ID: 829671
Sample Name: szDGo5lHdl.exe
Cookbook: default.jbs
Time: 20:56:13
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

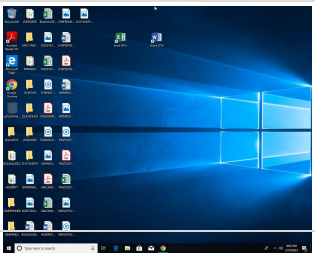
Windows Analysis Report

szDGo5lHdI.exe

Overview

General Information

Sample Name:	szDGo5lHdI.exe
Original Sample Name:	d20ba0ceff50b…
Analysis ID:	829671
MD5:	d20ba0ceff50b…
SHA1:	c7c3b7084066…
SHA256:	bfe36fe57256d…
Tags:	exe RedLineStealer
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

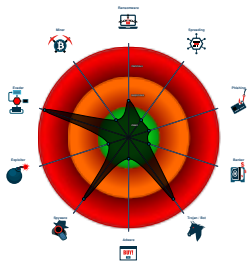
Amadey, RedLine

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Disable Windows Defender real time…
- Machine Learning detection for sam…
- Queries sensitive video device infor…

Classification



Process Tree

- **System is w10x64**
- szDGo5lHdI.exe (PID: 4688 cmdline: C:\Users\user\Desktop\szDGo5lHdI.exe MD5: D20BA0CEFF50B0A05C84F694E28462AA)
  - kino0095.exe (PID: 5248 cmdline: C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.exe MD5: 566C1099548DF136503F4DC814D54B17)
    - kino2456.exe (PID: 5212 cmdline: C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe MD5: EBD95183957BECDB18025FC9D553B15E)
      - kino0588.exe (PID: 6088 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe MD5: 54A8FD200F50B6AF0F10CA6EB68471D3)
        - bus9402.exe (PID: 6120 cmdline: C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe MD5: 7E93BACBBC33E6652E147E7FE07572A0)
        - con1332.exe (PID: 5144 cmdline: C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe MD5: 0B63FCA2981CA840B845011956E212AD)
      - dvL76s65.exe (PID: 1332 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe MD5: C49DABA1E54976E33808914E11DEE05B)
- rundll32.exe (PID: 4968 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: 812 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: 5892 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/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

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\IXP001.TMP\en675431.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.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\ge821663.exe	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.412783124.0000000004A20000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.412783124.0000000004A20000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x2d742:$pat14: , CommandLine: • 0x1f823:$v2_1: ListOfProcesses • 0x1df49:$v4_3: base64str • 0x1df08:$v4_4: stringKey • 0x1df53:$v4_5: BytesToStringConverted • 0x1df3e:$v4_6: FromBase64 • 0x1f4de:$v4_8: procName • 0x1cc30:$v5_5: FileScanning • 0x1ce4e:$v5_7: RecordHeaderField • 0x1cd80:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
0000000F.00000003.345188702.0000000002C80000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000F.00000003.345188702.0000000002C80000.00000004.00001000.00020000.00000000.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:$s3: 83 EC 38 53 B0 05 88 44 24 2B 88 44 24 2F B0 95 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... • 0x1ed8a:$s4: B|BxBtBpBlBhBdB`B\BXBTBPBLBHBDB@B<B8B4B0B,B(B$B B • 0x1e9d0:$s5: delete[] • 0x1de88:$s6: constructor or from DllMain.
0000000F.00000002.411952742.0000000002C00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.dvL76s65.exe.2cd7c6e.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
15.2.dvL76s65.exe.2cd7c6e.3.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x2c85a:$pat14: , CommandLine: • 0x1e93b:$v2_1: ListOfProcesses • 0x1d061:$v4_3: base64str • 0x1d020:$v4_4: stringKey • 0x1d06b:$v4_5: BytesToStringConverted • 0x1d056:$v4_6: FromBase64 • 0x1e5f6:$v4_8: procName • 0x1bd48:$v5_5: FileScanning • 0x1bf66:$v5_7: RecordHeaderField • 0x1be98:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
13.2.con1332.exe.2bf0e67.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
13.2.con1332.exe.2bf0e67.1.raw.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.
13.3.con1332.exe.2c20000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 37 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: 193.233.20.30	
Timestamp:	192.168.2.3193.233.20.304970141252043231 03/18/23-20:58:24.653479
SID:	2043231
Source Port:	49701
Destination Port:	4125
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: 193.233.20.30	
Timestamp:	192.168.2.3193.233.20.304970141252043233 03/18/23-20:58:07.054155
SID:	2043233
Source Port:	49701
Destination Port:	4125
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 193.233.20.30 - Destination IP: 192.168.2.3	
Timestamp:	193.233.20.30192.168.2.34125497012043234 03/18/23-20:58:08.632497
SID:	2043234
Source Port:	4125
Destination Port:	49701
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for dropped file
- Multi AV Scanner detection for submitted 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

- Snort IDS alert for network traffic
- 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)

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)

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

Found many strings related to Crypto-Wallets (likely being stolen)

