ID: 829685
Sample Name: SzznpUhljo.exe
Cookbook: default.jbs
Time: 21:05:04
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

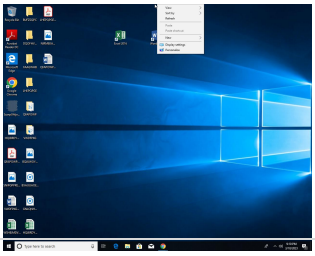
Windows Analysis Report

SzznpUhIjo.exe

Overview

General Information

Sample Name:	SzznpUhIjo.exe
Original Sample Name:	f62fe8447c5e9…
Analysis ID:	829685
MD5:	f62fe8447c5e9…
SHA1:	847f52f9fff9b08..
SHA256:	d7f0a89495629..
Tags:	exe RedLineStealer
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

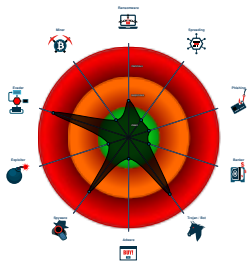
Amadey, RedLine

Score:	93
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Disable Windows Defender real time…
- Machine Learning detection for sam…
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- SzznpUhIjo.exe (PID: 6092 cmdline: C:\Users\user\Desktop\SzznpUhIjo.exe MD5: F62FE8447C5E9B9EA5AC424543AD20B3)
  - kino5628.exe (PID: 6084 cmdline: C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe MD5: 51B7FE413501DC9DD84CF1FCBB4C4BA2)
    - kino6423.exe (PID: 6028 cmdline: C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe MD5: DB27DCB2B593E449358CEC94D3D257DA)
      - kino4801.exe (PID: 6116 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe MD5: 211103CF935C81941C9A7C527A99891E)
        - bus7600.exe (PID: 4084 cmdline: C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe MD5: 7E93BACBBC33E6652E147E7FE07572A0)
        - con1165.exe (PID: 5392 cmdline: C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe MD5: 3930494C030BFEF77C7C0624C1F6BAEB)
- rundll32.exe (PID: 680 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: 2432 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: 1504 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\ MD5: 73C519F050C20580F8A62C849D49215A)
- rundll32.exe (PID: 2460 cmdline: C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP001.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/41450/https://blog.minerva-labs.com/underminer-exploit-kit-the-more-you-check-the-more-evasive-you-becomehttps://blog.talosintelligence.com/2021/08/raccoon-and-amadey-install-servhelper.htmlhttps://blogs.blackberry.com/en/2020/01/threat-spotlight-amadey-bothttps://blogs.blackberry.com/en/2022/05/dot-net-stubs-sowing-the-seeds-of-discord	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.amadey

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

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "31.41.244.200/games/category/index.php",
  "Version": "3.68"
}
```


Threatname: RedLine


```
{
  "C2 url": "193.233.20.30:4125",
  "Bot Id": "relon",
  "Authorization Header": "17da69809725577b595e217ba006b869"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a434:$pat14: , CommandLine: • 0x134a7:$v2_1: ListOfProcesses • 0x13286:$v4_3: base64str • 0x13dff:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12811:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge280443.exe	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.316570894.0000000002DA0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000009.00000002.316570894.0000000002DA0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000009.00000003.291817431.0000000004510000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000003.291817431.0000000004510000.00000004.00001000.00020000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1d0b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x700:$s3: 83 EC 38 53 B0 C4 88 44 24 2B 88 44 24 2F B0 3F 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x1ed8a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1e9d0:$s5: delete[] • 0x1de88:$s6: constructor or from DllMain.
00000009.00000002.316168321.0000000000400000.00000040.00000001.01000000.0000000A.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.con1165.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
9.2.con1165.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
9.2.con1165.exe.400000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1e4b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x1300:$s3: 83 EC 38 53 B0 C4 88 44 24 2B 88 44 24 2F B0 3F 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x2018a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1fdd0:$s5: delete[] • 0x1f288:$s6: constructor or from DllMain.
9.2.con1165.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1d0b0:$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 • 0x80:$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E • 0x700:$s3: 83 EC 38 53 B0 C4 88 44 24 2B 88 44 24 2F B0 3F 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x1ed8a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1e9d0:$s5: delete[] • 0x1de88:$s6: constructor or from DllMain.
9.2.con1165.exe.2da0e67.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 9 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance

Detected unpacking (overwrites its own PE header)

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Lowering of HIPS / PFW / Operating System Security Settings

Disable Windows Defender real time protection (registry)

