

JoeSandbox Cloud BASIC



ID: 829683

Sample Name:

pYHrqNhFKr.exe

Cookbook: default.jbs

Time: 21:03:42

Date: 18/03/2023

Version: 37.0.0 Beryl

Table of Contents

Table of Contents	2
Windows Analysis Report pYHrqNhFKr.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Threat Intel	4
Malware Configuration	5
Threatname: RedLine	5
Yara Signatures	5
Dropped Files	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	6
Snort Signatures	6
Joe Sandbox Signatures	6
AV Detection	6
Compliance	6
Networking	6
System Summary	7
Data Obfuscation	7
Lowering of HIPS / PFW / Operating System Security Settings	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	11
General Information	11
Warnings	11
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\7051zl.exe.log	12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h99af07.exe.log	12
C:\Users\user\AppData\Local\Temp\IXP000.TMP\l64fQ59.exe	13
C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe	13
C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe	13
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe	14
C:\Users\user\AppData\Local\Temp\IXP002.TMP\7051zl.exe	14
C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe	14
Static File Info	15
General	15
File Icon	15
Static PE Info	15
General	15
Entrypoint Preview	16
Data Directories	17
Sections	17
Resources	17
Imports	18
Possible Origin	19

Network Behavior	19
Statistics	19
Behavior	19
System Behavior	19
Analysis Process: pYHrqNhFKr.exePID: 2980, Parent PID: 3452	19
General	19
File Activities	20
Registry Activities	20
Key Value Created	20
Analysis Process: niba6073.exePID: 2968, Parent PID: 2980	20
General	20
File Activities	20
File Created	20
File Deleted	20
File Written	21
Registry Activities	21
Key Value Created	21
Analysis Process: niba2214.exePID: 5268, Parent PID: 2968	22
General	22
File Activities	22
File Created	22
File Deleted	22
File Written	22
Registry Activities	23
Key Value Created	23
Analysis Process: f7051zl.exePID: 5244, Parent PID: 5268	23
General	23
File Activities	24
File Created	24
File Written	24
File Read	24
Registry Activities	24
Key Created	24
Key Value Created	25
Analysis Process: rundll32.exePID: 408, Parent PID: 3452	25
General	25
File Activities	25
Analysis Process: h99af07.exePID: 6132, Parent PID: 5268	25
General	25
File Activities	26
File Created	26
File Written	26
File Read	26
Registry Activities	27
Key Created	27
Key Value Created	27
Analysis Process: rundll32.exePID: 5140, Parent PID: 3452	27
General	27
File Activities	27
Analysis Process: rundll32.exePID: 1004, Parent PID: 3452	27
General	27
File Activities	28
Disassembly	28

Windows Analysis Report

pYHrqNhFKr.exe

Overview

General Information

Sample Name:	pYHrqNhFKr.exe
Original Sample Name:	65cab4a566b1...
Analysis ID:	829683
MD5:	65cab4a566b1...
SHA1:	5628ef015cc37..
SHA256:	4700abbc439a...
Tags:	exe RedLineStealer
Infos:	

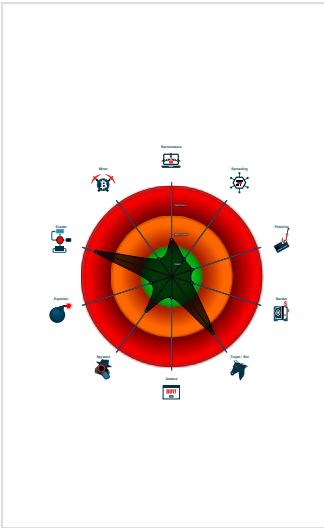
Detection

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

Signatures

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

Classification



Process Tree

System is w10x64
pYHrqNhFKr.exe (PID: 2980 cmdline: C:\Users\user\Desktop\pYHrqNhFKr.exe MD5: 65CAB4A566B172D984C8F8EBFDBDFEA0)
niba6073.exe (PID: 2968 cmdline: C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe MD5: 7ED66C765EC9F99A5D8215486D6BC8C9)
niba2214.exe (PID: 5268 cmdline: C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe MD5: 6775BA3EF89ACFDA026F96DF54C2C21D)
f7051zl.exe (PID: 5244 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\f7051zl.exe MD5: 7E93BACBBC33E6652E147E7FE07572A0)
h99af07.exe (PID: 6132 cmdline: C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe MD5: C8B5287FF76DDEC6B7F8C0DA94084603)
rundll32.exe (PID: 408 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: 5140 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: 1004 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
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	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://aunhofer.de/details/win.redline_stealer