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality

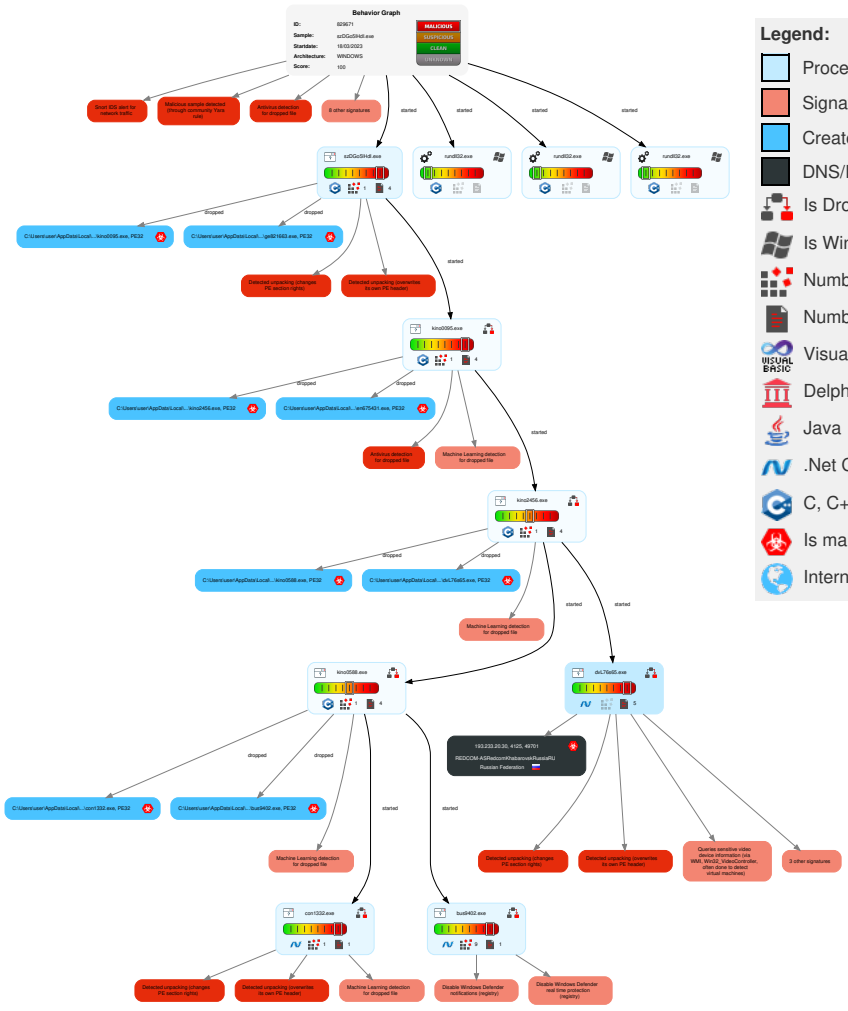
Yara detected RedLine Stealer

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	1 Windows Service	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	3 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	3 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)	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	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Service Execution	Logon Script (Mac)	1 Process Injection	2 2 Software Packing	NTDS	1 3 7 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	3 6 1 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 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	1 Masquerading	DCSync	1 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 3 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Access Token Manipulation	/etc/passwd and /etc/shadow	1 System Owner/User 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

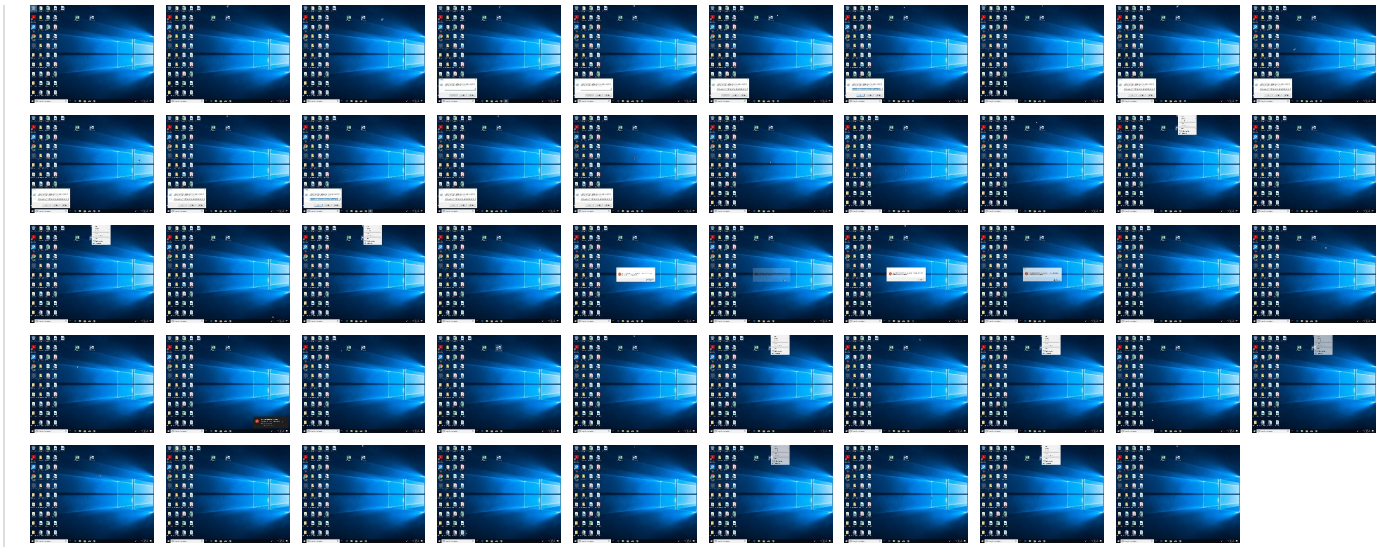
Behavior Graph



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
szDGo5lHdI.exe	46%	ReversingLabs	Win32.Trojan.Generic	

