00000020.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000000.361157707.0000000000E82000. 00000002.00000001.01000000.00000008.sdmp, b7687179.exe, 00000006.00000002.426987 259.000000000325F000.00000004.00000800.0 0020000.00000000.sdmp, b7687179.exe.2.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	b7687179.exe, 00000006.00000002.42698725 9.00000000032B3000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.00000000031D1000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	b7687179.exe, 00000006.00000002.43485452 7.0000000004204000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	b7687179.exe, 00000006.00000002.42698725 9.00000000032AB000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.00000000031D1000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high

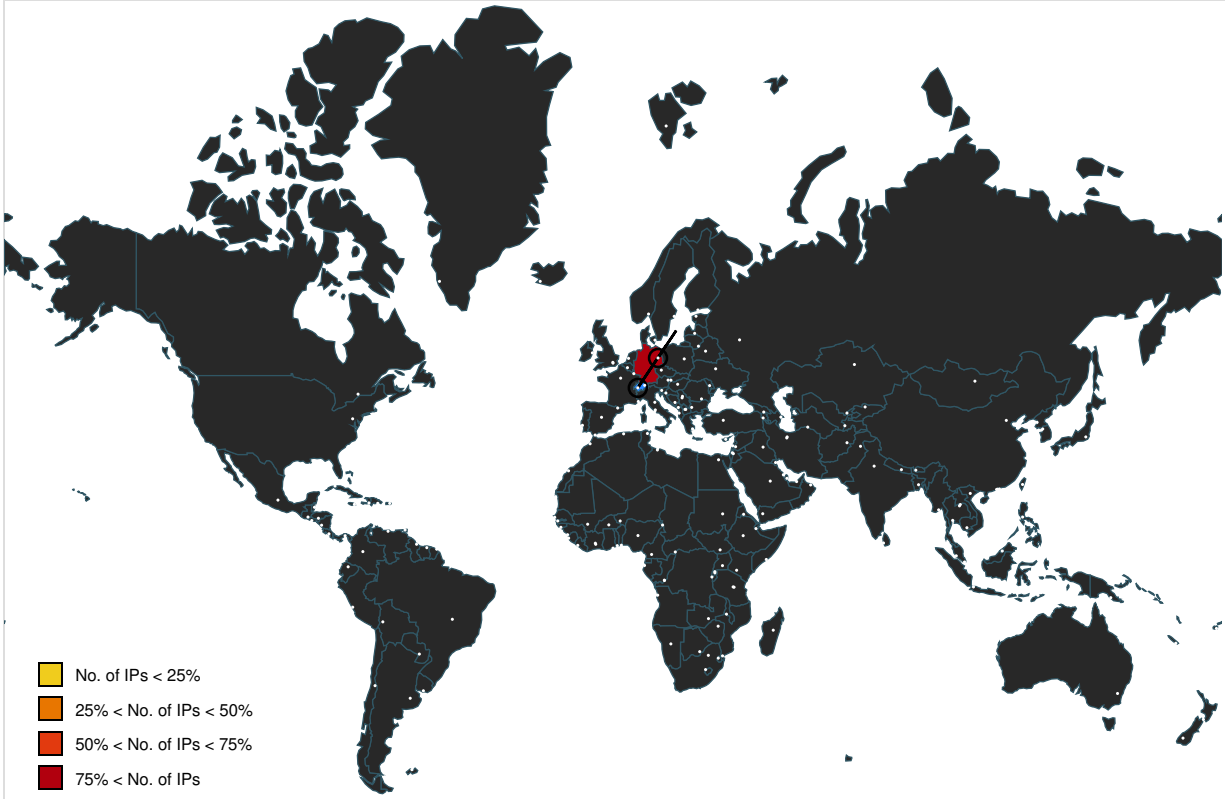
Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id1Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	b7687179.exe, 00000006.00000002.43485452 7.0000000004375000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.434854527.00000000043F3000. 00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854 527.00000000042DA000.00000004.00000800.0 0020000.00000000.sdmp, b7687179.exe, 000 00006.00000002.426987259.00000000032DF00 0.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.0000 000003488000.00000004.00000800.00020000. 00000000.sdmp, b7687179.exe, 00000006.00 000002.434854527.00000000042F7000.000000 04.00000800.00020000.00000000.sdmp, b768 7179.exe, 00000006.00000002.434854527.00 00000004453000.00000004.00000800.0002000 0.00000000.sdmp, b7687179.exe, 00000006. 00000002.434854527.00000000043D6000.0000 0004.00000800.00020000.00000000.sdmp, b7 687179.exe, 00000006.00000003.422839734. 0000000004482000.00000004.00000800.00020 000.00000000.sdmp, b7687179.exe, 0000000 6.00000002.426987259.00000000033FB000.00 000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.43485452 7.0000000004470000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000336E000. 00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987 259.0000000003515000.00000004.00000800.0 0020000.00000000.sdmp, b7687179.exe, 000 00006.00000002.434854527.000000000427300 0.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.0000 000004358000.00000004.00000800.00020000. 00000000.sdmp, b7687179.exe, 00000006.00 000003.422839734.000000000449F000.000000 04.00000800.00020000.00000000.sdmp, b768 7179.exe, 00000006.00000002.434854527.00 00000004204000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id10	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000325F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id40	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	b7687179.exe, 00000006.00000002.43485452 7.0000000004375000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.434854527.00000000043F3000. 00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854 527.00000000042DA000.00000004.00000800.0 0020000.00000000.sdmp, b7687179.exe, 000 00006.00000002.426987259.00000000032DF00 0.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.0000 000003488000.00000004.00000800.00020000. 00000000.sdmp, b7687179.exe, 00000006.00 000002.434854527.00000000042F7000.000000 04.00000800.00020000.00000000.sdmp, b768 7179.exe, 00000006.00000002.434854527.00 0000004453000.00000004.00000800.0002000 0.00000000.sdmp, b7687179.exe, 00000006. 00000002.434854527.00000000043D6000.0000 0004.00000800.00020000.00000000.sdmp, b7 687179.exe, 00000006.00000003.422839734. 