Malware Configuration

Threatname: RedLine

```
{
  "C2_url": "193.233.20.28:4125",
  "Bot_Id": "ruka",
  "Message": "",
  "Authorization_Header": "5d1d0e51ebe1e3f16cca573ff651c43c"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\I\XP000.TMP\I64fQ59.exe	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
C:\Users\user\AppData\Local\Temp\I\XP000.TMP\I64fQ59.exe	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	0x1a430:\$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

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.307087402.0000000002E97000.0000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	0x1328:\$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000005.00000002.306344937.000000000400000.0000040.00000001.01000000.00000009.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000005.00000002.306344937.000000000400000.0000040.00000001.01000000.00000009.sdmp	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	0x1e4b0:\$s1: 23 00 2B 00 33 00 3B 00 43 00 53 00 63 00 73 00 0x80:\$s2: 68 10 84 2D 2C 71 EA 7E 2C 71 EA 7E 2C 71 EA 7E 32 23 7F 7E 3F 71 EA 7E 0B B7 91 7E 2B 71 EA 7E 2C 71 EB 7E 5C 71 EA 7E 32 23 6E 7E 1C 71 EA 7E 32 23 69 7E A2 71 EA 7E 32 23 7B 7E 2D 71 EA 7E 0x1300:\$s3: 83 EC 38 53 B0 C4 88 44 24 2B 88 44 24 2F B0 3F 88 44 24 30 88 44 24 31 88 44 24 33 55 56 8B F1 B8 0C 00 FE FF 2B C6 89 44 24 14 B8 0D 00 FE FF 2B C6 89 44 24 1C B8 02 00 FE FF 2B C6 89 44 24 ... 0x2018a:\$s4: B BxBtBpB BhBdB`B\BXBTBPBLBHbdb@B<B8B4B0B,B(B\$B B 0x1fdd0:\$s5: delete[] 0x1f288:\$s6: constructor or from DllMain.
00000005.00000002.306851644.0000000002BF0000.0000040.00001000.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000005.00000002.306851644.0000000002BF0000.0000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	0x30d:\$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.h99af07.exe.2bf0e67.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Lowering of HIPS / PFW / Operating System Security Settings



Disable Windows Defender real time protection (registry)

Disable Windows Defender notifications (registry)

Stealing of Sensitive Information



Yara detected RedLine Stealer

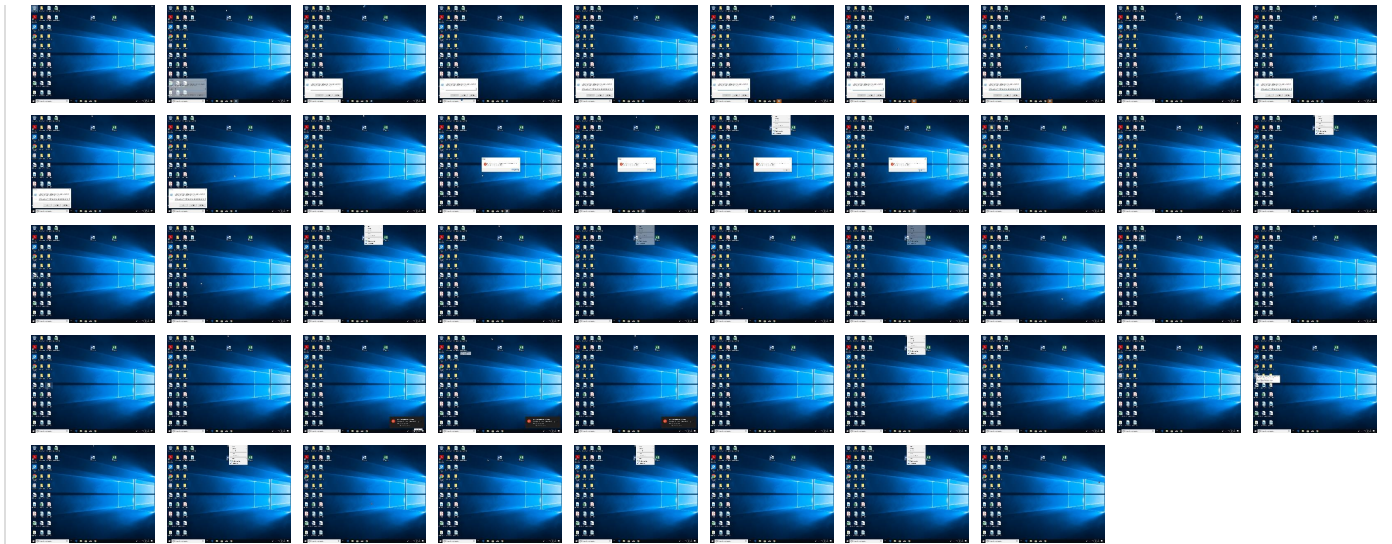
Remote Access Functionality



Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	1 Windows Service	2 Bypass User Access Control	2 1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Service Execution	Logon Script (Windows)	1 Windows Service	3 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Process Injection	2 2 Software Packing	NTDS	2 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	1 3 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Bypass User Access Control	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue



Antivirus, Machine Learning and Genetic Malware Detection				
Initial Sample				
Source	Detection	Scanner	Label	Link
pYHrqNhFKr.exe	69%	ReversingLabs	Win32.Trojan.Plug x	

Source	Detection	Scanner	Label	Link
pYHrqNhFKr.exe	51%	Virustotal		Browse
pYHrqNhFKr.exe	100%	Avira	HEUR/AGEN.1252166	
pYHrqNhFKr.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\IXP000.TMP\I64fQ59.exe	100%	Avira	HEUR/AGEN.1252166	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\I64fQ59.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\I7051zI.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\IXP000.TMP\I64fQ59.exe	88%	ReversingLabs	ByteCode-MSIL.Trojan.Whispergate	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\I64fQ59.exe	81%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe	59%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe	57%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe	49%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe	52%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe	59%	ReversingLabs	Win32.Trojan.Plugx	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe	54%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\IXP002.TMP\I7051zI.exe	88%	ReversingLabs	ByteCode-MSIL.Trojan.Casdet	
C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe	46%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.pYHrqNhFKr.exe.8a0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