Source	Detection	Scanner	Label	Link
szDGo5lHdl.exe	45%	Virustotal		Browse
szDGo5lHdl.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge821663.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge821663.exe	63%	ReversingLabs	Win32.Trojan.Amadey	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge821663.exe	80%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.3.kino0588.exe.43e3c20.0.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
1.2.kino0095.exe.10b0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
1.0.kino0095.exe.10b0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
0.2.szDGo5lHdl.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
2.3.kino2456.exe.4eee420.0.unpack	100%	Avira	HEUR/AGEN.1253311		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
31.41.244.200/games/category/index.php	0%	URL Reputation	safe	
31.41.244.200/games/category/index.php	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/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/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	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/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://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	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/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	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/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/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	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	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/Id17Response	0%	URL Reputation	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 • URL Reputation: safe	low

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	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004FA3000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.416452346.0000000005ED2000. 00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.416452 346.0000000005F50000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000002.416452346.0000000005E3700 0.00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281318.0000 000004F16000.00000004.00000800.00020000. 00000000.sdmp, dvL76s65.exe, 0000000F.00 000002.413281318.0000000005030000.000000 04.00000800.00020000.00000000.sdmp, dvL7 6s65.exe, 0000000F.00000002.416452346.00 00000005E54000.00000004.00000800.0002000 0.00000000.sdmp, dvL76s65.exe, 0000000F. 00000002.416452346.0000000005DB9000.0000 0004.00000800.00020000.00000000.sdmp, dv L76s65.exe, 0000000F.00000002.416452346. 0000000005D5D000.00000004.00000800.00020 000.00000000.sdmp, dvL76s65.exe, 0000000 F.00000002.416452346.0000000005F8C000.00 000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.41645234 6.0000000005DD6000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.416452346.0000000005F33000. 00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281 318.0000000004DFD000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000002.416452346.0000000005EB500 0.00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281318.0000 000004E8A000.00000004.00000800.00020000. 00000000.sdmp, dvL76s65.exe, 0000000F.00 000002.416452346.0000000005CB2000.000000 04.00000800.00020000.00000000.sdmp, dvL7 6s65.exe, 0000000F.00000002.416452346.00 00000005CCF000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	dvL76s65.exe, 0000000F.00000002.41645234 6.0000000005CCF000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id12Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id7	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	dvL76s65.exe, 0000000F.00000002.41328131 8.000000000503D000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 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	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	dvL76s65.exe, 0000000F.00000002.41328131 8.000000000503D000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high