0000000004482000.00000004.00000800.00020 000.00000000.sdmp, b7687179.exe, 0000000 6.00000002.426987259.00000000033FB000.00 000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.43485452 7.0000000004470000.00000004.00000800.000 20000.00000000.sdmp, b7687179.exe, 00000 006.00000002.426987259.000000000336E000. 00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987 259.0000000003515000.00000004.00000800.0 0020000.00000000.sdmp, b7687179.exe, 000 00006.00000002.434854527.000000000427300 0.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.434854527.0000 000004358000.00000004.00000800.00020000. 00000000.sdmp, b7687179.exe, 00000006.00 000003.422839734.000000000449F000.000000 04.00000800.00020000.00000000.sdmp, b768 7179.exe, 00000006.00000002.434854527.00 0000004204000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	b7687179.exe, 00000006.00000002.42698725 9.00000000031D1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	b7687179.exe, 00000006.00000002.42698725 9.000000000325F000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id17Response	b7687179.exe, 00000006.00000002.426987259.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, b7687179.exe, 00000006.00000002.426987259.000000000325F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	b7687179.exe, 00000006.00000002.426987259.000000000325F000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
83.97.73.122	unknown	Germany		25206	UNACS-AS-BG8000BurgasBG	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876163
Start date and time:	2023-05-26 11:39:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
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:	14
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:	qu0t4ukLoN.exe
Original Sample Name:	1df346c349b9b71b11825690be73e635.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@15/8@0/1
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 96.9%) • Quality average: 82.6% • Quality standard deviation: 24.1%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- Execution Graph export aborted for target b7687179.exe, PID 3320 because it is empty
- 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 NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:40:47	API Interceptor	11x Sleep call for process: b7687179.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.3467126928258955
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2LDY3U21v:Q3La/KDLI4MWuPk21v
MD5:	DD8B7A943A5D834CEEAB90A6BBBF4781
SHA1:	2BED8D47DF1C0FF76B40811E5F11298BD2D06389
SHA-256:	E1D0A304B16BE51AE361E392A678D887AB0B76630B42A12D252EDC0484F0333B
SHA-512:	24167174EA259CAF57F65B9B9B9C113DD944FC957DB444C2F66BC656EC2E6565EFE4B4354660A5BE85CE4847434B3BDD4F7E05A9E9D61F4CC99FF0284DAA1C87
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_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\b7687179.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHK1HG1qX:iqXeqm00YqhQnouOqLqdqNq2qzcGtIxk
MD5:	EBF4AEAE98F14F4480152E9EDBB24123
SHA1:	21F9D2A708D7709FECD4A837536B588D953FA6FC
SHA-256:	6278F6B29B841FD578D1F01D6BA7CD9FD7A3D977BE1D503A2E19C9B2017EA1B7
SHA-512:	F7A1EEA0AB96145F8AA49D43CC8C8E171137FA89E4780DCF7FC236488747518C42BCABED71CB8CB6DAF35DDF701CB1BC01A122A4E8E553E028DAA0DC0287FDC9
Malicious:	false
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_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\IXP000.TMP\d4851931.exe