Disable Windows Defender notifications (registry)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Yara detected Amadeys stealer DLL

Remote Access Functionality

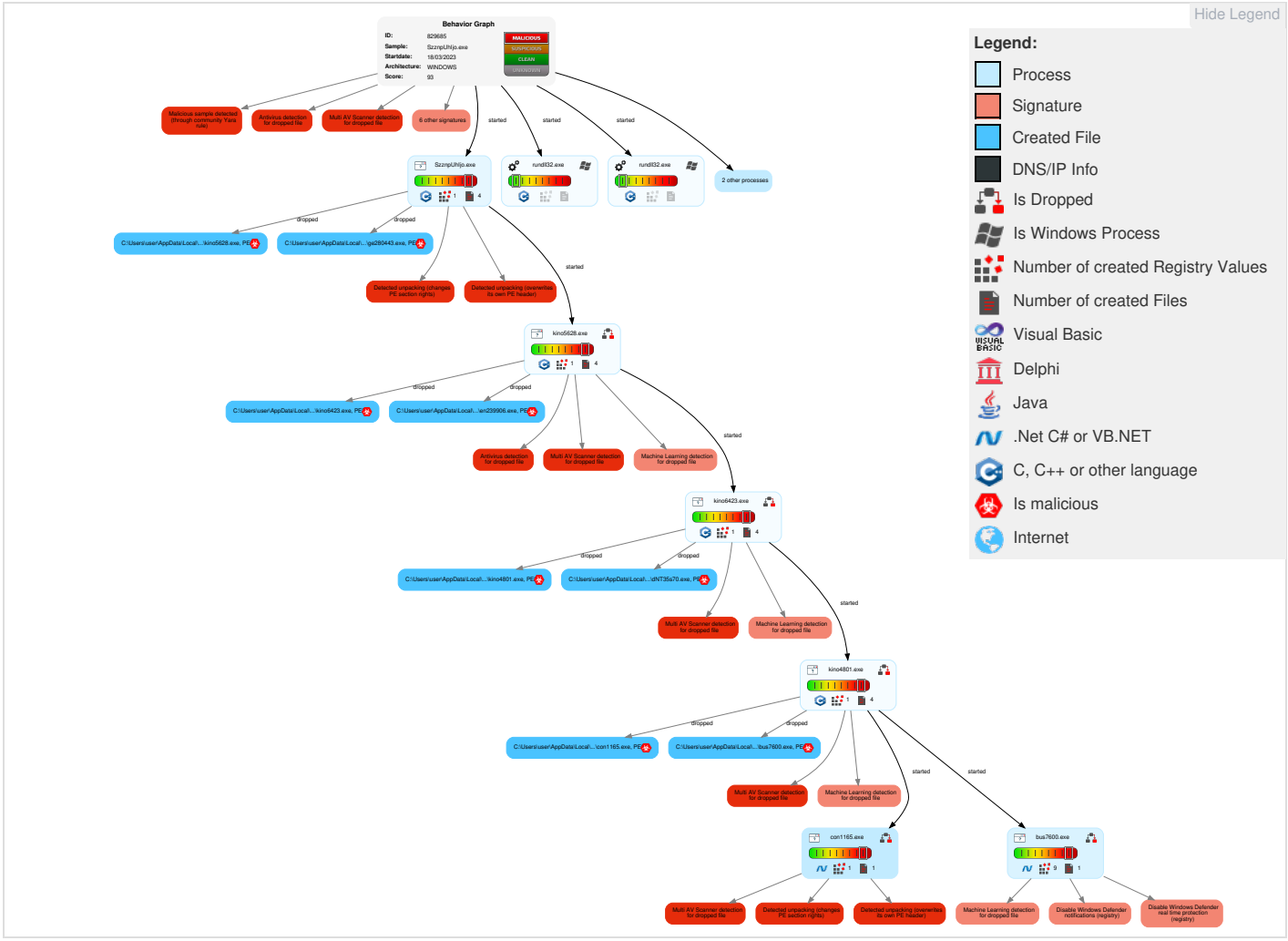
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 Windows Service	2 Bypass User Access Control	2 1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Service Execution	Logon Script (Windows)	1 Windows Service	3 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Process Injection	2 2 Software Packing	NTDS	2 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 3 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Bypass User Access Control	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Process Injection	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SzznpUhljo.exe	44%	ReversingLabs	Win32.Trojan.Pwsx	
SzznpUhljo.exe	49%	Virustotal		Browse
SzznpUhljo.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge280443.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dNT35s70.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge280443.exe	63%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge280443.exe	80%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe	68%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe	65%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	88%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	80%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe	64%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dNT35s70.exe	44%	ReversingLabs	Win32.Trojan.CrypterX	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe	59%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe	88%	ReversingLabs	ByteCode-MSIL.Trojan.Casdet	
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe	67%	ReversingLabs	Win32.Trojan.Babar	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.kino5628.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
0.2.SzznpUhIjo.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
1.0.kino5628.exe.8e0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
31.41.244.200/games/category/index.php	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
193.233.20.30:4125	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
31.41.244.200/games/category/index.php	true	• URL Reputation: safe	low
193.233.20.30:4125	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	kino5628.exe, 00000001.00000003.25667581 9.00000000046C5000.00000004.00000020.000 20000.00000000.sdmp, en239906.exe.1.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829685
Start date and time:	2023-03-18 21:05:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SzznpUhIjo.exe
Original Sample Name:	f62fe8447c5e9b9ea5ac424543ad20b3.exe
Detection:	MAL
Classification:	mal93.troj.spyw.evad.winEXE@15/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 54.2% (good quality ratio 52%) • Quality average: 85.2% • Quality standard deviation: 23.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\bus7600.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZilv:Q3La/KDLI4MWuPTxAlv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\con1165.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.355221377978991
Encrypted:	false
SSDEEP:	6:Q3La/xwchM3RJoDLIP12MUAvvR+uCqDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21v
MD5:	03C5BA5FCE7124B503EA65EF522177C3
SHA1:	F76B1F538D5EA66664355901E927B2F870ACCDD8
SHA-256:	8128CE419BBE0419F1A0BDE97C3A14E3377C0184DC1D7AF61AA01AAB756B625B
SHA-512:	151A974DDABA852144EC4BC18C548227A32E5261736F186A3920F2497434AEE9DBB0E0AB77E0E52A84A9FBC4529A158882B7549763400DDC2082D384B1135141
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge280443.exe