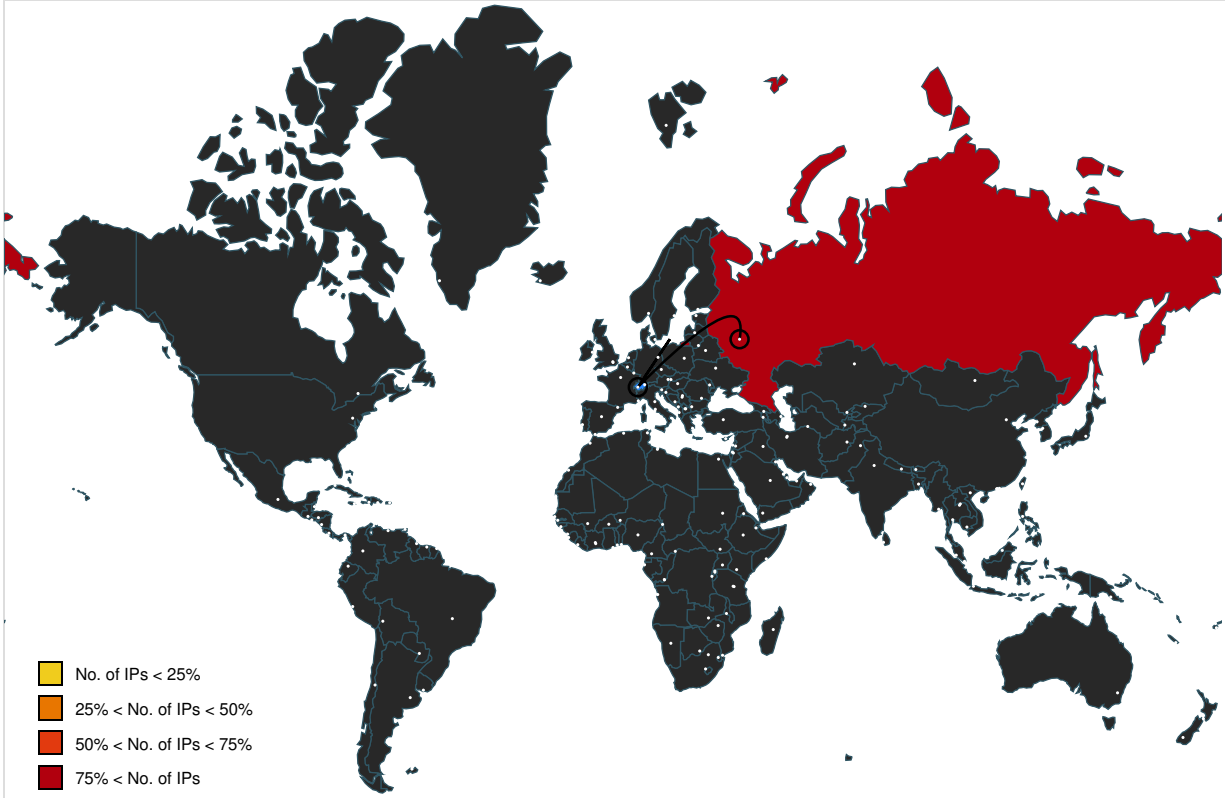
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	kino0095.exe, 00000001.00000003.26192493 1.0000000004C7C000.00000004.00000020.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.412783124.0000000004A20000. 00000004.08000000.00040000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281 318.0000000004D1E000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000003.346294709.0000000002EA000 0.00000004.00000020.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413068385.0000 000004C10000.00000004.08000000.00040000. 00000000.sdmp, en675431.exe.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm8D#	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	dvL76s65.exe, 0000000F.00000002.41645234 6.0000000005CCF000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id21	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004FA3000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.416452346.0000000005ED2000. 00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.416452 346.0000000005F50000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000002.416452346.0000000005E3700 0.00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281318.0000 000004F16000.00000004.00000800.00020000. 00000000.sdmp, dvL76s65.exe, 0000000F.00 000002.413281318.0000000005030000.000000 04.00000800.00020000.00000000.sdmp, dvL7 6s65.exe, 0000000F.00000002.416452346.00 00000005E54000.00000004.00000800.0002000 0.00000000.sdmp, dvL76s65.exe, 0000000F. 00000002.416452346.0000000005DB9000.0000 0004.00000800.00020000.00000000.sdmp, dv L76s65.exe, 0000000F.00000002.416452346. 0000000005D5D000.00000004.00000800.00020 000.00000000.sdmp, dvL76s65.exe, 0000000 F.00000002.416452346.0000000005F8C000.00 000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.41645234 6.0000000005DD6000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.416452346.0000000005F33000. 00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281 318.0000000004DFD000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000002.416452346.0000000005EB500 0.00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281318.0000 000004E8A000.00000004.00000800.00020000. 00000000.sdmp, dvL76s65.exe, 0000000F.00 000002.416452346.0000000005CB2000.000000 04.00000800.00020000.00000000.sdmp, dvL7 6s65.exe, 0000000F.00000002.416452346.00 00000005CCF000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id12	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	dvL76s65.exe, 0000000F.00000002.41328131 8.000000000503D000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com?fr=crmas_sfpf	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004FA3000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.416452346.0000000005ED2000. 00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.416452 346.0000000005F50000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000002.416452346.0000000005E3700 0.00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281318.0000 000004F16000.00000004.00000800.00020000. 00000000.sdmp, dvL76s65.exe, 0000000F.00 000002.413281318.0000000005030000.000000 04.00000800.00020000.00000000.sdmp, dvL7 6s65.exe, 0000000F.00000002.416452346.00 00000005E54000.00000004.00000800.0002000 0.00000000.sdmp, dvL76s65.exe, 0000000F. 00000002.416452346.0000000005DB9000.0000 0004.00000800.00020000.00000000.sdmp, dv L76s65.exe, 0000000F.00000002.416452346. 0000000005D5D000.00000004.00000800.00020 000.00000000.sdmp, dvL76s65.exe, 0000000 F.00000002.416452346.0000000005F8C000.00 000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.41645234 6.0000000005DD6000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.416452346.0000000005F33000. 00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281 318.0000000004DFD000.00000004.00000800.0 0020000.00000000.sdmp, dvL76s65.exe, 000 0000F.00000002.416452346.0000000005EB500 0.00000004.00000800.00020000.00000000.sdmp, dvL76s65.exe, 0000000F.00000002.413281318.0000 000004E8A000.00000004.00000800.00020000. 00000000.sdmp, dvL76s65.exe, 0000000F.00 000002.416452346.0000000005CB2000.000000 04.00000800.00020000.00000000.sdmp, dvL7 6s65.exe, 0000000F.00000002.416452346.00 00000005CCF000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004C71000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	dvL76s65.exe, 0000000F.00000002.41328131 8.0000000004D1E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17Response	dvL76s65.exe, 0000000F.00000002.41328131 8.000000000503D000.00000004.00000800.000 20000.00000000.sdmp, dvL76s65.exe, 00000 00F.00000002.413281318.0000000004C71000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.233.20.30	unknown	Russian Federation		8749	REDCOM-ASRedcomKhabarovskRussiaRU	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829671
Start date and time:	2023-03-18 20:56:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 28s
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:	szDGo5lHdl.exe
Original Sample Name:	d20ba0ceff50b0a05c84f694e28462aa.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@16/11@0/1

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 45% (good quality ratio 43.1%) • Quality average: 85.1% • Quality standard deviation: 23.8%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.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 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
20:59:20	API Interceptor	11x Sleep call for process: dvL76s65.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\UsageLogs\bus9402.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.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\con1332.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.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\Microsoft\CLR_v4.0_32\UsageLogs\dvL76s65.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MIHK5HKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHKx15:Pq5qXeqm00YqhQnouOqLqdqNq2qzcGtX
MD5:	B8422A20BE05209187B69B7EEFA138B5
SHA1:	E1FDD185B2277732AB2D728A2657291077A66811
SHA-256:	FAD57E6847B4B32DF6AE6665F75F388886058EB6CC492718EED2589D830C626E
SHA-512:	1729D8A82C212C61E2395941D3B23625A5EF09EDEA7AA25E6653827E3259EC11A38885C296E12AE82A82A1338066AFFFAEF389F21EE887DA18AC489E39B64B73
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..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, Cultu