Process:	C:\Users\user\Desktop\qu0t4ukLoN.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	324094
Entropy (8bit):	7.54372131384144
Encrypted:	false
SSDEEP:	6144:xcDje7OxoovhLLDLjC4d8QvV+hdaLB4rOlEnQ2m3bR:iDyOVvhLLH24dBvmdaLBzEnQ2
MD5:	AAE88589C2939D21D935B6DE0E73870B
SHA1:	AA7CB7CFA1BCB86B52E105EA7D8D5D77A4013325
SHA-256:	F6A7AE755C44744C961C5C054EE17E7E1209E9E97FBDA412BC406FBE61E2A90F
SHA-512:	70AC1FC2670E5C1098E7994FD95751302619A800BF15C42CF065AC8E86E7B799CF6044D4C7DB96BFA9B0605794F94B15EE34BC3E220828503BAE33F852537AA5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c..dc..c..uc..c..rcW..c.b.c..c...c..c..c...c..uc..c..ec..c..` c..cRich..c.....PE..L....vpd.....Bl.....@.....S..<.....(.....S.....=..@.....X .....text....e.....f..... ..`.OuoYr.....j..... ..`.rdata...K.....L.....@..@.data...h{...`...\..:.....@....rsrc...(.....@..@... .....

C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe

Process:	C:\Users\user\Desktop\qu0t4ukLoN.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	457216
Entropy (8bit):	7.786373811719987
Encrypted:	false
SSDEEP:	6144:Kpy+bnr+5p0yN90QEmoGpHE2TQYNCZje6TsbzxxTgINo2hUVE2MyrOGdKbert:TMrRy900oGpxTQaCjixxTy2bXat
MD5:	A9A0FDF699EB764206C59FF3CA3FAC53
SHA1:	2578C481B0D67C710FC64163712021043D49CAA8
SHA-256:	B41DD10009E2BD916D9C7AFAB7D3D9E673D4E111278EFFDD05D44F68E9F84FE4
SHA-512:	2D3784C01F16E11BA8D2DAC7D91BD6FCB3B1D5095578D4C6C82A788CFDAF278D18E31B1FF5FB284AA593AD96F39CA8789BF182FE030D6318CA080072CE3191E8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
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.....@..... .....xs.....@.....T.....@.....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....t...|.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	210873
Entropy (8bit):	6.33924537885446
Encrypted:	false
SSDEEP:	3072:meTRJ0kHbnpN23kQKp5XzutZXKGrpeN84LuZAIybiy3xEfbi:FTR2AnpN2wDurXBeBuZAIMEj
MD5:	3ED5D8F4F6620DE95B8EF02F28C9C5E9
SHA1:	EEFDA1DF3A3297B00D08475B93084495ECB7FD0A
SHA-256:	3E2696E2C4CCC222063F06F6031DC8DACF54A3B0D923650135AF17C74789738A
SHA-512:	C4CB8AFE75866A9D7346BD9241D9119B8478259A037A39663EC0A507E5ABE2F95B10393E412BA2DC15A93316F3DE0A4E043EBC1A53E298785DB431FC70B91D4C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 69%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]..M.o...o...o..B....o..B....o..B....o.....o.....o.....5o..B....o...o...o.....o....m..o.....o..Rich.o.....PE..L...opod.....v.....V.....@.....@.....d....@.....P... ..`...p.....t.....@.....text....t.....v..... ..`.rdata..t\|.....~...z.....@..@.data...h$.....@....rsrc.....@.....@..@.reloc... ...P..."....@..B.....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	281600
Entropy (8bit):	7.572515848405127
Encrypted:	false
SSDEEP:	6144:KTy+bnr+0p0yN90QEsZjeETsbzxgggINo2wUME2aR:tMr0y90elixggy2P
MD5:	4D67FD4D3D62A45215D1FBDF9CA87397
SHA1:	FB686838CEC8323CE6EC87A133C48E9723C3DED5
SHA-256:	0C36FA81B63A4C7D12FA7A0CF055BACCA0C423E7DFEDAD6EB55281C914CA0003
SHA-512:	D3718984BC81E18624EE801AA01F5B482DDBB2551C3AB25772F88947BAADB637733F633F77D376EF46126C4FDE6629E9DE85D898425AF655E817C0466CB9457
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