Process:	C:\Users\user\Desktop\SzznpUhIjo.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	231424
Entropy (8bit):	6.351317966279805
Encrypted:	false

SSDEEP:	6144:4rzyIG8IcCnD5A2QdY8rWpau1CYUqfhYdMBg:KmlLnD5qdY8Fu1CYUehrBg
MD5:	8627EBE3777CC777ED2A14B907162224
SHA1:	06EEED93EB3094F9D0B13AC4A6936F7088FBBDAA
SHA-256:	319B22945BEEB7424FE6DB1E9953AD5F2DC12CBBA2FE24E599C3DEDA678893BB
SHA-512:	9DE429300C95D52452CAEB80C9D44FF72714F017319E416649C2100F882C394F5AB9F3876CC68D338F4B5A3CD58337DEFFF9405BE64C87D078EDD0D86259C84
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge280443.exe, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 63% • Antivirus: Virustotal, Detection: 80%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]..M.o...o...o..B....o..B....o..B....o.....o.....o.....5o..B....o...o...o.... ...o....m..o.....o..Rich.o.....PE..L...gv.d.....V.....@.....@.....M..d.....'...#..p.....$ .....#..@.....text...}..... ..`.rdata..p.....@..@.data...H'...`.....F.....@....rsrc.....^.....@..@.reloc...'..... (...`.....@..B.....