2.3.niba2214.exe.4a0ec20.0.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
1.3.niba6073.exe.4577020.0.unpack	100%	Avira	HEUR/AGEN.1253311		Download File
0.0.pYHrqNhFKr.exe.8a0000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File

Domains



No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
193.233.20.28:4125	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains



No contacted domains info

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
193.233.20.28:4125	true	URL Reputation: safe	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ip.sb/ip	pYHrqNhFKr.exe, 00000000.00000003.241248149.0000000004BCC000.00000004.00000020.00020000.00000000.sdmp, l64fQ59.exe.0.dr	false	URL Reputation: safe	unknown

World Map of Contacted IPs	
	No contacted IP infos

General Information	
Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829683
Start date and time:	2023-03-18 21:03:42 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 30s
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:	18
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:	pYHrqNhFKr.exe
Original Sample Name:	65cab4a566b172d984c8f8ebfdbdfea0.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@12/8@0/0
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 58.8% (good quality ratio 56.4%) - Quality average: 85% - Quality standard deviation: 24.1%
HCA Information:	- Successful, ratio: 92% - 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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe - Excluded domains from analysis (whitelisted): fs.microsoft.com - Not all processes where analyzed, report is missing behavior information - Report size exceeded maximum capacity and may have missing behavior information. - Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\f7051zl.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\i7051zl.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wIAsDZilv:Q3La/KDLI4MWuPTxAIv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h99af07.exe.log

Process:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.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:	F76B1F538D5EA66664355901E927B2F870ACCCDD8
SHA-256:	8128CE419BBE0419F1A0BDE97C3A14E3377C0184DC1D7AF61AA01AAB756B625B
SHA-512:	151A974DDABA852144EC4BC18C548227A32E5261736F186A3920F2497434AEE9DBB0E0AB77E0E52A84A9FBC4529A158882B7549763400DDC2082D384B1135141
Malicious:	false
Reputation:	high, very likely benign file
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\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Temp\IXP000.TMP\l64fQ59.exe  	
Process:	C:\Users\user\Desktop\pYHrqNhFKr.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	179200
Entropy (8bit):	4.951964215863173
Encrypted:	false
SSDEEP:	3072:PqxZWN9abUP0Pv3Elye7597h4HxNn2pU9f2MKTv/wi4lr55R9TxlnsPsUw0jOuwM:5qZ5v3fV7h
MD5:	6C4C2A56D5DD785ADBE4FE60FA3CC1F2
SHA1:	F8BD4379310258F8E54C47B56F5EEC7394ADB9A2
SHA-256:	B182F2D3D49BDDA2E29A0ED312DEEF4BEE03983DE54080C5E97AD64422DE192D2
SHA-512:	F6958CAB80E2F7736CEA307B51BE546E50ACD5494B72DB0343A09E6EF8C446114F51BE6C9826FCB6E9F7190E4EC8415C0A403C3C1706183577C2604B877FF830
Malicious:	true
Yara Hits:	- Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\l64fQ59.exe, Author: Joe Security - Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: C:\Users\user\AppData\Local\Temp\IXP000.TMP\l64fQ59.exe, Author: ditekShen
Antivirus:	- Antivirus: Avira, Detection: 100% - Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 88% - Antivirus: Virustotal, Detection: 81%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..L.....0.....z.....@.....@.....(..O......H.....text......rsrc.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe  	
Process:	C:\Users\user\Desktop\pYHrqNhFKr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	711680
Entropy (8bit):	7.8902015677558275
Encrypted:	false
SSDEEP:	12288:wMrPy90wwLaLRKc8ivC60x+WwOwFz7/INS6nilOaHaCeDR7pxR:vyLw+wc8g30MW5xANSUiXCY7LR
MD5:	7ED66C765EC9F99A5D8215486D6BC8C9
SHA1:	F328914BCA7292FCBDF8F0E8856DA373E04DCF52
SHA-256:	B92AD2C0F810D458ACA00DAEE24510480D3483D174BA0A2957E2E08AC10000D9