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 h..K.....PE..L....`.b.....d.....`j.....@.....C....@..... .....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....B.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	186366
Entropy (8bit):	6.898951882290762
Encrypted:	false
SSDEEP:	3072:lAZJrtymkLKh/gH2TPDXD1qk+yxXeOx5lTx:l+yvKdFPDXDM2D
MD5:	1BE37E0816A88025F557178CA7FC03C8
SHA1:	BE1947797AC7B4CDED7F3524B5AD1CD6A4B28CFC
SHA-256:	F8DA12B0DDF6695F8669679E0148756B3676E55D2F1C9121E5A04DDAF78C6E6B
SHA-512:	E3D189AE5918D6DC9128B8564FD90DE5FCDC2DD9BFDE5C3BFB2130BBB739CB348DD2A9B8B08D84D322C41A85F6C3409EA3C78173CA3894606B71DAF4584D8DFB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c..dc..c..uc..c..rcW..c.b.c..c...c..c..c...c..uc..c..ec..c..` c..cRich..c.....PE..L....vpd.....Bl.....@.....S..<.....(.....S.....=..@.....X .....text....e.....f..... ..`.miJql.....j..... ..`.rdata...K.....L.....@..@.data...hc...`...D...8.....@....rsrc...(.....|.....@..@... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	148489
Entropy (8bit):	5.412914556371622
Encrypted:	false
SSDEEP:	3072:LV+m5chQmRSZsBxioW/JruNFmRsZhCZR8e8ha:LjEx6U3ZhC7
MD5:	927C5B1DEF98D855184A0ED56D8A2787
SHA1:	EEB57B0120D4C1F6539CDC372A5E71A8947FDE3C
SHA-256:	1A0C4908C739CF9C405A050A6FE29214525F46350E7BA49BD26F9BD7E60F6BC9
SHA-512:	93957AD10BE2B54D2E5AB9E40B3C1A7767C9295A74E854A98FB9EDBD42D7F32C2F463913A0A7832C73697A3264F966A7E45713CBFEA8326A306DFED80FF9A1CB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 78%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!1.....0..... .....@.. ....@.....K.....N..... ....H.....text..... ....`.rsrc...N.....@..@.reloc..... .....B.....@..B.....H.....X...H.....u.....a.u.t.o.f.i.l.l.P.r.o.f.i.l.e.s.T.o.t.a.l. .o.f. .R.A.M.V.P.E.n.t.i.t.y.1.2.N...A.p.p.D.a.t.a.\.L.o.c.a.l.\.....[.^.\.u.0.0.2.0.-.\.u.0.0.7.F.].U.N.K.N.O.W.N...L.o.c.a.l. .S.t.a.t.e...P.r.o.c.e.s.s.l.d.....1.*...1.l.1.d.1.b.....P.r.o.f.i.l.e._.%.a.p.p.d.a.t.a.%.\.....l.o.g.i.n.s.....{.0.}.\.F.i.l.e.Z.i.l.l.a.\.r.e.c.e.n.t.s.e.r.v.e.r.s...x.m.l...%.a.p.p.d.a.t.a.%.\.d.i.s.c.o.r.d.\.L.o.c.a.l. .S.t.o.r.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.902876514651296
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:	qu0t4ukLoN.exe
File size:	782336
MD5:	1df346c349b9b71b11825690be73e635
SHA1:	13df3b1666b674f48b1fc2a836fee8ce99381fb5
SHA256:	8e96ef86e327dd3bbc1dab16ce1e57e8f380d9b2df919158f1b6786cfd6f717e
SHA512:	96ffdf2aa68e54bbbfa32659d5683851adba4c50f19ab348233af6a5c284cbbb45b19344cc3668990e51ca66ddfb7c66cf1186d01a793380187a37553967fc8f
SSDEEP:	12288:vMrGy90d/w92r1bjyeDmpa2lixNTy2luuomfds+nnII4d22mdQLBNEFz:VyqFvrNTy2dm1zn94Q2mdUS
TLSH:	56F42353A3D82133D8F81F7088FA028B1B397E616A78072B3745A99D1CF3D946576B27
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:	3b6120282c4c5a1f