C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe

Process:	C:\Users\user\Desktop\SzznpUhIjo.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	870912
Entropy (8bit):	7.918235779778771
Encrypted:	false
SSDEEP:	12288:xMrny90oTgVqmNTdrA26N6DLaDYUBXaSQzuMqXlxcDtMD6Og+Clkp4NE3SNwyc:eyWLNh7baXC3eCZApgEt
MD5:	51B7FE413501DC9DD84CF1FCBB4C4BA2
SHA1:	4D55BF3929ED65E32BBD774B8C4AA112ACF211E3
SHA-256:	E7161C00B03551D7A04E547110B71BC7CBC81B0CEC26AFEC42323A0511F7F572
SHA-512:	246EFFEFC9D395F83033DD9DEE9B7C1B6D40723C1195FCCA6DFDDA1F60848A0DD6A5BA79A6E4DAB1AE2EEE059F9EF27AEBEF81304805183CAB69CC2E0BAB60C0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 68% • Antivirus: Virustotal, Detection: 65%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...K..K..K...N..K...H..K...O..K...J..K..J...K...C..K.....K...I..K.Ric h..K.....PE..L....`.b.....d.....`j.....@.....@..... .....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	179200
Entropy (8bit):	4.951892860913068
Encrypted:	false
SSDEEP:	3072:W9xqZWBJaHEDgXGJ5MS8IL1eXx9vhxbxNn2pU9f2MKTV/wi4lr55R9TxlnsPsUw9:WHqZVGJ5bHLYvh
MD5:	6FBFF2D7C9BA7F0A71F02A5C70DF9DFC
SHA1:	003DA0075734CD2D7F201C5B0E4779B8E1F33621
SHA-256:	CB56407367A42F61993842B66BCD24993A30C87116313C26D6AF9E37BBB1B6B3
SHA-512:	25842B9DF4767B16096F2BFCEDC9D368A9696E6C6D9C7B2C75987769A5B338AE04B23B1E89F18EEF2244E84F04E4ACF6AF56643A97ABFE5B605F66CBA0BAC27F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Virustotal, Detection: 80%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E.....0.....~.... .....@.. ....@.....,...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	725504
Entropy (8bit):	7.892582618323688
Encrypted:	false
SSDEEP:	12288:sMrSy90DPz6pF226NPDLPQYUBma59zh8qXlzZDZMD6ObrCrk/2/V3Sl:+yiaL0qmUuKFVu/QVw
MD5:	DB27DCB2B593E449358CEC94D3D257DA
SHA1:	9BAF8FFCA3B41D45510491BE18B3C7925D3C2BBE
SHA-256:	211AEFFAE8C6C2E01ADFA9FC68EE1383EBA739F91E2E446F0015B46A5CE3EA7E
SHA-512:	931904EF2A1707DC53914C7EB26DB142417E75461DE76E27FBA839BFDA0EEAA5FFC49B8F73D0592DC71A82D11E9B2E917FF34B53D87B709A4126B6E8A29FF1D D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...K..K..K...N..K...H..K...O..K...J..K..J...K...C..K.....K...I..K.Ric h..K.....PE..L....`.b.....d.....`j.....@.....`.....@..... .....T.....P.....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\dNT35s70.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	439808
Entropy (8bit):	6.702697953069308
Encrypted:	false
SSDEEP:	6144:UeQq/CLl3o24+WlqXjJcDwZMND6WbrhYmpCTsPrIz:N/CZ3o243TeMZMD6WbrSmUml
MD5:	685668F97D2248E1D69DA6CC1553EC0B
SHA1:	1A034138A90ECADE47AA7FD6982CC2AE3CFF7F03
SHA-256:	AE3FAA7905D107E9209BE0EA000BA94A09752AE5DF064C86E662B2B1A75554AB
SHA-512:	DCCC56807CA396489DCC3BAA4BA5BEAD515427FAAEF074B9C4F72386D25CBBC8A4446EBCE306D470EBAAB4B31062FFF1A2564B818778B3B09CEFEDC06D9F 07E5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..,...,.....,.....,.....,..0W...,..-...,.....,.....,.....,.Rich..,..... .....PE..L.....a.....4...Nm.....n.....P....@.....q.....8..d....po.....q.x...../..@..... .....text....2.....4..... ..`.data...H.k..P...B...8.....@....rsrc.....po.....z.....@..@.reloc.....q.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	351744
Entropy (8bit):	7.691266649958334
Encrypted:	false
SSDEEP:	6144:KAy+bnr+op0yN90QExDhdvfGLgfYUNcQZR0OCxH8BjFOHCFPkBVHUF+b3K5:wMrgy907DLwQYU6mROVQS8qG
MD5:	211103CF935C81941C9A7C527A99891E
SHA1:	1F57C1B0E7784F36E6123BBD9F1F750C430AB7AD
SHA-256:	F5C28886725B88C1AE31FE02A8EB8B2A7D6E72ED41D8BFB80A5C468AA41A4DDE
SHA-512:	5A4CCA86C05D356D479E9DF6A08BC98CD795234FCCD4AB15109A2316033EE7EC6D26DA04CE788E967ACEC07E32192DFE6E20A4CFA52839D6CB987A0D74328 D4C
Malicious:	**true**