C:\Users\user\AppData\Local\Temp\IXP000.TMP\ge821663.exe

Process:	C:\Users\user\Desktop\szDGo5lHdI.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\ge821663.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\kino0095.exe

Process:	C:\Users\user\Desktop\szDGo5lHdI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	858624
Entropy (8bit):	7.9173206349168845
Encrypted:	false
SSDEEP:	12288:lMrOy90U9S1jZY7zjt4IrITYlgomWCWx8gl0GuNVn1DTYbgiCFC7D4jghvlWTUPL:LyH9UyyI9goXZ8gRuN34mC4jqly4P
MD5:	566C1099548DF136503F4DC814D54B17
SHA1:	31F3A2230D7043D645B5451DDBCA0FECE20DE8B9
SHA-256:	B251936E101904F6A72600EB714E7127B89E19E0EF9B4A64FD1578CE62208AF5
SHA-512:	D8D4507A960834EC68786D313321EA2186B09E08C47AEC73EF5067CA60550AA1D31D88C83B90C66A1602A25B8F124254409C0002D8A3DC3044C6FF372908C4BE
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.Ric h..K.....PE..L....`.b.....d.....`j.....@.....p.....@..... .....`.....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.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\en675431.exe, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\kino2456.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	713216
Entropy (8bit):	7.890631801900666
Encrypted:	false
SSDEEP:	12288:FMrAy90gyVe3l8BrITJln173C6x8g00G4NGnmDyYygiHBCSDsv9hJlWTUP:9yxyVql8FAn1bz8gA4NhMhC7v9ly8

MD5:	EBD95183957BECDB18025FC9D553B15E
SHA1:	73A57EE27624459B13318E13148A5812F9AFC72A
SHA-256:	23B519083DBE38A5E62CAA55B223BC7E9AE9F89075E241171005B31CCF903994
SHA-512:	E4EBB6A5E5639E5A99E03F94AAA820BE48EFA6971C36B89661E8094081BF89C295CD60FE5EFE7E5DCD9517C1B5D60990BA714A5CC0287B82FE223F5B31807ABE
Malicious:	**true**
Antivirus:	• 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..K.....PE..L....`.b.....d...z.....`j.....@.....0.....y.....@..... .....Z..... .....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc....`.....\...|.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	400896
Entropy (8bit):	6.799070583318619
Encrypted:	false
SSDEEP:	6144:GpBL6vPRiUryaNB5HC6XkN9UomaZ4RPDNr:GpBGvPIUOaThCpDTQr
MD5:	C49DABA1E54976E33808914E11DEE05B
SHA1:	327511A93186C8595A55CAB5552C641FD06906C5
SHA-256:	74F627228484CC1EF30DB15DCA717A6E35D89DAB79AA42EB3E40D10E5E82E547
SHA-512:	CFAC97EEB2703D0FC11116AD405B7A1E80AB3BAB408D8456655F6B7EF319FCF548DD84EE511E429A92C42E5895CCF07FC151AFEFDED79A92BF99586D803EA353
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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.....@..... q.....d.....n.....p.....x-..@.....text..... ..`.data...H.j.....&.....@....rsrc.....n.....@..@.reloc..x.....p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	353280
Entropy (8bit):	7.694403263596913
Encrypted:	false
SSDEEP:	6144:KXy+bnr+Bp0yN90QEDbIT9olnx142x9Q4lJEXqx8gOMn0GVRaGo8vxg50mE:ZMrNy90plTylnv4AC6x8g30GfNvNmE
MD5:	54A8FD200F50B6AF0F10CA6EB68471D3
SHA1:	2952B9DAD85AD87BCE0B2EFDA76ABB1149DCE018
SHA-256:	5FCEF4C6CF8F1815B6F4B54F6ACD3140DAFA5A24AFDFD876D570FD626CD191B0
SHA-512:	00CBF08050A1AE1A7D188F8F1C265CA882D9FD15587B6F396973F8695A25727B223966A2A0886152675DFE6A6DA125FF6C9524A614578E71B5F05DFFF55A30A3
Malicious:	**true**
Antivirus:	• 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..K.....PE..L....`.b.....d.....`j.....@.....U.....@..... .....T.....@..... .....text....c.....d..... ..`.data...H.....h.....@....idata..R.....j.....@..@.rsrc.....|.....@..@.reloc.....Z.....@..B..... ....

C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.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%
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\con1332.exe

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	341504
Entropy (8bit):	6.481872228762081
Encrypted:	false
SSDEEP:	6144:NZ3LYwHUxsB2a9D4lJERA0Cr4x+WBQYLwzAW0nr:NZ38wHU2BsCi0R+Weowar
MD5:	0B63FCA2981CA840B845011956E212AD
SHA1:	293B8C4F0C8981AE5B568D1CD722E91C16476049
SHA-256:	894D2B3D57258FE980414000FE66D5A483656746A12CEBF4849D883917F13C30
SHA-512:	AA357E4991C4CCA3FA11FC0CB5483E439C398835B9361AEC715C384D319A5D43578B2E2EAB84EBB048E3B8D3F97951A997DD630D915FDCE030D499DD29D519C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
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.....a.....m.....P.....@.....0p.....d.....n.....o..... ..x-..@.....text..... ..`.data...H.j.....&.....@....rsrc.....n.....@..@.reloc..x.....o.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.764342310125714
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:	szDGo5lHdl.exe
File size:	1228288
MD5:	d20ba0ceff50b0a05c84f694e28462aa
SHA1:	c7c3b70840660f8dd81770e3bd5200eb2feda120
SHA256:	bfe36fe57256d59f04350be588333d644cf1aac03039d14dfce313aa60d42ced
SHA512:	699336726b562a7b0ab766d15e305afca0ac7137a6105381fc4832c957f5b74dd27a8da478d2908b5ccebf0fddf2ac9822856ede31e9b1432c0ad4182c952fe6
SSDEEP:	24576:u1F4VX4ZsIETa80JWFst9LqGfEBz9terTMH9MbMx9upUenl6O:u1FWWbETahMszqGfu0rYHqbMxQpPl
TLSH:	6D45F14382E27D48F9268B739E1EC2E8B70DF670DE997B653218DA2F0075176C363A51
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.....a.....