SHA-512:	95B4F7838CDAB00F2FEF1215CA174F2A94B3FB58ED06432E45DF702AFBC771AA0CAB3581B370AD2E7F09D5706E89CBBF390C4738DB2A2BB2D3CF8B2716FEA0D1
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 59% - Antivirus: Virustotal, Detection: 57%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.K..K..K..N..K..H..K..O..K..J..K..J..C..K....K...I..K.Ric h..K.....PE..L...b.....d...t...`j.....@.....0.....@.....T.....T.....@..... .....text...c.....d.....`data..H.....h.....@..idata..R.....j.....@..@.rsrc...`V...j.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe  	
Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	400896
Entropy (8bit):	6.799086491924015
Encrypted:	false

SSDEEP:	6144:ipBL6vPRiUryaNB5HC6XkN9UomaZ4RPDNr:ipBGvPIUOaThCpDTQr
MD5:	096E2BA0F9570710D940FC8C2F472610
SHA1:	2ABAA5C867AA6AD1685585F2EEE03F598CB6FCCC
SHA-256:	E6BE26788855646BB6FB416D62BAB0383625C23C1A614D6819E983CCDEA9ECF
SHA-512:	B62EAA662ECBB1F71B95BFF7780F42A50E4DAC78AD8016E0F9EE47AE45D42256068AF903D63DDE45C71ACC6147AADBBB5EA6FD03A788C9D7D57D511699D2C697
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 49% - Antivirus: Virustotal, Detection: 52%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....@.....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\IXP001.TMP\niba2214.exe  	
Process:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	352256
Entropy (8bit):	7.693939457552631
Encrypted:	false
SSDEEP:	6144:Key+bnr+qp0yN90QE31x142x9Q4IJENM0Cr4x+W6QYLwztFz7MwE1w:SMrSy907v4AC60R+WnowZFz7jlw
MD5:	6775BA3EF89ACFDA026F96DF54C2C21D
SHA1:	557EE02A4A5438B9D7ED9BB6BB618B3C682ED9F7
SHA-256:	93F40046EA8851424C4E084BE7A9562EFC4553ECC9336AA7A41693A5A1382301
SHA-512:	25A1767570591807E972F459BF7D238ADC75CBA353FB81DB201A872D0D42693D62902275B389D5151342822F33BB43AA5D8D6C3F48158B038548ACB49D6C36D8
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 59% - Antivirus: Virustotal, Detection: 54%, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....%...K..K..N..K...H..K...O..K...J..K..J...K...C..K....K...I..K.Ric h..K.....PE..L....b.....d.....j.....@.....@.....\.....T.....@.....text...c.....d......data...H.....h.....@..idata..R.....j.....@...@.rsrc.....@...@.reloc.....V.....@..B.....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\f7051zl.exe  	
Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.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/vMth9sDLibql3A44P9QL4fwmPlmg+A03PvXLOzk+ggWYV4J6oP/zNt:yw+wGWt94+iANiCkc4Jhp
MD5:	7E93BACBBC33E6652E147E7FE07572A0
SHA1:	421A7167DA01C8DA4DC4D5234CA3DD84E319E762
SHA-256:	850CD190AAEEBCF1505674D97F51756F325E650320EAF76785D954223A9BEE38
SHA-512:	250169D7B6FCEBFF400BE89EDA8340F14130CED70C340BA9DA9F225F62B52B35F6645BFB510962EFB866F988688CB42392561D3E6B72194BC89D310EA43AA91
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..L....."....0.."......@.....`.....@..... .@.....@...O...`.....@..8.....H.....text.... "`rsrc.....`\$.....@...@.relo c.....*.....@..B.....@.....H.....T\$.....0.....@s.....@...(&*.0..K.....?...{.....~.....(*r...p....(%...(&...&...&...&*.0..e.....{.....~.....+G...o...#..p{.....-O.....{.....-.*{.....&{.....o{.....&X...i2... {.....&*.0..c.....?...{.....~.....{.....*.....{.....%...{.....

C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe  	
Process:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	341504

Entropy (8bit):	6.48186591893242
Encrypted:	false
SSDEEP:	6144.bZ3LYwHUxsB2a9D4IJERA0Cr4x+WBQYLwzAW0nr.bZ38wHU2BsCi0R+Weowar
MD5:	C8B5287FF76DDEC6B7F8C0DA94084603
SHA1:	A184F5E2899BC2EB8B46216866717C042AF714D1
SHA-256:	C3182B01766055A3711BD34FDEB4E6D585F8BB9C7A54BD532CE56DAF2D26219B
SHA-512:	8752AE46628FD8FF925A125AEE47853F4B28E2F1CC149D00C504439EFF0E57B1428B5751CDAC4DF82B82C9A76AB634EA1A302D8A17FC0647F20D3CF7550F1C99
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 46%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....@.....P...P...(P/..P..9P...P../Pm..P#z.P...Py..P..&P.. P..8P...P..=P...PRich...P.....PE.L.....a.....m.....P.....@.....0p...C.....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):	7.916514632003815
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:	pYHrqNhFKr.exe
File size:	856576
MD5:	65cab4a566b172d984c8f8ebfdbdfea0