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 59%
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.....@.....@..... .....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....T.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	4.97029807367379
Encrypted:	false
SSDEEP:	96:yA/vMth9sDLibql3A44P9QL4fwmPImg+A03PvXLOzk+gqWYV4J6oP/zNt:yw+wGWt94+iANiCkc4Jhp
MD5:	7E93BACBBC33E6652E147E7FE07572A0
SHA1:	421A7167DA01C8DA4DC4D5234CA3DD84E319E762
SHA-256:	850CD190AAEEBCF1505674D97F51756F325E650320EAF76785D954223A9BEE38
SHA-512:	250169D7B6FCEBFF400BE89EDAE8340F14130CED70C340BA9DA9F225F62B52B35F6645BFB510962EFB866F988688CB42392561D3E6B72194BC89D310EA43AA91
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0.."....@... ...`....@.. ..... .@.....@..O...`.....@..8..... ....H.....text.... ... ..."..... ..`.rsrc.....`.....$.....@..@.relo c.....*.....@..B.....@.....H.....T$.....0.....@s.....@...(....&*..0..K..... ?...(.....~....(....,.*r...p.....(....%..(....& ....(.... (....&.(....&*..0..e.....(....~.....+G.....o....r#..p(....,-.o.... .....(....-.*.(....&(.....o....(....&..X....i2..(....&*....0..`.....(....~.....+B.....o....r...p(....,(.o.... .....(....-.*.(....&.o....(....&..X....i2.. (....&*.0..c..... ?...(.....~....(....,.*....(.....%...(...

C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	340992
Entropy (8bit):	6.466677658359874
Encrypted:	false
SSDEEP:	6144:sZJLa5SdfYUNcQZc0OzxE8RjF/HCFPdBMkhDHK:sZJ+5ShYU6mcn5Q/K
MD5:	3930494C030BFEF77C7C0624C1F6BAEB
SHA1:	3FFC69B116C370D6372A62E1C623EA8457808152
SHA-256:	76A3221E1DCEF4CF9B0F8856DB1E20D24D782C4BF068CF76E95A57EAA6B1516E
SHA-512:	AB2A772BC04DB434AF4D2C5CD5253A3634A9679E329AD7CE53FAFDE8E7C81CDCC53B3D00F5D2CBC47EAD6BF4EFD1A0D8BAD81FD63E452D4401E3C82A7577910
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....P...P...P..(P/..P..9P...P../Pm..P#z.P...P...Py..P..&P.. .P..8P...P..=P...PRich...P.....PE..L...=..b.....m.....P.....@.....0p.....d.....n.....o..... ..P-..@.....text...h..... ..`.data...H.j.....&.....@....rsrc.....n.....@..@.reloc..l.....o.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.76751253637924
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:	SzznpUhljo.exe
File size:	1238528

MD5:	f62fe8447c5e9b9ea5ac424543ad20b3
SHA1:	847f52f9fff9b080e44de6738b61141b289cd09c
SHA256:	d7f0a894956299f235cc735af3469746f223b3394abc85660e89872503e55982
SHA512:	c003f5dba14ac90cfbfcb66c8efff3caecad59ef4938fffb4b8c9cba776bfd7363dd8e1f37174d884582e5d237f4241d404014f82617b8fcdcb77352d327a205
SSDEEP:	24576:bogX4PvpDseL3ckNcZQrKxl3fXZ16b4PEPtYn1h7Xn6iZGyF:bdoPLrcepKfBG4PEED7XF
TLSH:	5D45F14392E13C48E9268B339E1FD6E8F71EF6B1EE89676531189E2F0471172D163B90
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....P...P...P.. (P/..P..9P...P../Pm..P#z.P...P...Py..P..&P...P..8P...P..=P...PRich...P.....PE..L....Dbb.....

File Icon

Icon Hash:	a4a484a4a4a4a4e2

Static PE Info

General

Entrypoint:	0x405088
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x62624480 [Fri Apr 22 06:00:32 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	8b512f0a0b2cd54ff600ee8ace8b2bd0

Entrypoint Preview

Instruction
call 00007F6B44C7F123h
jmp 00007F6B44C7B35Eh
mov edi, edi
push ebp
mov ebp, esp
push ecx
push esi
mov esi, dword ptr [ebp+0Ch]
push esi
call 00007F6B44C7CBE5h
mov dword ptr [ebp+0Ch], eax
mov eax, dword ptr [esi+0Ch]
pop ecx
test al, 82h
jne 00007F6B44C7B4F9h
call 00007F6B44C7C48Dh
mov dword ptr [eax], 00000009h
or dword ptr [esi+0Ch], 20h
or eax, FFFFFFFFh
jmp 00007F6B44C7B614h
test al, 40h
je 00007F6B44C7B4EFh