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 00007FEAA9141CD5h
jmp 00007FEAA91415E5h
push 00000058h
push 004072B8h
call 00007FEAA9141D77h
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]
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 00007FEAA91415FAh

Instruction
cmp eax, esi
jne 00007FEAA91415E9h
xor esi, esi
inc esi
mov edi, esi
jmp 00007FEAA91415F2h
push 000003E8h
call dword ptr [0040A188h]
jmp 00007FEAA91415B9h
xor esi, esi
inc esi
cmp dword ptr [004088B0h], esi
jne 00007FEAA91415ECh
push 0000001Fh
call 00007FEAA9141B0Bh
pop ecx
jmp 00007FEAA914161Ch
cmp dword ptr [004088B0h], ebx
jne 00007FEAA914160Eh
mov dword ptr [004088B0h], esi
push 004010C4h
push 004010B8h
call 00007FEAA9141736h
pop ecx
pop ecx
test eax, eax
je 00007FEAA91415F9h
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, 000000FFh
jmp 00007FEAA9141719h
mov dword ptr [004081E4h], esi
cmp dword ptr [004088B0h], esi
jne 00007FEAA91415FDh
push 004010B4h
push 004010ACh
call 00007FEAA9141CC5h
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	0xb68ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc3000	0x888	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1410	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
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	0xb7000	0xb6a00	False	0.95906191178987	data	7.930785235213812	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc3000	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
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	0x9b354	Microsoft Cabinet archive data, many, 635732 bytes, 2 files, at 0x2c +A "v7020033.exe" +A "d4851931.exe", ID 1672, number 1, 24 datablocks, 0x1503 compression	English	United States
RT_RCDATA	0xc1bc4	0x4	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0xc1bc8	0x24	data	English	United States
RT_RCDATA	0xc1bec	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xc1bf4	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xc1bfc	0x4	data	English	United States
RT_RCDATA	0xc1c00	0xd	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xc1c10	0x4	data	English	United States
RT_RCDATA	0xc1c14	0xd	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xc1c24	0x4	data	English	United States
RT_RCDATA	0xc1c28	0x9	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xc1c34	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xc1c3c	0x7	ASCII text, with no line terminators	English	United States
RT_GROUP_ICON	0xc1c44	0xbc	data	English	United States
RT_VERSION	0xc1d00	0x408	data	English	United States
RT_MANIFEST	0xc2108	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
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.383.97.73.1224 9697190622043231 05/26/23-11:40:50.159297	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49697	19062	192.168.2.3	83.97.73.122

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.383.97.73.1224 9697190622043233 05/26/23-11:40:32.455619	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49697	19062	192.168.2.3	83.97.73.122
83.97.73.122192.168.2.31 9062496972043234 05/26/23-11:40:36.975680	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	19062	49697	83.97.73.122	192.168.2.3