File Icon

Icon Hash:	a4a4a08484a484e0

Static PE Info

General

Entrypoint:	0x4050c8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x61EC0DDE [Sat Jan 22 13:59:58 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:	9c97db954c6eab8dfde4a4fd207d98cc

Entrypoint Preview
Instruction
call 00007F48586CA793h
jmp 00007F48586C69CEh
mov edi, edi
push ebp
mov ebp, esp
push ecx
push esi
mov esi, dword ptr [ebp+0Ch]
push esi
call 00007F48586C8255h
mov dword ptr [ebp+0Ch], eax
mov eax, dword ptr [esi+0Ch]
pop ecx
test al, 82h
jne 00007F48586C6B69h
call 00007F48586C7AFDh
mov dword ptr [eax], 00000009h
or dword ptr [esi+0Ch], 20h
or eax, FFFFFFFFh
jmp 00007F48586C6C84h
test al, 40h
je 00007F48586C6B5Fh
call 00007F48586C7AE2h
mov dword ptr [eax], 00000022h
jmp 00007F48586C6B35h
push ebx
xor ebx, ebx
test al, 01h
je 00007F48586C6B68h
mov dword ptr [esi+04h], ebx
test al, 10h
je 00007F48586C6BDDh
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

Instruction
mov dword ptr [esi+04h], ebx
mov dword ptr [ebp-04h], ebx
test eax, 0000010Ch
jne 00007F48586C6B7Eh
call 00007F48586C7DDEh
add eax, 20h
cmp esi, eax
je 00007F48586C6B5Eh
call 00007F48586C7DD2h
add eax, 40h
cmp esi, eax
jne 00007F48586C6B5Fh
push dword ptr [ebp+0Ch]
call 00007F48586CB181h
pop ecx
test eax, eax
jne 00007F48586C6B59h
push esi
call 00007F48586CB12Dh
pop ecx
test dword ptr [esi+0Ch], 00000108h
push edi
je 00007F48586C6BD6h
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	0x106f40	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27b8000	0x1a612	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27d3000	0xaa0	.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	0x2d78	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	0x106906	0x106a00	False	0.9755557249524036	data	7.985286241021559	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x108000	0x26af548	0x2600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x27b8000	0x1a612	0x1a800	False	0.38375221108490565	data	4.307961956559254	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x27d3000	0x8178	0x8200	False	0.0734375	data	0.9144732522290139	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x27b88b0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27b9758	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27ba000	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27bc5a8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27bd650	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27bdab8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Spanish	Mexico
RT_ICON	0x27be960	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Spanish	Mexico
RT_ICON	0x27bf208	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Spanish	Mexico
RT_ICON	0x27bf8d0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Spanish	Mexico
RT_ICON	0x27bfe38	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Spanish	Mexico
RT_ICON	0x27c23e0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Spanish	Mexico
RT_ICON	0x27c3488	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Spanish	Mexico
RT_ICON	0x27c3e10	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Spanish	Mexico
RT_ICON	0x27c4278	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27c5120	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27c59c8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27c5f30	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27c84d8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27c9580	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27c9f08	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27ca370	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27cb218	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27cbac0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27cc188	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27cc6f0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27cec98	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27cfd40	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Spanish	Mexico
RT_ICON	0x27d06c8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x27d0b30	0x86	data		
RT_STRING	0x27d0bb8	0x490	data		
RT_STRING	0x27d1048	0x3d6	data		
RT_STRING	0x27d1420	0x492	data		
RT_STRING	0x27d18b4	0x382	data		
RT_ACCELERATOR	0x27d1c38	0x48	data	Spanish	Mexico
RT_ACCELERATOR	0x27d1c80	0x18	data	Spanish	Mexico
RT_GROUP_ICON	0x27d1c98	0x68	data	Spanish	Mexico
RT_GROUP_ICON	0x27d1d00	0x4c	data	Spanish	Mexico
RT_GROUP_ICON	0x27d1d4c	0x76	data	Spanish	Mexico
RT_GROUP_ICON	0x27d1dc4	0x76	data	Spanish	Mexico
RT_VERSION	0x27d1e3c	0x1e0	data		
RT_MANIFEST	0x27d201c	0x5eb	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		
None	0x27d2608	0xa	data		

Imports

DLL	Import
KERNEL32.dll	GetLogicalDriveStringsW, SetDefaultCommConfigW, CreateHardLinkA, GetConsoleAliasesA, LoadLibraryW, _lread, IsBadCodePtr, CreateEventA, FormatMessageW, GetFileAttributesA, GetExitCodeProcess, SetConsoleMode, WriteConsoleW, WritePrivateProfileSectionW, 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
Spanish	Mexico	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.233.20.304970141252043231 03/18/23-20:58:24.653479	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49701	4125	192.168.2.3	193.233.20.30
192.168.2.3193.233.20.304970141252043233 03/18/23-20:58:07.054155	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49701	4125	192.168.2.3	193.233.20.30
193.233.20.30192.168.2.34125497012043234 03/18/23-20:58:08.632497	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	4125	49701	193.233.20.30	192.168.2.3