Instruction
call 00007F6B44C7C472h
mov dword ptr [eax], 00000022h
jmp 00007F6B44C7B4C5h
push ebx
xor ebx, ebx
test al, 01h
je 00007F6B44C7B4F8h
mov dword ptr [esi+04h], ebx
test al, 10h
je 00007F6B44C7B56Dh
mov ecx, dword ptr [esi+08h]
and eax, FFFFFFFEh
mov dword ptr [esi], ecx
mov dword ptr [esi+0Ch], eax
mov eax, dword ptr [esi+0Ch]
and eax, FFFFFFEFh
or eax, 02h
mov dword ptr [esi+0Ch], eax
mov dword ptr [esi+04h], ebx
mov dword ptr [ebp-04h], ebx
test eax, 0000010Ch
jne 00007F6B44C7B50Eh
call 00007F6B44C7C76Eh
add eax, 20h
cmp esi, eax
je 00007F6B44C7B4EEh
call 00007F6B44C7C762h
add eax, 40h
cmp esi, eax
jne 00007F6B44C7B4EFh
push dword ptr [ebp+0Ch]
call 00007F6B44C7FB11h
pop ecx
test eax, eax
jne 00007F6B44C7B4E9h
push esi
call 00007F6B44C7FABDh
pop ecx
test dword ptr [esi+0Ch], 00000108h
push edi
je 00007F6B44C7B566h
mov eax, dword ptr [esi+08h]
mov edi, dword ptr [esi]
lea ecx, dword ptr [eax+01h]
mov dword ptr [esi], ecx

Rich Headers

Programming Language:	• [C++] VS2008 build 21022 • [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x109740	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27bb000	0x1a612	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27d6000	0xa9c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11f0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x2d50	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.text
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	0x109108	0x109200	False	0.9758442362093352	data	7.985785026742163	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x10b000	0x26af548	0x2600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x27bb000	0x1a612	0x1a800	False	0.38334684551886794	data	4.303385034614976	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x27d6000	0x816c	0x8200	False	0.07370793269230769	data	0.9145308616917248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x27bb8b0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27bc758	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27bd000	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27bf5a8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27c0650	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27c0ab8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Mexico
RT_ICON	0x27c1960	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Mexico
RT_ICON	0x27c2208	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Mexico
RT_ICON	0x27c28d0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Mexico
RT_ICON	0x27c2e38	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Spanish	Mexico
RT_ICON	0x27c53e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Spanish	Mexico
RT_ICON	0x27c6488	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Spanish	Mexico
RT_ICON	0x27c6e10	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Spanish	Mexico
RT_ICON	0x27c7278	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27c8120	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27c89c8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27c8f30	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico

Name	RVA	Size	Type	Language	Country
RT_ICON	0x27cb4d8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27cc580	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27ccf08	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27cd370	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27ce218	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27ceac0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27cf188	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27cf6f0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27d1c98	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27d2d40	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27d36c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_DIALOG	0x27d3b30	0x86	data		
RT_STRING	0x27d3bb8	0x490	data		
RT_STRING	0x27d4048	0x3d6	data		
RT_STRING	0x27d4420	0x492	data		
RT_STRING	0x27d48b4	0x382	data		
RT_ACCELERATOR	0x27d4c38	0x48	data	Spanish	Mexico
RT_ACCELERATOR	0x27d4c80	0x18	data	Spanish	Mexico
RT_GROUP_ICON	0x27d4c98	0x68	data	Spanish	Mexico
RT_GROUP_ICON	0x27d4d00	0x4c	data	Spanish	Mexico
RT_GROUP_ICON	0x27d4d4c	0x76	data	Spanish	Mexico
RT_GROUP_ICON	0x27d4dc4	0x76	data	Spanish	Mexico
RT_VERSION	0x27d4e3c	0x1e0	data		
RT_MANIFEST	0x27d501c	0x5eb	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		
None	0x27d5608	0xa	data		