SHA1:	5628ef015cc37598a43b0f032b1ef91ad7f24934
SHA256:	4700abbc439afe49697e67333bf6d3fcb04b73d73f44b40f68ed20a1e4812a8b
SHA512:	81d853e8a29305edf1c8f1039ad7d2d64ec9d694f45affdff39a9d36c455e88270bdb4bcea85fe0ce9ecd3345f631774ce868c8abf1b77f3dad844db2a561f60
SSDEEP:	24576:ByMW6YJ+DKboT0MWrOJNSAz2CjqVZAe0m:066+64fGOJIAzCVZA
TLSH:	42052253F7D46022E1BA177449F713D30A36BC91AA38436F3386A61E1D72BC9997036B
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....%...K...K...N...H...K...O...K...J...K...J...K...C...K.....K...l...K.Rich..K.....PE.L....`.b.....d.

File Icon	
	
Icon Hash:	f8e0e4e8ecccc870

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

Subsystem Version Minor:	0
Import Hash:	646167cce332c1c252cdcb1839e0cf48

Entrypoint Preview
Instruction
call 00007F67F116FC45h
jmp 00007F67F116F555h
push 00000058h
push 004072B8h
call 00007F67F116FCE7h
xor ebx, ebx
mov dword ptr [ebp-20h], ebx
lea eax, dword ptr [ebp-68h]
push eax
call dword ptr [0040A184h]
mov dword ptr [ebp-04h], ebx
mov eax, dword ptr fs:[00000018h]
mov esi, dword ptr [eax+04h]
mov edi, ebx
mov edx, 004088ACh
mov ecx, esi
xor eax, eax
lock cmpxchg dword ptr [edx], ecx
test eax, eax
je 00007F67F116F56Ah
cmp eax, esi
jne 00007F67F116F559h
xor esi, esi
inc esi
mov edi, esi
jmp 00007F67F116F562h
push 000003E8h
call dword ptr [0040A188h]
jmp 00007F67F116F529h
xor esi, esi
inc esi
cmp dword ptr [004088B0h], esi
jne 00007F67F116F55Ch
push 0000001Fh
call 00007F67F116FA7Bh
pop ecx
jmp 00007F67F116F58Ch
cmp dword ptr [004088B0h], ebx
jne 00007F67F116F57Eh
mov dword ptr [004088B0h], esi
push 004010C4h
push 004010B8h
call 00007F67F116F6A6h
pop ecx
pop ecx
test eax, eax
je 00007F67F116F569h
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, 000000FFh
jmp 00007F67F116F689h
mov dword ptr [004081E4h], esi
cmp dword ptr [004088B0h], esi
jne 00007F67F116F56Dh
push 004010B4h
push 004010ACh

Instruction
call 00007F67F116FC35h
pop ecx
pop ecx
mov dword ptr [000088B0h], 00000000h

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa28c	0xb4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0xc8b90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd5000	0x888	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1410	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1008	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa000	0x288	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6314	0x6400	False	0.5744140625	data	6.314163792045976	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x8000	0x1a48	0x200	False	0.609375	data	4.970639543960129	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xa000	0x1052	0x1200	False	0.4140625	data	5.025949912909207	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0xc9000	0xc8c00	False	0.962984267979452	data	7.941202576330205	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd5000	0x888	0xa00	False	0.746484375	data	6.222637930812128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
AVI	0xc9f8	0x2e1a	RIFF (little-endian) data, AVI, 272 x 60, 10.00 fps, video: RLE 8bpp	English	United States
RT_ICON	0xf814	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	United States
RT_ICON	0xfe7c	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	United States
RT_ICON	0x10164	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	English	United States
RT_ICON	0x1034c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	United States
RT_ICON	0x10474	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x1131c	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x11bc4	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	English	United States
RT_ICON	0x1228c	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States

Name	RVA	Size	Type	Language	Country
RT_ICON	0x127f4	0xd9d2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x201c8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x22770	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x23818	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x241a0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x24608	0x2f2	data	English	United States
RT_DIALOG	0x248fc	0x1b0	data	English	United States
RT_DIALOG	0x24aac	0x166	data	English	United States