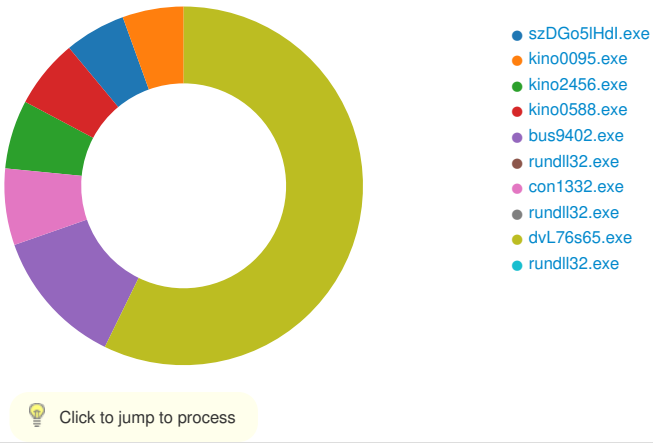
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 20:58:06.663388014 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:06.686135054 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:06.686362982 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:07.054155111 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:07.077070951 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:07.122698069 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:08.609289885 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:08.632497072 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:08.685370922 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:19.614017010 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:19.638431072 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:19.638463974 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:19.638484955 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:19.638664961 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:19.638720989 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:20.938442945 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:20.962827921 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.014508009 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.380616903 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.403899908 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.457176924 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.541018009 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.563800097 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.564196110 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.608309031 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.731764078 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.755337954 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.763166904 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.788644075 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.794116974 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.817415953 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.821443081 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:21.846554041 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:21.889859915 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:22.177835941 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:22.208134890 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:22.208218098 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:22.208268881 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:22.248943090 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:22.619117022 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:22.649648905 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:22.665638924 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:22.689857006 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:22.733931065 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:23.998817921 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.021681070 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.022135973 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.171370029 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.356787920 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.380835056 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.443901062 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.468919039 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.468954086 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.468971014 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.469019890 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.500091076 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.524600983 CET	4125	49701	193.233.20.30	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 18, 2023 20:58:24.569483995 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.594418049 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.604362011 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.627705097 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.629317045 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.652537107 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.653479099 CET	49701	4125	192.168.2.3	193.233.20.30
Mar 18, 2023 20:58:24.680087090 CET	4125	49701	193.233.20.30	192.168.2.3
Mar 18, 2023 20:58:24.712532997 CET	49701	4125	192.168.2.3	193.233.20.30

Statistics

Behavior



System Behavior

Analysis Process: szDGo5lHdl.exe PID: **4688**, Parent PID: **3452**

General

Target ID:	0
Start time:	20:58:10
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\szDGo5lHdl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\szDGo5lHdl.exe
Imagebase:	0x400000
File size:	1228288 bytes
MD5 hash:	D20BA0CEFF50B0A05C84F694E28462AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.447521600.0000000006902000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 00000000.00000003.260695646.0000000006E55000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.447701625.0000000006A00000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
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: kino0095.exe PID: **5248**, Parent PID: **4688**

General

Target ID:	1
Start time:	20:58:11
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\kino0095.exe
Imagebase:	0x10b0000
File size:	858624 bytes
MD5 hash:	566C1099548DF136503F4DC814D54B17
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: 00000001.00000003.261924931.0000000004C7C000.00000004.00000020.00020000.00000000.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\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	10B5458	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	10B5949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10B48E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10B48E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe	success or wait	1	10B5300	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\kino2456.exe	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 25 fd fd fd 4b 13 fd 4b 13 fd 4b fd fd fd 4e 52 fd 4b fd fd fd 48 52 fd 4b fd fd fd 4f 47 fd 4b fd fd fd 4a 42 fd 4b 13 fd 4a fd 0d fd 4b fd fd fd 43 5a fd 4b fd fd fd 12 fd 4b fd fd fd 49 52 fd 4b fd 52 69 63 68 fd fd 4b fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 60 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0e 0d 00 64 00	MZ@!L!This program cannot be run in DOS mode.$%KKKNKHKOKJKJKCKKIKRichKPEL`bd	success or wait	22	10B4B0B	WriteFile
C:\Users\user\AppData\Local\Temp\IXP001.TMP\en675431.exe	0	7680	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 45 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 01 00 00 14 01 00 00 00 00 00 7e fd 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 04 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 03 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELE0~ @ @	success or wait	7	10B4B0B	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	10B2243	RegSetValueExA

Analysis Process: kino2456.exe PID: **5212**, Parent PID: **5248**

General

Target ID:	2

Start time:	20:58:12
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\kino2456.exe
Imagebase:	0x960000
File size:	713216 bytes
MD5 hash:	EBD95183957BECDB18025FC9D553B15E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• 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	965458	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	965949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	9648E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	9648E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe	success or wait	1	965300	DeleteFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe	success or wait	1	965300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.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	964B0B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe	0	7168	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 00 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=PPRichPPELb	success or wait	14	964B0B	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	962243	RegSetValueExA