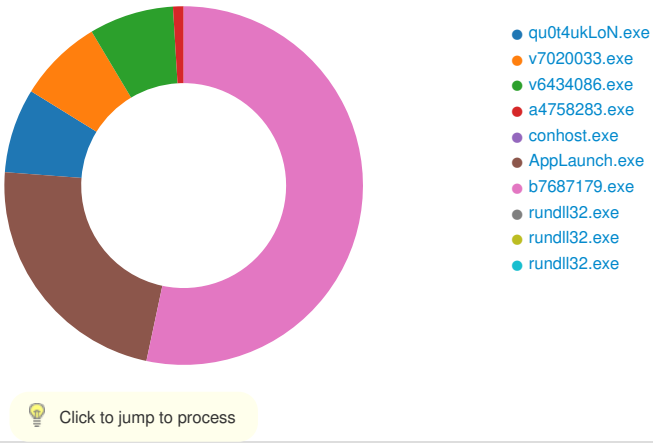
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:40:31.586014032 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:31.643364906 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:31.645324945 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:32.455619097 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:32.512979031 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:32.562242985 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:36.918205976 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:36.975680113 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:37.062699080 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:43.996256113 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:44.056159019 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:44.056250095 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:44.056337118 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:44.056369066 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:44.110127926 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:45.734921932 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:45.838387966 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:45.844085932 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:45.891550064 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:45.927423954 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:45.985167980 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.022172928 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.079714060 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.082263947 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.139978886 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.188452959 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.343362093 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.400934935 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.432321072 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.489912987 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.511499882 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.569073915 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.610366106 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.665498018 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.723166943 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.731164932 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.788501978 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.790275097 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.847825050 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.880130053 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:46.937726021 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:46.985423088 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:47.030561924 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:47.087986946 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:47.088042021 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:47.141644955 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:47.356575966 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:47.413834095 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:47.414064884 CEST	19062	49697	83.97.73.122	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:40:47.414083004 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:47.414403915 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:47.469794989 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:47.487380028 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:47.545372009 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:47.594831944 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:50.101281881 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:50.158529997 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:50.158723116 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:50.159296989 CEST	49697	19062	192.168.2.3	83.97.73.122
May 26, 2023 11:40:50.216737986 CEST	19062	49697	83.97.73.122	192.168.2.3
May 26, 2023 11:40:50.262445927 CEST	49697	19062	192.168.2.3	83.97.73.122

Statistics

Behavior



System Behavior

Analysis Process: qu0t4ukLoN.exe PID: **4908**, Parent PID: **3452**

General

Target ID:	0
Start time:	11:40:16
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\qu0t4ukLoN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\qu0t4ukLoN.exe
Imagebase:	0xa90000
File size:	782336 bytes
MD5 hash:	1DF346C349B9B71B11825690BE73E635
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	A92243	RegSetValueExA

Analysis Process: v7020033.exe PID: **5988**, Parent PID: **4908**

General

Target ID:	1
Start time:	11:40:17
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\v7020033.exe
Imagebase:	0x210000
File size:	457216 bytes
MD5 hash:	A9A0FDF699EB764206C59FF3CA3FAC53
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: 00000001.00000003.357315003.0000000004D41000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 50%, ReversingLabs
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	215458	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	215949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2148E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2148E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe	success or wait	1	215300	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\v6434086.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.$%KKKNKHKOKJKJKCKKIKRichKPEL`bd	success or wait	9	214B0B	WriteFile
C:\Users\user\AppData\Local\Temp\IXP001.TMP\c6803120.exe	0	13312	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5d 0e fd 4d 19 6f fd 1e 19 6f fd 1e 19 6f fd 1e 42 07 fd 1f 13 6f fd 1e 42 07 fd 1f fd 6f fd 1e 42 07 fd 1f 0b 6f fd 1e fd 02 fd 1f 0b 6f fd 1e fd 02 fd 1f 0a 6f fd 1e fd 02 fd 1f 35 6f fd 1e 42 07 fd 1f 16 6f fd 1e 19 6f fd 1e fd 6f fd 1e fd 01 fd 1f 18 6f fd 1e fd 01 6d 1e 18 6f fd 1e fd 01 fd 1f 18 6f fd 1e 52 69 63 68 19 6f fd 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$]MoooBoBoBooo5oBoooomooRicho	success or wait	8	214B0B	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	212243	RegSetValueExA