RT_DIALOG	0x24c14	0x1c0	data	English	United States
RT_DIALOG	0x24dd4	0x130	data	English	United States
RT_DIALOG	0x24f04	0x120	data	English	United States
RT_STRING	0x25024	0x8c	Matlab v4 mat-file (little endian) I, numeric, rows 0, columns 0	English	United States
RT_STRING	0x250b0	0x520	data	English	United States
RT_STRING	0x255d0	0x5cc	data	English	United States
RT_STRING	0x25b9c	0x4b0	data	English	United States
RT_STRING	0x2604c	0x44a	data	English	United States
RT_STRING	0x26498	0x3ce	data	English	United States
RT_RCDATA	0x26868	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0x26870	0xad5fd	Microsoft Cabinet archive data, many, 710141 bytes, 2 files, at 0x2c +A "niba6073.exe" +A "I64fQ59.exe", ID 1861, number 1, 28 datablocks, 0x1503 compression	English	United States
RT_RCDATA	0xd3e70	0x4	data	English	United States
RT_RCDATA	0xd3e74	0x24	data	English	United States
RT_RCDATA	0xd3e98	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xd3ea0	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xd3ea8	0x4	data	English	United States
RT_RCDATA	0xd3eac	0xc	data	English	United States
RT_RCDATA	0xd3eb8	0x4	data	English	United States
RT_RCDATA	0xd3ebc	0xd	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xd3ecc	0x4	data	English	United States
RT_RCDATA	0xd3ed0	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xd3ed8	0x7	ASCII text, with no line terminators	English	United States
RT_RCDATA	0xd3ee0	0x7	ASCII text, with no line terminators	English	United States
RT_GROUP_ICON	0xd3ee8	0xbc	data	English	United States
RT_VERSION	0xd3fa4	0x408	data	English	United States
RT_MANIFEST	0xd43ac	0x7e2	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports	
DLL	Import
ADVAPI32.dll	GetTokenInformation, RegDeleteValueA, RegOpenKeyExA, RegQueryInfoKeyA, FreeSid, OpenProcessToken, RegSetValueExA, RegCreateKeyExA, LookupPrivilegeValueA, AllocateAndInitializeSid, RegQueryValueExA, EqualSid, RegCloseKey, AdjustTokenPrivileges
KERNEL32.dll	_lopen, _lseek, CompareStringA, GetLastError, GetFileAttributesA, GetSystemDirectoryA, LoadLibraryA, DeleteFileA, GlobalAlloc, GlobalFree, CloseHandle, WritePrivateProfileStringA, IsDBCSLeadByte, GetWindowsDirectoryA, SetFileAttributesA, GetProcAddress, GlobalLock, LocalFree, RemoveDirectoryA, FreeLibrary, _lclose, CreateDirectoryA, GetPrivateProfileIntA, GetPrivateProfileStringA, GlobalUnlock, ReadFile, SizeofResource, WriteFile, GetDriveTypeA, lstrcpA, SetFileTime, SetFilePointer, FindResourceA, CreateMutexA, GetVolumeInformationA, ExpandEnvironmentStringsA, GetCurrentDirectoryA, FreeResource, GetVersion, SetCurrentDirectoryA, GetTempPathA, LocalFileTimeToFileTime, CreateFileA, SetEvent, TerminateThread, GetVersionExA, LockResource, GetSystemInfo, CreateThread, ResetEvent, LoadResource, ExitProcess, GetModuleHandleW, CreateProcessA, FormatMessageA, GetTempFileNameA, DosDateTimeToFileTime, CreateEventA, GetExitCodeProcess, FindNextFileA, LocalAlloc, GetShortPathNameA, MulDiv, GetDiskFreeSpaceA, EnumResourceLanguagesA, GetTickCount, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, QueryPerformanceCounter, TerminateProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, GetStartupInfoW, Sleep, FindClose, GetCurrentProcess, FindFirstFileA, WaitForSingleObject, GetModuleFileNameA, LoadLibraryExA
GDI32.dll	GetDeviceCaps

DLL	Import
USER32.dll	SetWindowLongA, GetDlgItemTextA, DialogBoxIndirectParamA, ShowWindow, MsgWaitForMultipleObjects, SetWindowPos, GetDC, GetWindowRect, DispatchMessageA, GetDesktopWindow, CharUpperA, SetDlgItemTextA, ExitWindowsEx, MessageBeep, EndDialog, CharPrevA, LoadStringA, CharNextA, EnableWindow, ReleaseDC, SetForegroundWindow, PeekMessageA, GetDlgItem, SendMessageA, SendDlgItemMessageA, MessageBoxA, SetWindowTextA, GetWindowLongA, CallWindowProcA, GetSystemMetrics
msvcrt.dll	_controlfp, ?terminate@@YAXXZ, _acmdln, _initterm, __setusermatherr, _except_handler4_common, memcpy, _ismbblead, __p__fmode, _cexit, _exit, __set_app_type, __getmainargs, _amsg_exit, __p__commode, _XcptFilter, memcpy_s, _vsprintf, memset
COMCTL32.dll	
Cabinet.dll	
VERSION.dll	GetFileVersionInfoA, VerQueryValueA, GetFileVersionInfoSizeA