Analysis Process: kino0588.exe PID: **6088**, Parent PID: **5212**

General

Target ID:	3
Start time:	20:58:13
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\kino0588.exe
Imagebase:	0x190000
File size:	353280 bytes
MD5 hash:	54A8FD200F50B6AF0F10CA6EB68471D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• 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\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	195458	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	195949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1948E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1948E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe	success or wait	1	195300	DeleteFileA
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe	success or wait	1	195300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.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 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.$PEL"0"@ `@ @	success or wait	1	194B0B	WriteFile
C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe	0	21504	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 40 fd fd 03 04 fd fd 50 04 fd fd 50 04 fd fd 50 1a fd 28 50 2f fd fd 50 1a fd 39 50 15 fd fd 50 1a fd 2f 50 6d fd fd 50 23 7a fd 50 0d fd fd 50 04 fd fd 50 79 fd fd 50 1a fd 26 50 05 fd fd 50 1a fd 38 50 05 fd fd 50 1a fd 3d 50 05 fd fd 50 52 69 63 68 04 fd fd 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$@PPP(P/P9PP/P m P#zPPPyP&PP8PP=PPR ichPPELa	success or wait	11	194B0B	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	192243	RegSetValueExA

Analysis Process: bus9402.exe PID: **6120**, Parent PID: **6088**

General

Target ID:	4
Start time:	20:58:13
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\bus9402.exe
Imagebase:	0x4d0000
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
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\bus9402.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC0CB186ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\bus9402.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	7FFC0CB18769	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	7FFC0C57B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0C57B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0C6512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0C582625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0C6512E7	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	7FFC0B3DE75B	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	success or wait	1	7FFC0B3DE75B	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	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableIOAVProtection	dword	1	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	DisableNotifications	dword	1	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AUOptions	dword	2	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AutoInstallMinorUpdates	dword	0	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers	dword	1	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	UseWUServer	dword	1	success or wait	1	7FFC0BABA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate	DoNotConnectToWindowsUpdateInternetLocations	dword	1	success or wait	1	7FFC0BABA911	RegSetValueExW

Analysis Process: rundll32.exe PID: **4968**, Parent PID: **3452**

General

Target ID:	12
Start time:	20:58:25
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:	0x7ff6922f0000
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: con1332.exe PID: **5144**, Parent PID: **6088**

General

Target ID:	13
Start time:	20:58:30
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP003.TMP\con1332.exe
Imagebase:	0x400000
File size:	341504 bytes
MD5 hash:	0B63FCA2981CA840B845011956E212AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000D.00000002.328271047.0000000002DE6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000002.326634560.0000000000400000.00000040.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000D.00000002.326634560.0000000000400000.00000040.00000001.01000000.0000000A.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000002.327606223.0000000002BF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000D.00000002.327606223.0000000002BF0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000003.302283247.0000000002C20000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000D.00000003.302283247.0000000002C20000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• 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\Microsoft\CLR_v4.0_32\UsageLogs\con1332.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\con1332.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	718E5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	718E5F3C	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	718EC075	RegSetValueExW

Analysis Process: rundll32.exe PID: **812**, Parent PID: **3452**

General

Target ID:	14
Start time:	20:58:37
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:	0x7ff6922f0000
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: dvL76s65.exe PID: 1332, Parent PID: 5212

General

Target ID:	15
Start time:	20:58:44
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\dvL76s65.exe
Imagebase:	0x400000
File size:	400896 bytes
MD5 hash:	C49DABA1E54976E33808914E11DEE05B
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: 0000000F.00000002.412783124.0000000004A20000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000F.00000002.412783124.0000000004A20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000003.345188702.0000000002C80000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000F.00000003.345188702.0000000002C80000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.411952742.0000000002C00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000F.00000002.411952742.0000000002C00000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.411593767.0000000000400000.00000040.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000F.00000002.411593767.0000000000400000.00000040.00000001.01000000.0000000B.sdmp, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000F.00000002.412282672.0000000002E28000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.413281318.0000000004D1E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.412058173.0000000002C96000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000003.346294709.0000000002EA0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000F.00000002.413068385.0000000004C10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000F.00000002.413068385.0000000004C10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	718EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	718EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dvL76s65.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\dvL76s65.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 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
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\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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	718E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	11	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	718E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	718E1B4F	ReadFile
C:\Users\user\Desktop\BXAJUJAOEO.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Desktop\BXAJUJAOEO.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\BXAJUJAOEO.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\HQJBRDYKDE.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Desktop\HQJBRDYKDE.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\HQJBRDYKDE.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\LHEPQPGEWF.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\LHEPQPGEWF.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\LHEPQPGEWF.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\NIRMEKAMZH.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Desktop\NIRMEKAMZH.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Desktop\NIRMEKAMZH.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\BXAJUJAOEO.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Documents\BXAJUJAOEO.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\BXAJUJAOEO.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\HQJBRDYKDE.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Documents\HQJBRDYKDE.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\HQJBRDYKDE.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\LHEPQPGEWF.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Documents\LHEPQPGEWF.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\LHEPQPGEWF.docx	unknown	4096	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\NIRMEKAMZH.docx	unknown	4096	success or wait	1	718E1B4F	ReadFile
C:\Users\user\Documents\NIRMEKAMZH.docx	unknown	1022	end of file	1	718E1B4F	ReadFile
C:\Users\user\Documents\NIRMEKAMZH.docx	unknown	4096	end of file	1	718E1B4F	ReadFile

Analysis Process: rundll32.exe PID: **5892**, Parent PID: **3452**

General

Target ID:	16
Start time:	20:58:48
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:	0x7ff6922f0000
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

Disassembly

No disassembly