Analysis Process: v6434086.exe

PID: **2336**, Parent PID: **5988**

General

Target ID:	2
Start time:	11:40:17

Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\v6434086.exe
Imagebase:	0xbc0000
File size:	281600 bytes
MD5 hash:	4D67FD4D3D62A45215D1FBDF9CA87397
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: 00000002.00000003.358780202.0000000004C12000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
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	BC5458	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	BC5949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BC48E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	BC48E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	success or wait	1	BC5300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.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 5f 30 e4 fd 63 e4 fd 63 e4 fd 63 fd fd 64 63 a4 fd 63 fd fd 75 63 fd fd 63 fd fd 72 63 57 fd fd 63 fd 62 fd 63 64 fd 63 10 fd fd 63 24 fd 63 e4 fd 63 fd fd fd 63 fd fd 75 63 a4 fd 63 fd fd 65 63 a4 fd 63 fd fd 60 63 a4 fd 63 52 69 63 68 e4 fd 63 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 76 70 64 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$0cccdccuccrcWcbccccccuccecc`ccRichcPELvpd	success or wait	6	BC4B0B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe	0	10242	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 21 31 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 01 00 00 fd 00 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 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 02 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!10 @ @	success or wait	6	BC4B0B	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_cleanup2	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\"	success or wait	1	BC2243	RegSetValueExA

Analysis Process: a4758283.exe PID: **6988**, Parent PID: **2336**

General

Target ID:	3
Start time:	11:40:18
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\a4758283.exe
Imagebase:	0x400000
File size:	186366 bytes
MD5 hash:	1BE37E0816A88025F557178CA7FC03C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	1			invalid handle	1	40E87E	WriteFile

Analysis Process: conhost.exe PID: **6104**, Parent PID: **6988**

General	
Target ID:	4
Start time:	11:40:18
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AppLaunch.exe PID: **6072**, Parent PID: **6988**

General	
Target ID:	5
Start time:	11:40:19
Start date:	26/05/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe
Imagebase:	0xe0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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_32\UsageLogs\AppLaunch.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.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 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 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_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0	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\applaunch.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	72975705	unknown
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\applaunch.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	7297CA54	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
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	717E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center	success or wait	1	717E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	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
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableIOAVProtection	dword	1	success or wait	1	717EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	717EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	DisableNotifications	dword	1	success or wait	1	717EC075	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AUOptions	dword	2	success or wait	1	717EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AutoInstallMinorUpdates	dword	0	success or wait	1	717EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers	dword	1	success or wait	1	717EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	UseWUServer	dword	1	success or wait	1	717EC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate	DoNotConnectToWindowsUpdateInternetLocations	dword	1	success or wait	1	717EC075	RegSetValueExW

Analysis Process: b7687179.exe PID: **3320**, Parent PID: **2336**

General

Target ID:	6
Start time:	11:40:19
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe
Imagebase:	0xe80000
File size:	148489 bytes
MD5 hash:	927C5B1DEF98D855184A0ED56D8A2787
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: 00000006.00000000.361157707.0000000000E82000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000006.00000002.426987259.000000000325F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Users\user\AppData\Local\Temp\IXP002.TMP\b7687179.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 78%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Local\SystemCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\b7687179.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\b7687179.exe.log	0	2843	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 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	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\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
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	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	5	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	17	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile

Analysis Process: rundll32.exe PID: **5760**, Parent PID: **3452**

General

Target ID:	7
Start time:	11:40:26
Start date:	26/05/2023
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:	0x7ff658210000
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: **5116**, Parent PID: **3452**

General

Target ID:	8
Start time:	11:40:35
Start date:	26/05/2023
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:	0x7ff658210000
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: **5296**, Parent PID: **3452**

General

Target ID:	9
Start time:	11:40:43
Start date:	26/05/2023
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:	0x7ff658210000
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

Disassembly

No disassembly