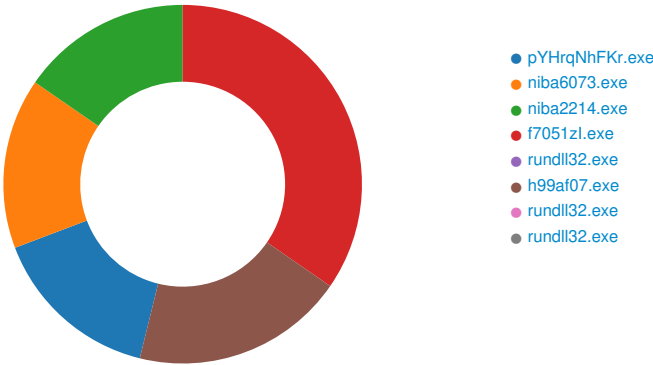
Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

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

Statistics

Behavior



- pYHrqNhFKr.exe
- niba6073.exe
- niba2214.exe
- f7051zl.exe
- rundll32.exe
- h99af07.exe
- rundll32.exe
- rundll32.exe

 Click to jump to process

System Behavior

Analysis Process: pYHrqNhFKr.exe PID: 2980, Parent PID: 3452

General

Target ID:	0
Start time:	21:04:36
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\pYHrqNhFKr.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\pYHrqNhFKr.exe
Imagebase:	0x8a0000
File size:	856576 bytes
MD5 hash:	65CAB4A566B172D984C8F8EBFDBDFA0
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: 00000000.00000003.241248149.0000000004BCC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities							
Registry Activities							
Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce	wextract_cleanupo	unicode	rundll32.exe C:\Windows\system32\advpack.dll,DelNodeRunDLL32 "C:\Users\user\AppData\Local\Temp\IXP000.TMP\"	success or wait	1	8A2243	RegSetValueExA

Analysis Process: niba6073.exe PID: 2968, Parent PID: 2980	
General	
Target ID:	1
Start time:	21:04:36
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP000.TMP\niba6073.exe
Imagebase:	0x70000
File size:	711680 bytes
MD5 hash:	7ED66C765EC9F99A5D8215486D6BC8C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 59%, ReversingLabs - Detection: 57%, Virustotal, Browse
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp\IXP001.TMP	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	75458	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	75949	CreateFileA	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	748E4	CreateFileA	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	748E4	CreateFileA	

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe	success or wait	1	75300	DeleteFileA

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.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 00 00 40 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 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 50 45 00 00 4c 01 05 00 fd 60 fd 62 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.\$%KKKNKHKOKJ KJKCKKIKRichKPEL`bd	success or wait	11	74B0B	WriteFile	
C:\Users\user\AppData\Local\Temp\IXP001.TMP\imYkV36.exe	0	8192	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 40 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 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 50 45 00 00 4c 01 04 00 14 31 62 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	13	74B0B	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	72243	RegSetValueExA

Analysis Process: niba2214.exe PID: 5268, Parent PID: 2968

General

Target ID:	2
Start time:	21:04:37
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP001.TMP\niba2214.exe
Imagebase:	0x1250000
File size:	352256 bytes
MD5 hash:	6775BA3EF89ACFDA026F96DF54C2C21D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 59%, ReversingLabs - Detection: 54%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	1255458	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	1255949	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\7051zl.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	12548E4	CreateFileA
C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	12548E4	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe	success or wait	1	1255300	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\7051zl.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\7051zl.exe
Imagebase:	0xca0000
File size:	11264 bytes
MD5 hash:	7E93BACBBC33E6652E147E7FE07572A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 88%, ReversingLabs
Reputation:	high