Imports

DLL	Import
KERNEL32.dll	SetDefaultCommConfigW, CreateHardLinkA, GetConsoleAliasesA, LoadLibraryW, _hread, IsBadCodePtr, CreateEventA, FormatMessageW, GetStringTypeExW, GetExitCodeProcess, GetFileAttributesW, WriteConsoleW, WritePrivateProfileSectionW, GetLogicalDriveStringsA, ChangeTimerQueueTimer, SetLastError, GetProcAddress, GlobalAddAtomA, EnumSystemCodePagesW, LocalAlloc, FoldStringA, FreeEnvironmentStringsW, VirtualProtect, GetWindowsDirectoryW, GetFileInformationByHandle, GlobalReAlloc, InterlockedPushEntrySList, LCMapStringW, CloseHandle, CreateFileA, HeapSize, lstrcpynA, CallNamedPipeA, VirtualAlloc, GetVolumeNameForVolumeMountPointA, GetStartupInfoW, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, GetLastError, HeapFree, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetModuleFileNameA, GetModuleFileNameW, GetEnvironmentStringsW, GetCommandLineW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapReAlloc, InitializeCriticalSectionAndSpinCount, RtlUnwind, MultiByteToWideChar, LoadLibraryA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, LCMapStringA, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, RaiseException
USER32.dll	ClientToScreen, LoadMenuA, InvalidateRgn, GetMenuInfo, MessageBoxIndirectW, CountClipboardFormats, SetScrollInfo
GDI32.dll	GetGlyphIndicesW
ADVAPI32.dll	RegOpenKeyA

Possible Origin

Language of compilation system	Country where language is spoken	Map

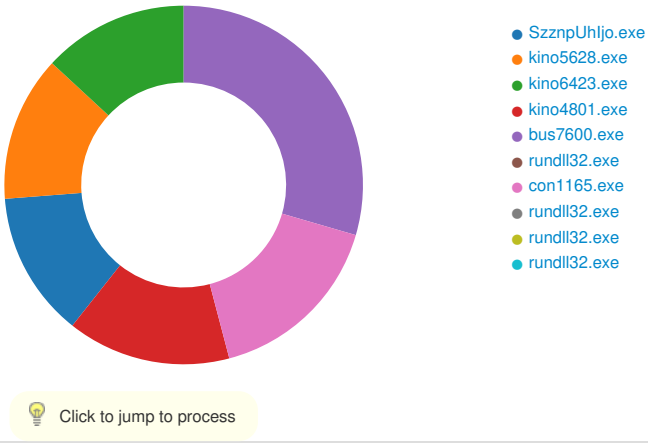
Language of compilation system	Country where language is spoken	Map
Spanish	Mexico	

Network Behavior

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

Statistics

Behavior



System Behavior

Analysis Process: SzznpUhljo.exe PID: **6092**, Parent PID: **3452**

General

Target ID:	0
Start time:	21:06:01
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\SzznpUhljo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SzznpUhljo.exe
Imagebase:	0x400000
File size:	1238528 bytes
MD5 hash:	F62FE8447C5E9B9EA5AC424543AD20B3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.341685333.0000000006A30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.341440182.0000000006880000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000003.255438944.0000000006E80000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup0	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\"	success or wait	1	402243	RegSetValueExA

Analysis Process: kino5628.exe PID: **6084**, Parent PID: **6092**

General

Target ID:	1
Start time:	21:06:02
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino5628.exe
Imagebase:	0x8e0000
File size:	870912 bytes
MD5 hash:	51B7FE413501DC9DD84CF1FCBB4C4BA2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000003.256675819.00000000046C5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 68%, ReversingLabs • Detection: 65%, Virustotal, Browse
Reputation:	moderate

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	8E5458	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	8E5949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8E48E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	8E48E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe	success or wait	1	8E5300	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\kino6423.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.$%KKKNKHKOKJKJKCKKIKRichKPEL`bd	success or wait	23	8E4B0B	WriteFile
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en239906.exe	0	28160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 45 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 01 00 00 14 01 00 00 00 00 00 7e fd 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 04 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 03 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELE0~ @ @	success or wait	6	8E4B0B	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	8E2243	RegSetValueExA

Analysis Process: kino6423.exe PID: **6028**, Parent PID: **6084**

General

Target ID:	2

Start time:	21:06:02
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino6423.exe
Imagebase:	0xe50000
File size:	725504 bytes
MD5 hash:	DB27DCB2B593E449358CEC94D3D257DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 64%, ReversingLabs
Reputation:	moderate

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	E55458	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	E55949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	E548E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dNT35s70.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	E548E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe	success or wait	1	E55300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.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	11	E54B0B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dNT35s70.exe	0	8704	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 42 2f fd 2c fd fd fd 2c fd fd fd 2c fd fd fd fd fd fd 2c fd fd fd fd fd fd 2c fd fd fd fd fd fd 2c fd fd 30 57 fd fd fd 2c fd fd fd 2d fd fd fd 2c fd fd fd fd fd fd 2c fd fd fd fd fd fd 2c fd fd fd fd fd fd 2c fd 52 69 63 68 fd fd 2c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 9c 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$B,,,,,,0W,-,,, ,Rich,PELa	success or wait	15	E54B0B	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup2	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\"	success or wait	1	E52243	RegSetValueExA