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0\UsageLogs\7051zl.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7FFCFD9386ED	CreateFileW	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0\UsageLogs\7051zl.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 5f 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","N otApp",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	7FFCFD938769	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	7FFCFD39B9DD	unknown	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFCFD39B9DD	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFCFD4712E7	ReadFile	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFD3A2625	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFCFD4712E7	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	7FFCFC1FE75B	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	success or wait	1	7FFCFC1FE75B	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	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableIOAVProtection	dword	1	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\Notifications	DisableNotifications	dword	1	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AUOptions	dword	2	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	AutoInstallMinorUpdates	dword	0	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoRebootWithLoggedOnUsers	dword	1	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU	UseWUServer	dword	1	success or wait	1	7FFCFC8DA911	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate	DoNotConnectToWindowsUpdateInternetLocations	dword	1	success or wait	1	7FFCFC8DA911	RegSetValueExW

Analysis Process: rundll32.exe PID: 408, Parent PID: 3452

General	
Target ID:	4
Start time:	21:04:45
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:	0x7ff704b20000
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: h99af07.exe PID: 6132, Parent PID: 5268

General

Target ID:	5
Start time:	21:04:49
Start date:	18/03/2023
Path:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\IXP002.TMP\h99af07.exe
Imagebase:	0x400000
File size:	341504 bytes
MD5 hash:	C8B5287FF76DDEC6B7F8C0DA94084603
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: 00000005.00000002.307087402.0000000002E97000.00000040.00000020.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000002.306344937.0000000000400000.00000040.00000001.01000000.00000009.sdmp, Author: Joe Security - Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000005.00000002.306344937.0000000000400000.00000040.00000001.01000000.00000009.sdmp, Author: ditekSHen - Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000005.00000002.306851644.0000000002BF0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000005.00000002.306851644.0000000002BF0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 46%, ReversingLabs
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\h99af07.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	7325C78D	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\h99af07.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	7325C907	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	72F25705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72F25705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.dll.aux	unknown	176	success or wait	1	72E803DE	ReadFile	

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	72F2CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E803DE	ReadFile

Registry Activities						
Key Created						
Key Path			Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender			success or wait	1	71E95F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features			success or wait	1	71E95F3C	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	71E9C075	RegSetValueExW

Analysis Process: rundll32.exe PID: 5140, Parent PID: 3452	
General	
Target ID:	6
Start time:	21:04:54
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:	0x7ff704b20000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities	
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.	
File Path	Completion Count Source Address Symbol

Analysis Process: rundll32.exe PID: 1004, Parent PID: 3452	
General	
Target ID:	14
Start time:	21:05:03
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:	0x7ff704b20000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high
-------------	------

File Activities

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

File Path	Completion	Count	Source Address	Symbol
-----------	------------	-------	----------------	--------

Disassembly

 No disassembly