Analysis Process: kino4801.exe PID: **6116**, Parent PID: **6028**

General

Target ID:	3
Start time:	21:06:03
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino4801.exe
Imagebase:	0x10d0000
File size:	351744 bytes
MD5 hash:	211103CF935C81941C9A7C527A99891E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 59%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	10D5458	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\TMP4351$.TMP	read attributes | delete | synchronize | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	10D5949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10D48E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10D48E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe	success or wait	1	10D5300	DeleteFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe	success or wait	1	10D5300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe	0	11264	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 01 02 fd 00 00 00 00 00 00 00 00 fd 00 22 00 0b 01 30 00 00 22 00 00 00 08 00 00 00 00 00 00 fd 40 00 00 00 20 00 00 00 60 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL"0"@ `@ @	success or wait	1	10D4B0B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe	0	21504	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 40 fd fd 03 04 fd fd 50 04 fd fd 50 04 fd fd 50 1a fd 28 50 2f fd fd 50 1a fd 39 50 15 fd fd 50 1a fd 2f 50 6d fd fd 50 23 7a fd 50 0d fd fd 50 04 fd fd 50 79 fd fd 50 1a fd 26 50 05 fd fd 50 1a fd 38 50 05 fd fd 50 1a fd 3d 50 05 fd fd 50 52 69 63 68 04 fd fd 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 3d fd fd 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$@PPP(P/P9PP/Pm P#zPPPyP&PP8PP=PPRichPPEL=b	success or wait	11	10D4B0B	WriteFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanup3	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP003.TMP\"	success or wait	1	10D2243	RegSetValueExA

Analysis Process: bus7600.exe PID: **4084**, Parent PID: **6116**

General

Target ID:	4
Start time:	21:06:03
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus7600.exe
Imagebase:	0x820000
File size:	11264 bytes
MD5 hash:	7E93BACBBC33E6652E147E7FE07572A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 88%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\bus7600.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0C9386ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\bus7600.exe.log	0	226	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0	success or wait	1	7FFC0C938769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C39B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0C39B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0C4712E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C3A2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0C4712E7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center	success or wait	1	7FFC0B2FE75B	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	success or wait	1	7FFC0B2FE75B	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableIOAVProtection	dword	1	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	DisableNotifications	dword	1	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AUOptions	dword	2	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AutoInstallMinorUpdates	dword	0	success or wait	1	7FFC0B9DA911	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers	dword	1	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	UseWUServer	dword	1	success or wait	1	7FFC0B9DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate	DoNotConnectToWindowsUpdateInternetLocations	dword	1	success or wait	1	7FFC0B9DA911	RegSetValueExW

Analysis Process: rundll32.exe PID: **680**, Parent PID: **3452**

General

Target ID:	6
Start time:	21:06:14
Start date:	18/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\
Imagebase:	0x7ff6759a0000
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: con1165.exe PID: **5392**, Parent PID: **6116**

General

Target ID:	9
Start time:	21:06:18
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1165.exe
Imagebase:	0x400000
File size:	340992 bytes
MD5 hash:	3930494C030BFEF77C7C0624C1F6BAEB
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: 00000009.00000002.316570894.0000000002DA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000009.00000002.316570894.0000000002DA0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000009.00000003.291817431.0000000004510000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000009.00000003.291817431.0000000004510000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000009.00000002.316168321.0000000000400000.00000040.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000009.00000002.316168321.0000000000400000.00000040.00000001.01000000.0000000A.sdmp, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000009.00000002.316668372.0000000002E26000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs
Reputation:	moderate

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\con1165.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\con1165.exe.log	0	321	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	WriteFile

File Read

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

Registry Activities

Key Created

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

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

Key Value Created

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

Analysis Process: rundll32.exe PID: **2432**, Parent PID: **3452**

General

Target ID:	14
Start time:	21:06:22
Start date:	18/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP001.TMP\
Imagebase:	0x7ff6759a0000
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: **1504**, Parent PID: **3452**

General

Target ID:	15
Start time:	21:06:30
Start date:	18/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP002.TMP\
Imagebase:	0x7ff6759a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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: **2460**, Parent PID: **3452**

General

Target ID:	16
Start time:	21:06:44
Start date:	18/03/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe" C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP001.TMP\
Imagebase:	0x7ff6759a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly