ID: 876992
Sample Name:
un78exGoa4.exe
Cookbook: default.jbs
Time: 09:28:42
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

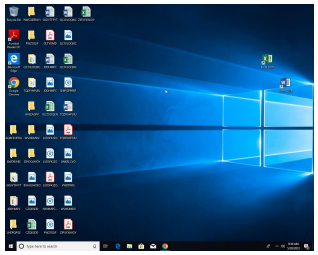
Windows Analysis Report

un78exGoa4.exe

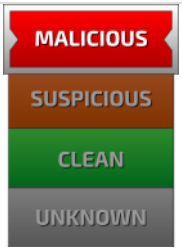
Overview

General Information

Sample Name:	un78exGoa4.exe
Original Sample Name:	84f304e30439c..
Analysis ID:	876992
MD5:	84f304e30439c..
SHA1:	257518ece774...
SHA256:	cb7f4e286a4a8..
Tags:	exe Stealc
Infos:	



Detection



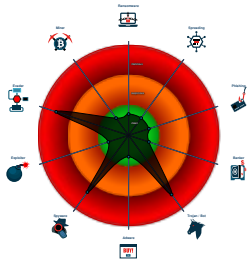
Stealc, Vidar

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

Signatures

- Multi AV Scanner detection for subm...
- Yara detected Stealc
- Malicious sample detected (through...
- Detected unpacking (overwrites its o...
- Yara detected Vidar stealer
- Detected unpacking (changes PE se...
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Tries to steal Crypto Currency Walle...
- Self deletion via cmd or bat file
- Machine Learning detection for sam...
- Found evasive API chain (may stop...

Classification



Process Tree

- **System is w10x64**
- un78exGoa4.exe (PID: 7132 cmdline: C:\Users\user\Desktop\un78exGoa4.exe MD5: 84F304E30439CF1F837ED4F31C1FBB28)
  - cmd.exe (PID: 6808 cmdline: "C:\Windows\system32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\Desktop\un78exGoa4.exe" & del "C:\ProgramData*.dll"" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7112 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Stealc	Stealc is an information stealer advertised by its presumed developer Plymouth on Russian-speaking underground forums and sold as a Malware-as-a-Service since January 9, 2023. According to Plymouth's statement, stealc is a non-resident stealer with flexible data collection settings and its development is relied on other prominent stealers: Vidar, Raccoon, Mars and Redline.Stealc is written in C and uses WinAPI functions. It mainly targets date from web browsers, extensions and Desktop application of cryptocurrency wallets, and from other applications (messengers, email clients, etc.). The malware downloads 7 legitimate third-party DLLs to collect sensitive data from web browsers, including sqlite3.dll, nss3.dll, vcruntime140.dll, mozglue.dll, freebl3.dll, softokn3.dll and msvcp140.dll. It then exfiltrates the collected information file by file to its C2 server using HTTP POST requests.	No Attribution	**http://** https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-1/https://blog.sekoia.io/stealc-a-copycat-of-vidar-and-raccoon-infostealers-gaining-in-popularity-part-2/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.stealc

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Vidar	Vidar is a forked malware based on Arkei. It seems this stealer is one of the first that is grabbing information on 2FA Software and Tor Browser.	No Attribution	http://https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-1-(-Unpacking-)/https://0x00-0x7f.github.io/A-Case-of-Vidar-Infostealer-Part-2/https://0xtoxin-labs.gitbook.io/malware-analysis/malware-analysis/vidar-stealer-h-and-m-campaignhttps://0xtoxin.github.io/malware%20analysis/Vidar-Stealer-Campaign/https://asec.ahnlab.com/en/22932/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.vidar

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.421505626.0000000002410000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000002.421100115.00000000006B5000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Stealc	Yara detected Stealc	Joe Security	
00000000.00000002.421165078.00000000006D9000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x5af9:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000000.00000002.421176016.0000000000734000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: un78exGoa4.exe PID: 7132	JoeSecurity_Stealc	Yara detected Stealc	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.un78exGoa4.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.5 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.58.8.8.865323532023883 05/28/23-09:29:39.799894
SID:	2023883
Source Port:	65323
Destination Port:	53
Protocol:	UDP

Classtype:	Potentially Bad Traffic

ET TROJAN Win32/Stealc Requesting browsers Config from C2 - Source IP: 192.168.2.5 - Destination IP: 193.106.175.215	
Timestamp:	192.168.2.5193.106.175.21549712802044244 05/28/23-09:29:40.725978
SID:	2044244
Source Port:	49712
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/Stealc Requesting plugins Config from C2 - Source IP: 192.168.2.5 - Destination IP: 193.106.175.215	
Timestamp:	192.168.2.5193.106.175.21549713802044246 05/28/23-09:29:40.856625
SID:	2044246
Source Port:	49713
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [SEKOIA.IO] Win32/Stealc C2 Check-in - Source IP: 192.168.2.5 - Destination IP: 193.106.175.215	
Timestamp:	192.168.2.5193.106.175.21549711802044243 05/28/23-09:29:40.524393
SID:	2044243
Source Port:	49711
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Malware Analysis System Evasion

Found evasive API chain (may stop execution after checking locale)

Stealing of Sensitive Information

Yara detected Stealc

Yara detected Vidar stealer

Tries to steal Crypto Currency Wallets

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

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

Remote Access Functionality

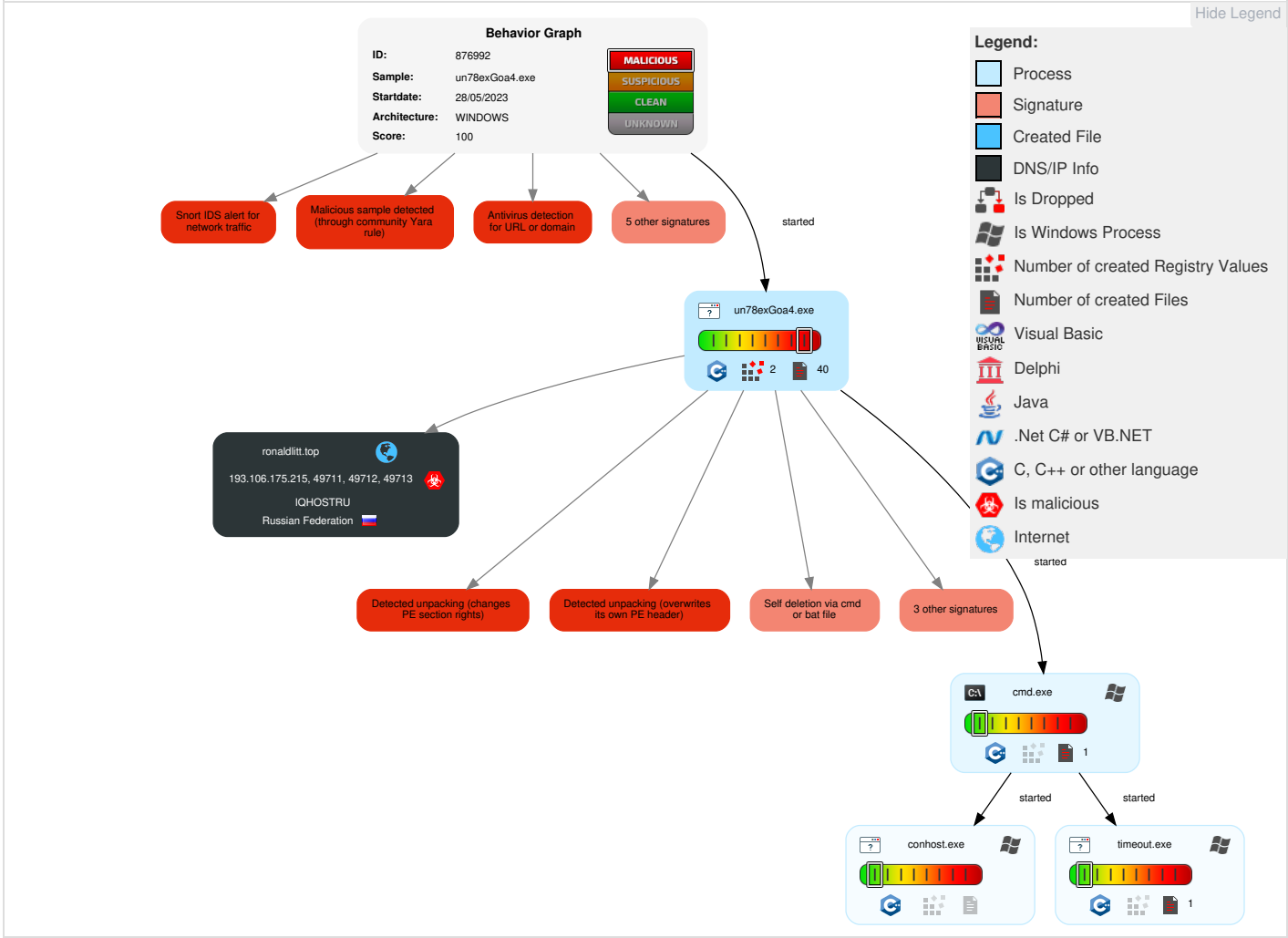
Yara detected Stealc

Yara detected Vidar 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	1 2 Native API	Path Interception	1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	1 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Input Capture	1 1 Security Software Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 2 Software Packing	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	1 System Owner/User Discovery	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	Compile After Delivery	DCSync	1 Remote System 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	Indicator Removal from Tools	Proc Filesystem	3 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 5 3 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
un78exGoa4.exe	49%	ReversingLabs	Win32.Trojan.Privateloader	
un78exGoa4.exe	38%	Virustotal		Browse
un78exGoa4.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ronaldlitt.top/3abdf8b5527012d0/sqlite3.dllY	0%	Avira URL Cloud	safe	
http://ronaldlitt.top/3abdf8b5527012d0/sqlite3.dll5	0%	Avira URL Cloud	safe	
http://ronaldlitt.top/25d4fc7fb0cb6b78.php89c6ee431893fde88e49579e17ef5	0%	Avira URL Cloud	safe	
http://ronaldlitt.top	0%	Avira URL Cloud	safe	
http://ronaldlitt.top/25d4fc7fb0cb6b78.php	100%	Avira URL Cloud	phishing	
http://ronaldlitt.top/25d4fc7fb0cb6b78.phption:	100%	Avira URL Cloud	phishing	
http://ronaldlitt.top/3abdf8b5527012d0/sqlite3.dll	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ronaldlitt.top	193.106.175.215	true	true		unknown

Contacted URLs

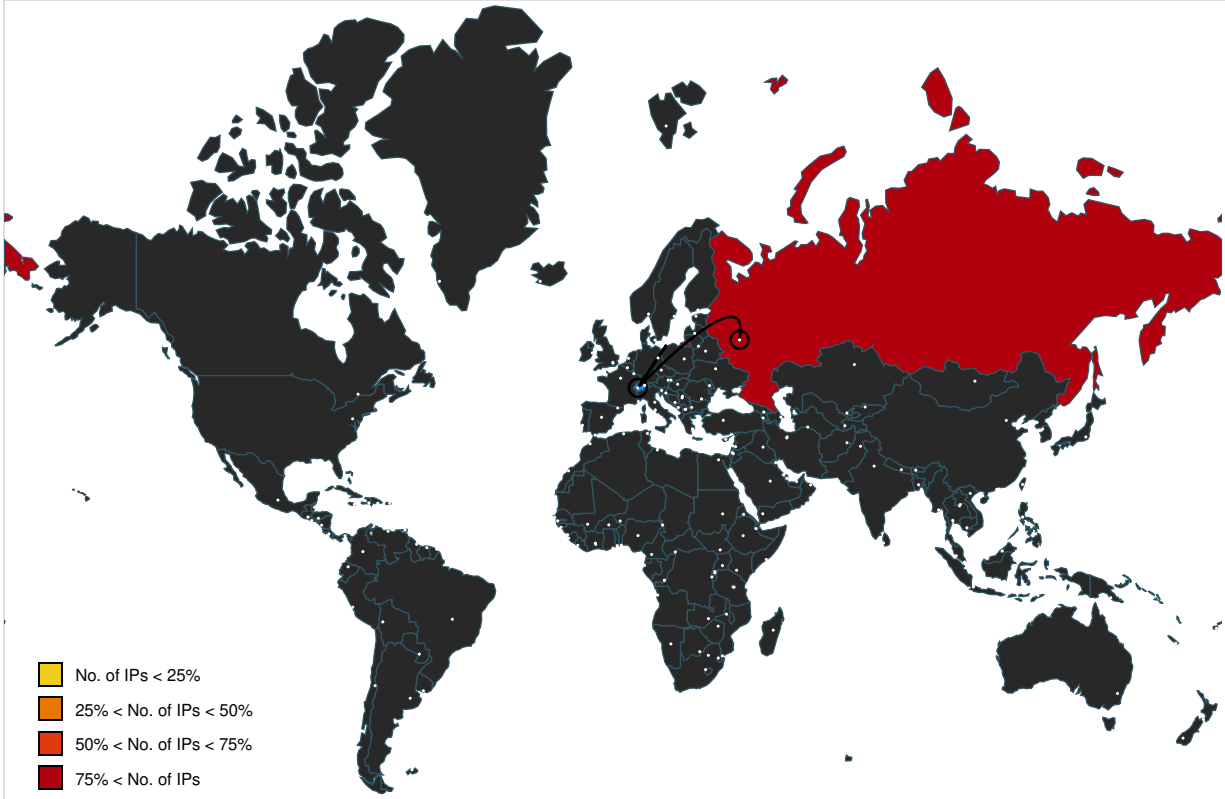
Name	Malicious	Antivirus Detection	Reputation
http://ronaldlitt.top/25d4fc7fb0cb6b78.php	true	• Avira URL Cloud: phishing	unknown
http://ronaldlitt.top/3abdf8b5527012d0/sqlite3.dll	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	FCFIJEBF.0.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	un78exGoa4.exe, 00000000.00000002.421176016.00000000007B7000.00000004.00000020.00020000.00000000.sdmp, FCFIJEBF.0.dr	false		high
http://ronaldlitt.top/3abdf8b5527012d0/sqlite3.dllY	un78exGoa4.exe, 00000000.00000002.421176016.000000000070A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	un78exGoa4.exe, 00000000.00000002.421176016.00000000007B7000.00000004.00000020.00020000.00000000.sdmp, FCFIJEBF.0.dr	false		high
http://ronaldlitt.top/25d4fc7fb0cb6b78.phption:	un78exGoa4.exe, 00000000.00000002.417733641.00000000004E5000.00000040.00000001.01000000.00000003.sdmp, un78exGoa4.exe, 00000000.00000002.417733641.00000000005B6000.00000040.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://duckduckgo.com/ac/?q=	FCFIJEBF.0.dr	false		high
http://ronaldlitt.top/25d4fc7fb0cb6b78.php89c6ee431893fde88e49579e17ef5	un78exGoa4.exe, 00000000.00000002.417733641.00000000004E5000.00000040.00000001.01000000.00000003.sdmp, un78exGoa4.exe, 00000000.00000002.417733641.0000000000429000.00000040.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	un78exGoa4.exe, 00000000.00000002.421176016.00000000007B7000.00000004.00000020.00020000.00000000.sdmp, FCFIJEBF.0.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	un78exGoa4.exe, 00000000.00000002.421176016.00000000007B7000.00000004.00000020.00020000.00000000.sdmp, FCFIJEBF.0.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	FCFIJEBF.0.dr	false		high
http://ronaldlitt.top	un78exGoa4.exe, 00000000.00000002.421100115.00000000006B5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	un78exGoa4.exe, 00000000.00000002.421176016.00000000007B7000.00000004.00000020.00020000.00000000.sdmp, FCFIJEBF.0.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	FCFIJEBF.0.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	un78exGoa4.exe, 00000000.00000002.421176016.00000000007B7000.00000004.00000020.00020000.00000000.sdmp, FCFIJEBF.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ronaldlitt.top/3abdf8b5527012d0/sqlite3.dll5	un78exGoa4.exe, 00000000.00000002.421176016.000000000070A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sqlite.org/copyright.html.	un78exGoa4.exe, 00000000.00000002.426550844.0000000032B34000.00000004.00000020.00020000.00000000.sdmp, un78exGoa4.exe, 00000000.00000002.428729273.0000000061ED3000.00000004.00001000.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.106.175.215	ronaldlitt.top	Russian Federation		50465	IQHOSTRU	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876992
Start date and time:	2023-05-28 09:28:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 27s
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:	6
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:	un78exGoa4.exe
Original Sample Name:	84f304e30439cf1f837ed4f31c1fbb28.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/19@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 90%) • Quality average: 70.1% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey 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:\ProgramData\BGDAAKJJDAAKFHJKJKFCAEHDAF

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 10, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 10
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.4393511334109407
Encrypted:	false
SSDEEP:	24:TLqlj1czkwubXYFpFNYcw+6UwcYzHrSl:TyxcYwuLopFgU1YzLSl
MD5:	8C31C5487A97BBE73711C5E20600C1F6
SHA1:	D4D6B04226D8FFC894749B3963E7DB7068D6D773
SHA-256:	A1326E74262F4B37628F2E712EC077F499B113181A1E937E752D046E43F1689A
SHA-512:	394391350524B994504F4E748CCD5C3FA8EF980AED850A5A60F09250E8261AC8E300657CBB1DBF305729637BC0E1F043E57799E2A35C82EEA3825CE5C9E7051D
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\ProgramData\BYIMNPJCRL.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696849723934257
Encrypted:	false
SSDEEP:	24:9XS3L9Z9achquy916X7oC9YYukwxDMvS7zwUzl9waqHG:hSb9Z9achACukw9Ma73KHG
MD5:	69842C9599BCE04D8727DF49107BEA31
SHA1:	C048464364668A13DD84EAC5E9B765A1D1B00D7A
SHA-256:	32C7FA5D55D3658A65B08F42FEE16884DC5EA6457AB3E6AC50995BC815377134
SHA-512:	AA0DFA923086A78927024585571D55EAA18D7C3C907A80B5DB82396769599717619B1125973479DC848ED352447C6114EB8460B8125F6C47486290884FE26480
Malicious:	false
Preview:	BYIMNPJCRLRBMQEEEUFHTSTCVFQEABUOILZJXSTRKVJYXTSCICYXTUCYTBORUVFEXVHXXHZLPHJNYDQGTPVLWILVQNCPUYBTSIQLWUERWREMYA BMDZZQTVDNTDDHAGUUVTCTOOJWFEHSBVTOXXUQRGZNKAYEATNKOEHDUHBLXOYGPQDCOFLMJTHQSYDSBPDURESTXHCQMZBOOMLDWV LKZNKZWNZJSKCJVOCLVGIKQVRJDVKWMRZZTYMEJZFGSYHHXFIVOVJRITSASFJMXNDQBLTKXRYCCLEPTRWCBSLWQQGIZLHEMWQLBCXIJLRDZVGB DMKPQCSAJHPDMQCONOLPJKQSXXWKXLWGWFLLNMOMWBJEMUURYOXEPKNSYCCDIBYHFEDOGZJJRSRKSEMLUDJXBZKLOYRGSOIOLAQQ GOKRCRGRTJLWRORHIWNHMGGIWOMOTUTBZAJWLDKALGXBHMLHYLYFZMDYBGWJNWGFVHKCBLXCJPCCAPBVNXOULSIAXANDUOFOTRQE VRFUWUFZCRTHLJQLYEGBPFFBTVSXPLLXDZYMBEAYTIBROCPJVZZSUDJWHANFEHHFHWNIBUHZUDXOLNPGFFLXTLGFZMCQYAGSBHRBITQCSUSVYI HHPNSIDTAQFELFTVTYPAWRKKUYJGRHBOBKCYSQKYEHBXDBGGWIPSQQCYDWZSIIAMYULFQOWVLCWSKUUWOHVIFAGEZJFLQYMCPCCBYXRGJOIZQI OIXSSUJSAMFTHHTCZWSIBUVVURBKAFKXSFMJOWKBXSGIZJARBEJSEPITNOSZGHQXWXOUAERJHEXAIAIJXJBCXQVJCAXHQYYJOOVFEZBKSDJJCT GJPWBAITTSUDYIKNPSTBUYHBNPCEEMIBYEKTOBEZFPKIONTMHFMSRYEGQBWJVYZOPGLWXFVPHCHOVMZAIDRTGJPBLDKIATOXKOSRGCRSMGGORA LNTMZEZXSDRSQYSYAIOLFOYGEVJDRGTSRFAUZPOU

C:\ProgramData\CZQKSDDMWR.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.700739677288544
Encrypted:	false
SSDEEP:	24:ppydEKvTSBiqFHi8v+wyNV+fxloGJjN3y5j1xTEC3ugbIvso8wFjas:rmEKvMiYC8Wwyr88GFAH/UvsuZI
MD5:	57582F5B6AE65D8DFCBD4A26382C6138
SHA1:	DC27AD5E54D1BDCCA4EC0D54ED1FB5A3235E9842
SHA-256:	7918D6E76741E42934BB32547E2D7EA395304AEA3383C0E6B7FCF82ACE125749
SHA-512:	6D75F68E608CB12378605F06C74F2F0414486072CC25961A1EA421B94EA5827F92110B902C2190E04AAE2D79152B0AB9B5B1ACECDCAAADD93A6F25028DD1E06 0
Malicious:	false

Preview:	CZQKSDDMWRVXFLQDZCLIIZCHKUTASMCLXARWUFPBFEESBCKPMBKHTZOAVUSGWGQBPZXNCLVHGKNWOAOTOSOFYOKUZEGHVYFBBGTM FWOOTOTSLTKZBTPTBZMUKYOSGWCRRYGDZWOEMUMCRRCZIEIYJAYGXMDKNOLEIKRXPEZKZGIXGYJYIBDXPZGYVGHMUCSHXXAYXQQNWIVOLMGKTX TGEAEKAOKQQSCTUWFEFQMLQUREMQDBYWFEQOMAJXVXIMMKWJJFKSSTMQZNWPBIQBZROXFYPWCYBVRMKUOGMEJJHYTWCOZYZXVANC HSTYZHRBVSORLGLSOWPDGEBVMQLDWKSLQFPEZDXWPZYNPSNTKGPNKUHFMAEGDWSDLCDNYFQZWURNIMQZDJNJPPOXINSGMUVHRDBW XOXDRPWKGITAKUVBIDIBIWIIANONNQUMKNATQWTVSOUCLOFKCCAISNABSKDPLNCYIQIFQMVEHZLIAFYDDSJJTQSUEVQKACGQHHXCYTZJABESDN XLIPGYKWXJZQWYJMSZUZHKYCGKQIKCYIWZOHAVHKCRNACDVNLPEXUPOQVKBGVFKCQDKJPNALRMAYMZRBAGMTICYZEFMXXYLDXTMKSZLDKSKSRQ TDUDGFZXFQEHEDXVFBYBNEOVKFLNIRSTGZDIJXNRZEZFJHNPZDGPGECJTHNVMTSURANVWOVRBTYGZGIPOXWTRIHNKWFKCTXVVKOFHISZVHNVVR XJGJEZEJDSCKNIDUQYQWFNDXBQQJAYENVZXKXVUERYEPFEGNWBAJHHQSAFTHXGXMHUHJVQEYGVKPBTQMWUEZMBBSFENGBBVZIYHLXFRDPALQUU RINJMTQGTPGJRGIWXIXWOPVDTWDBDNJJVXOPMTWAGMWQFUPMRROBBTRTOQBMZKPGWTYPWAVOKTSPLMOWJJDVZIIDATCEGNLHPVRONAQJFLFUZX JVRXMCGQNRKTYBRGRMKBPVPQSPFOIOHXGEGDHOJP

C:\ProgramData\DUKNXICOZT.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694015263253693
Encrypted:	false
SSDEEP:	24:pE8hRSoFxFv2tFu66PaDs7Wya/4QEssgd8uS:pE8nSoFxFvaCgoWc/gd8L
MD5:	CA67F06C14A077335756DA58259702DC
SHA1:	38A16C7089B83C544B5A58A1A91EE36AB2EE7F38
SHA-256:	6EDC691DABB9C6D794637CB2149341BB454C0490C01BBEF92C3BD48BB86B2329
SHA-512:	1754DE4F4BAC84BD0D0E605157AEFD00599B1641042A3F77AEA16614FE595B7090595C982C1679D910C20A2BF53936BAB648FF31C2CF82F3F9AD985D22EA14E
Malicious:	false
Preview:	DUKNXICOZTGLPDSRRQNKVCEQUFBSMCGTLOLLPKYXLUAXKQNZYDHXTQPNHHFHJTMIGEVVJMXNTUPFEQSTIPWCYHGFUQMXUYJBEEKJNRRCNFODXC AMAXLAZTIQUNTNPGERBSYITUYWBHPPZHKLUNSGUFMHVRZKTGCTKCZZJDJJKZRDBOFQSLPJQVAUHFJGITHWOZYPLVWBUXHBXXXJUCPJMVLNEPNK DIZKYGMCDARTHGXLNZDXRLUSQRQMRUGCFVVHERGNVXKXGPTCXBJJSYOTZHCRWDCIILVDANNRVWIHRUKXNEWVKZLEBJFPCBFWGQGWGNAHYWNRYI LMVTJYSQGDDEIOTQFNFCPBIFXMUECMBHHGKFHGYAPHBDYRWVLPTNZQXENCWRMKRIQEHFZXOHUQUMEVRRXBUGYMSBZKQNTNXORTCH QQTODUBHKLIIDLWFSVAULMVBXACHFRLSBSAGSWTRHIIZFLUSWOCTUGDAHTWKZBYIVQRRYRKRAUTQQLIUHDWFKYDUVNGBMEZUTAFTTKYLQLJJTE VOLXVXBJATRZJRTOISUFLOLZCIBSUKLPDJXJBNUXCGPOLEGGOYZSOMTIWZMXNMUQTDLWGLIFCOJBEBCJQCSUDSWMKJERKRVNPKGTBPKKHLFCUU LARSYSMUUYOBVXGHJPZEQKZTIWHIOQYDFCLYHJZKEDUCRZKCLMBUTIQDOHZOSLLXZMPKRTSVSHOIOGCLWGQOYRPDVACEIULCNRQDMRTSTZBWQM CLPDYWEXUCNSMFNSLTBNUAJKDHOPGLEHJPRKNWCKRZSOJXBNVSNBJBRTNVXHVKISJRPDYQBKOXYGOTQXOJKNGSOSFTFSIVNPFOAYLIRBSAREFW QPLONYPUBHJPFGRFFPXAQEEPWYSTOTGMJMHXBQMNEWRCBJRORHQBKISQFFCDYLOWZILZFBCXTYETKBEANFDVZBQHUOSIHHQTXPKVPTCPOPJEEG GSIDPOLYQHTCFCAHOXRL

C:\ProgramData\DUKNXICOZT.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694015263253693
Encrypted:	false
SSDEEP:	24:pE8hRSoFxFv2tFu66PaDs7Wya/4QEssgd8uS:pE8nSoFxFvaCgoWc/gd8L
MD5:	CA67F06C14A077335756DA58259702DC
SHA1:	38A16C7089B83C544B5A58A1A91EE36AB2EE7F38
SHA-256:	6EDC691DABB9C6D794637CB2149341BB454C0490C01BBEF92C3BD48BB86B2329
SHA-512:	1754DE4F4BAC84BD0D0E605157AEFD00599B1641042A3F77AEA16614FE595B7090595C982C1679D910C20A2BF53936BAB648FF31C2CF82F3F9AD985D22EA14E
Malicious:	false
Preview:	DUKNXICOZTGLPDSRRQNKVCEQUFBSMCGTLOLLPKYXLUAXKQNZYDHXTQPNHHFHJTMIGEVVJMXNTUPFEQSTIPWCYHGFUQMXUYJBEEKJNRRCNFODXC AMAXLAZTIQUNTNPGERBSYITUYWBHPPZHKLUNSGUFMHVRZKTGCTKCZZJDJJKZRDBOFQSLPJQVAUHFJGITHWOZYPLVWBUXHBXXXJUCPJMVLNEPNK DIZKYGMCDARTHGXLNZDXRLUSQRQMRUGCFVVHERGNVXKXGPTCXBJJSYOTZHCRWDCIILVDANNRVWIHRUKXNEWVKZLEBJFPCBFWGQGWGNAHYWNRYI LMVTJYSQGDDEIOTQFNFCPBIFXMUECMBHHGKFHGYAPHBDYRWVLPTNZQXENCWRMKRIQEHFZXOHUQUMEVRRXBUGYMSBZKQNTNXORTCH QQTODUBHKLIIDLWFSVAULMVBXACHFRLSBSAGSWTRHIIZFLUSWOCTUGDAHTWKZBYIVQRRYRKRAUTQQLIUHDWFKYDUVNGBMEZUTAFTTKYLQLJJTE VOLXVXBJATRZJRTOISUFLOLZCIBSUKLPDJXJBNUXCGPOLEGGOYZSOMTIWZMXNMUQTDLWGLIFCOJBEBCJQCSUDSWMKJERKRVNPKGTBPKKHLFCUU LARSYSMUUYOBVXGHJPZEQKZTIWHIOQYDFCLYHJZKEDUCRZKCLMBUTIQDOHZOSLLXZMPKRTSVSHOIOGCLWGQOYRPDVACEIULCNRQDMRTSTZBWQM CLPDYWEXUCNSMFNSLTBNUAJKDHOPGLEHJPRKNWCKRZSOJXBNVSNBJBRTNVXHVKISJRPDYQBKOXYGOTQXOJKNGSOSFTFSIVNPFOAYLIRBSAREFW QPLONYPUBHJPFGRFFPXAQEEPWYSTOTGMJMHXBQMNEWRCBJRORHQBKISQFFCDYLOWZILZFBCXTYETKBEANFDVZBQHUOSIHHQTXPKVPTCPOPJEEG GSIDPOLYQHTCFCAHOXRL

C:\ProgramData\FCFIJEBF

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.287139506398081
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944

MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3 1
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\GIGIYTFFYT.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.7020597455120665
Encrypted:	false
SSDEEP:	24:Yyd0vLZv9GwBegFWbhTY2P2m1O278kZUU3ZjGaIv:YhLZugsbh0m1bYUpjG9
MD5:	47F4925C44B6916FE1BEE7FBB1ACF777
SHA1:	D7BFAEF09A15A105540FC44D2C307778C0553CE5
SHA-256:	62FB407C253C01957EB5C9ED8075E409FD399C065B6478E5080FDC8573A1AED8
SHA-512:	6B4870B47569942B119533F4C519498D2E7D76FBBD36EC9CAE219BE800864CFA47FC65C98FDDA7D92C0B52F1EA381D7C3D5DC4DE204ABF04CED7F6C43004C B8
Malicious:	false
Preview:	GIGIYTFFYTJMXILDVGFXDVEFQCHNFYFEULLQEETZRJVMRRJHJRTSPPAOMDMYNAGWNEBMIDVTHKVEEQISBNMPHNFVYDEIXBDPFHYTCLNZABIXDF YKJDBRYRTWDLZOXHMMCFSILUYMHVQPPEGCEUDABQUBALGXBEBBTFQFPGZCSFMMFCTBAMXKOPCAJHDRXWLGLWELWIKNGHWJKDKBDV ZPNHUCSZFTPSDHZOUUHUWDVSEAQXIDUUMNXESGKGQYYBWVWCBVILKQLVAXNHJSZYYZUWKUTBRCTNQQXVQCKHLEJIFZFWACZEFAUJYVSEGBIHIZ RMKJYWHTJECURPVKKWUKKOFVGYEOSDEDBUWBYBNHTAOSHDXDTPIWBWQANBSHMKUUHFNTKLQLSWCOLNGFZPIBZTKTDJTYYNNHDUOZ EFWBJRQDBJTCXGDSCYEYJCUVSMWPBPZCBDOMCVGPOYMXSQANNOXIQBZMOMUCJZXAGIICUFLFDZJOBTEGSAQHEIBBWATDCJXSEIADCNGGARMLYL RJZSIBRRPFAORVDSNHOQWANXTRGLRQZZTEROQRQYBPGYXMSIGOYQMJDIJSQBFLNMQOGKOFUQVIWNLZBQMUSTEPCUCGVOFNLQMYFHDEDLGEYXHB HQNMKSASMZZEYCWBNZKYTKNRWJBUJJTXRIHTHPKRBWIFFKIBKCVEEYOHLCOOBFBXELQKMEOTDDLPFFLMCBOAJRNITAVONLYXBCYITNNXEUAVAV DHVGOGFHPXZDZUUQPRYTGQIFNRRHVDFAGSLTNZENPMFBPWMOHFFCIEPUUGBVHDOBSRPRHEPPLYLJUVAKAYIJRZKMAKRPYDSBIZTPWQFSZBWKYU IQXRDRUUPAWFEQRHVNMAPCFIPTHYPQPAZQNEACARWXUWSRKGERYPPRVAAPAVQYFCPYCRXLJQAMPXGLECYIZDRHPEMJPTXFOJABHMNZZHXHBCYX JEKEEQGKOAGJVHRWOSVEPEFFHDAVPR

C:\ProgramData\GLTYDMDUST.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69569301223482
Encrypted:	false
SSDEEP:	24:P1aJ3UFXnPRRqJn5Ao7J4kXjiut748cX3Gg6hQk:P1aWFX5RQnAuh48cHGg6hQk
MD5:	CA404BEA65D84F58838AF73B2DC67E02
SHA1:	56EDE3A3BF70705B1D42A2AE13F6605057C1E5F6
SHA-256:	4A28C898DF5967827C26FD633CD56275159EF4C4C0193E484E8E8F3E9ECC66B9
SHA-512:	10C144317CDB5A368733346EB8440A986A377916F98BE0E8232E668A8C5E107E06829ADF575751B94D0B0AA37F4CAC48DBD7BC64FFE8DCB140FB033C00CEC7 1
Malicious:	false
Preview:	GLTYDMDUSTFARDVTDTOSUXWTZPBTWYSDUWRWNQMOYZIOPMOCUVTIJOHJYLHKBCEDWQBIYLQPLFXNZVXOZBIBDNIIHCNZHRIZBCANIAZPBFFJNX GCWLILIHHCYJHZSFIZUUDHFLQEWBBOMWJOZCKSAOAVKAWDPLPLVPHHMTSMKFCHYLMZJYKTJZUGPCSSVJJOKBWSTSLHJSIZZNIHOVEXPMQSKABH GSGHFUWVNTWTGYCLXOQEPAIEYRMLWJNNZHEPKXAHFKJUQHDHBHMPKXFCHXQYMICUKIVHNMPIJURPFBDBUQWHFTUVKPWMJHVOENGHYYNPMJPLPT QKABBVHNTLFXAJUISPUCEXPQFWXNQKGLSPRPJEAIJQZNYNOWAKNLRQHQRIOFXWLXEJZPOKNRPRZQJIGYXOWWZDFNURUOTFOOSKCNYLZXJZIWHY YUTOQRDTTRMPEMHZSRVZISBDQKRQYXAZOKOCTHUJKZWNHJSEMHTCSKCARZUYORNVIXVWTGAWUONMQVDITNHLNLJNREIEBPKELOMXBMEUBFTSVS GBVXSXHICRIGHIFVXWPXMIKKKCBOFCJGKJYZJDAWFCHWCNIMOPOPYUXDESMSSFNZBKRVTKTFPFGCIMVLKPBRKBRZJRHIYUQFAFEODGJZAXKRAF GTBXKKKTOXYTJBCHZWBDPBSBRTICVTUOWNEXJIZFESQAIMINDZJFLHIQSMVIICPGSEVSLVSVPMBXUGAPVVXVNJEBHRRBRPIHKGVJJDRANYKMMF JJBFPKFDJAROFBZANTWLCLSELNCCDRQUPZIMXLCVFZOFWKZYXCLQVRUFHUTIFPNWERRWWXHSVZHEYMHULWKGIIWKBRWODYKIGEPXGOEZXMJVKV NTEOQXZBOZBXYKMUGZUYMELGGHJJVDPONTLTQGITEMXYMMOGRWMQDUHIGHPJWPGIEZDZPFZHQMQKLTBUGJXLBLEGTFQZOXBPYRZFHNMZGVZGRA KFYTWDWWKV

C:\ProgramData\GNLQNHOLWB.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026

Entropy (8bit):	4.698695541849584
Encrypted:	false
SSDEEP:	24:ZE+7+1bm31iNKty4eaTDMDURN6ZqyioAe1L:ZE+61bm0Qty41T5N6ZNLAeZ
MD5:	64E7020B0B401F75D3061A1917D99E04
SHA1:	785E09A2F76464E26CE282F41DE07D1B27FFB855
SHA-256:	9E5D6C897851C4A24A0D3BC4F9291A971550B9F1B9F9CFB86D7A2D5F12CD63B0
SHA-512:	14D18C0739A9B9097C2135DF001E31BA17772A9ED1DFC62318AD092C133F8C054E5C335354C57929137344E11AC6F0EBC5032211136D1F1B3F6DF8F1434D90E3
Malicious:	false
Preview:	GNLQNHOLWBOQVJIFTLNFGJNNXMGUZOMCUNVQXIPWIQSXJKHHVRYLBVHOHRRAZCZOOSABVUNECAWUZDTCLDYZAFJGGGUXKDFDPLZW HOYARDSHMWUJKNJPXNWQKOEVEVLWQLXKJLHTDQZQULYODUZGGIUHFXGBKGLAQBERUUCASFPJWCVSHYWEKXXBEZZVPBKVPPRGJJFXTGVBUVLUVQ NAPBMPJOZNNFCDPEHNHWSMZSBAYITASRGZTGXSYUNNLKZKAVLGDGRIUVYOWINQLHMWTCZYYSGNSZQWZQNLKENKZJSDTJDSZVFQGHKVENDXCIHQ VPCJNVXYVCJTKGGQJHTLGYJROSCXNGTCNNLCBSAOHAXWLQLCXTRIYCZVDEDWKBEHBEBKKXYVNQHTFFQFVFLHQRXMYLCHQAJKIRETOPSMFDVMJO ROHVBDNWQMACXDCGCPKSQUIXWYXSYDPSBSUJMXEBPBCWJDOKOSFYRZQSCWEIHCQFTRYQVAUUYDVCYUHDRUKCTOGNWSTPHONXNHSH ICTVCMWIDPOKQMNGFKZOADDJPTUVPEWWFNEKDLAVDZNBHHFIRSPGSQGUQUGGIRSVJTEIAUJEHUVHRJPWEMACBNRIWVFWWRDNGHYA ESSKWHOCXLPYRMKQYTXSSYLKESQEPWVDSSTKTYQDQTTAUVWPQFTTJMGMEGRECDIFCMPKXTYYNGENSBDKEVPPDNRRDLULORZGHRQI QWLMHMKLKDLNSNWXWGTMDLMPWAGGPUJXOOYWOGWZTDKIVNNXMKJEFALSJECCOVZVTAPKGAXWCUMHLAHYBPLBTDXBKKPKPJFJOKZK MPEWOOMMMCZHSENRPGKEJJHHOVFETVBBFBTDTSNLGGPVPAFDOXRJUKYZTGOFQUAVOGUZJARUUCKMRYUSWZIRYUATBQRRVCNMFMMB TGSFQCAOTPTSBPCICPBMURXQOIITZCLXKSJVDGFLGHUIHTALRYCNLFILDCLQXDOGMOKPXT

C:\ProgramData\HDHCGHDHIDHCBGCBGCAE

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\ProgramData\HVLFEFMHHB.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.688192278065048
Encrypted:	false
SSDEEP:	24:QpAScqpJqU2M0r6gHGZdxsLVOo2qf4l5MRduGv:QPtbqE0r4xMZ2qf4X
MD5:	E6B83E7618DE7C60467C035027CADC38
SHA1:	7A0812266C40EAF0F9C8829B49E087AD90D94E9C
SHA-256:	8391D2A7645B06DDB986C1A54E0AED11D95709A36D069D086620E8826BC3A330
SHA-512:	C36C40C23B7859FC2B2F87A8EDFEF247C68BC561BA1482C67EF5581B562A2937B1699325B94D5FEFA6C871E03FFDF15F1A3DB50E4C320FB2AD1E632E0947FDCB
Malicious:	false
Preview:	HVLFEFMHHBAZDOLLZUNPNIMHDSYDQCISTUECHUCHKIAZZFSVBOELUIHPSHSXTNSPZDGIETMGXZOYQTZRMDJQFPHHJHCMEQAMYDDSLZLLUVDYXM VXMJISSAHCKPLCLDDBZUFIHVCCXHATRPSYNOHWXWJCDWDHDDSPCXHPEIXNETRDYBQVDZCZSCETYTSJIPSGEXYYNWAPSXUGLJGMVDMSILOBIVRF UBILUJUUFFXRNCZYXSQGJHKUDBDJGZWNGLJTNJADAFVOPOEFRDJKVPITPOGUIZYBSRBAAHELWONYMPDQZRAGDWEYGIKGSEGSKLXCRIXYVYCNLF APZDPVJDSTOJJHRBYAFVUUHUPTGDCDAPEFBLYIAHZQXIZVAXOXOWQBKLVAPOMJLDTVBONRQXSZVABHXMVKXAHVBIWXPKRGZTDKAMPDAXSWNKCN NSMKKEECAANVALIIUEAXTYSXOKCYQYYXZTEBBANDVEICJYYAJPCRNGLJYSKLTEWKKIAXTZLKICCIAOQPAOQVEJXZPIYIXVSONSXMGRCKSVBNLN AKITKHATKVOAKZESLANUYNJSIOBTYYPZRGWXHMQEGVVXXRBNEVVYRTZWBSBZXBCTWATGHIYCHGUZXZLMYYHKVDAYMGQCLNOREHTSWUSWKHGEHR JJXNCAWTDRWOVTMGLOTCFSEWPQOLOOKFURNEANRYAOHFWBHJZKWTCLPCRLHHDVHKOLGCJQPRJFRUIBVIZISBXZQXHSJNMVPMLGKPIUUWWSDCKS OOKYNCPBNMWIEHWOTNUZYEZNJPVYKEUWDEEGMHFTVODLUKMYGXMOIQNSORSIJQDOIDNLRNHVCEAJNRJTMHQTNPWKWGMSDSPCXTWT IXGFTYXSNTASOZIBWKTZVHVXHWDZNBVOJXKIZAIZOUVEGBNGHYRGUKVNBWAJQMCAZRJGMOBMXLQXXVXCKJKYVDWBTSZUJDTZUKJCTZDHHLCOTJ GUSHFTFJZNKKTJVWMSES

C:\ProgramData\JDDHMPCDUJ.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators

Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.687055908915499
Encrypted:	false
SSDEEP:	24:X3rfasg2Tpd/zBJY+q9FZP0DJR6BdqWD5gB8H36D6jXLiUk2ZTV:X+52L/dJYBjYJRoddD5C8HqD8ZDZTV
MD5:	94EDB575C55407C555A3F710DF2A8CB3
SHA1:	3AB8DF4B92C320D7D4C661EAB608E24B43F3DD13
SHA-256:	DD3A4A93D60E4B7840557A44DAAF77F6B6F85032C7DD5FB10BE54C07B0E1E261
SHA-512:	F8F78D10AE19735413AF11F0C8DAC41644479D345DC6B300412DEDA9779A01DDFC7150FBFD54F2582A0DF8524B7E507886DBC49E59B084320017E9E64FC8DBF A
Malicious:	false
Preview:	JDDHMPCDUJFORBKGTIFQHFPQNEKFAIHGBDYZBWNZMVTSZXTGRUOCZPQRXMGXBNMAHGODCTVNAHQHZMJYIYXLTVDMEAVEXSWFQCDVPRSSLREITY MWHUXVVKLPJXQJOHYPAVYXSIMBBOTIWYDKNCDVKZZMEIFEDNNXHAHMYLPOUGNKMPZVDEQRUPZBQCKZDQINFECCUZINROAFGLIAMVWHXPPXOWZM WTITWBJFIENEHRXRHRPVUAIUAJUYDBBSQQMTJJXOAAMHVKJEOIQRSNKKQSGCHAUKUYPJEBZIGZTVKUXZEQOUSZPQBHKFHECDNFGTGIDHSJFVLA KZPDYVJVWECRIKKUCCFNNHBLBFCJEKSUZTITTTLQVOHKFHXFIIYDOZNAIBCDIRXJAYKHCOEXBOGSGEGGQEMHFXIZREOFZJSAFXTGSSZLVKYOAN MZNPNESDZMFYWTZHIKUSMZXACWZEIMGTFRSZCGICPOSTZRECQYWZECQVLAWXESWPCDXLHIMJHSZJSDAXNXHETAWLZDXTZAPKBHSMKMYYGVSJCU IJSIFUHHMPIRBASPUOUXKKPQCECQBBZUSIXEOXLFFSQIFCTAIRASCMWEHFOXGEJRXFGJODUTKITHEAKFFJQTQNWWKXXDELWDHHEDWUTMSLXQJP VGOBKELYSRBQFYKXFHWGSCVLTCFKOEJMLUXIZVDPFHXHTSMTDRTVCNLISGJFVQRUTMZDYPUYBAEASZCSEUVHWRIQDEJIZQQHJNTIIICFMMPVLX OIVTPCTDKFPDVWXSBXZDXFUMBJTJMKOOHIMIOAKEJSIDIOJSRMRYXLDVGDBBYXARBNHXOXMBXYOTEFOAXRAUKXTWKYYGWNAHHCIIKQHYAETGBW ABTEMJKNTEUQAWGHRIKDGGNHUIVVPPYPYTZERZKDPLUSIKPBDPJOCBYQJDEKAVQKHFTPBZJQOUCVBHAHZZGEXOCYGYDCZICBOETRSJSMVEZKIN DRIKZYTUIS

C:\ProgramData\KLIZUSIQEN.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696703751818505
Encrypted:	false
SSDEEP:	24:b16WkAmEUwq/rBFGdG3NQGsu7DYh3NTgfAtxoLxLP/VEmcM:hkAYzzbG4NPsuYh3N0fAjaxLnl
MD5:	19255ED5D4F37A096C105CEF82D0F5C0
SHA1:	96C5E995A91C8BC479E1C2ADB32C7E022EB8FAC7
SHA-256:	A0E9C6A5B14DB7AB22994C5017930720299F4492CE99D95A07BEB46BF2BAE7E8
SHA-512:	CDCD7E54677DE3BCE65BD80C855DE9684517F931ECA4D17E984C1D02E5E5CE9B50582ECCFA43F71A4F0A4E1743D74FCF3D588424AF519BFAE628EA49082C6 E68
Malicious:	false
Preview:	KLIZUSIQENZWQAFPHPIZMRSSYSYIINGOAPFQHPCFTPTNYLSNMTRTDZSWEBKDRHIUFOFGWKTHENHAQWTYTMOJNOWPWJAPIZKOPDMUAKVTHXYWDB HBVWDTBCFVXJHDCUGTPASHSDSKUVYPRPPUXKURDNZYJENQKRHCARIUAOIAFRFWGQDXOAPXUJAUWRVEASXCVARWJMIPINSQDPGOWLRMNRCAEZGZ IYDWBEWCOJWHLMOUROGZKCFGXDKPHAJADQCYUZYSYXQOIEGZIJWZLUJEKZUASKHQOGVFGVEXIQTENJDEKERNBPZGKNXWYZVXDDAYNSFBZAKWCE EYDSJONDKOYOBSAVICMHPZZRHRLNYDOIDQNYLXFDCCUOIJANPQCOIJDXFLDMIBVHBYSNYGAVWTHYCIPBRPTWSQXWXZZJBFNAUOMALKDRYIMJCR JXXQXCEREPQGNQHHOFEMEOXMSZEWOLTOLCOUCQNPRIPXUSVZNATFZKIJQZKGKTCYOMBXFTSXBXYIHMOONWWGRKPSNEMONASEFSVW NWIBXDSMEKQJIDCFPVMGAAUPBVOYAIKYQEFVSXOFTEMHNXVNMMENORLDYPZUSILNZRPHITCWDQMLEFZOEGPJDXQLBSIYRONLBYOSJVTEMBHNVX CMMRDVOAYSMNNRKRLBSQBIWIWHYUMBKTIYQTROZKTGZZMEFWINSQAXMWWLRRSPXAQZURXOTMUHPNLOUWMXRQSGXIAQILQCZUUTRJ ZVRNLBSHADNHZSDOQIYIZCEZHFRITTHSZOSBZGNCQVHXSFZJCEVSJCZZYTCFXLNBKMTPXYHPDXMMMXHUAAQWYYFHMKXWZBXZBWKFQHLPMVMGYF ZBMVSYGKGTOLLJCBFKHHWFIVPPXPTVEJEBZBXHKNYKDYLIAKLLPJZFPVJAROJUOZZUWNZRRDZNYLGBHMNWUKJLSAXBUBWJZYCMVLYBCQJLBORO BDSZGHMCIASVUCVNDTGDALKYLTOMJK

C:\ProgramData\KLIZUSIQEN.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.696703751818505
Encrypted:	false
SSDEEP:	24:b16WkAmEUwq/rBFGdG3NQGsu7DYh3NTgfAtxoLxLP/VEmcM:hkAYzzbG4NPsuYh3N0fAjaxLnl
MD5:	19255ED5D4F37A096C105CEF82D0F5C0
SHA1:	96C5E995A91C8BC479E1C2ADB32C7E022EB8FAC7
SHA-256:	A0E9C6A5B14DB7AB22994C5017930720299F4492CE99D95A07BEB46BF2BAE7E8
SHA-512:	CDCD7E54677DE3BCE65BD80C855DE9684517F931ECA4D17E984C1D02E5E5CE9B50582ECCFA43F71A4F0A4E1743D74FCF3D588424AF519BFAE628EA49082C6 E68
Malicious:	false

Preview:	KLIZUSIQENZWQAFPHPIZMRSSYSYIINGOAPFQHPCFTPTNYLSNMTRTDZSWEBKDRHIUFOFGWKTHENHAQWTYTMOJNOWPWJAPIZKOPDMUAKVTHXYWDB HBVWDTBCFVXJHDCUGTPASHSDSKUVYPRPPUXKURDNZYJENQKRHCARIUAOIAFRFWGQDXOAPXUJAUWRVEASXCVARWJMIPINSQDPGOWLRMNRCAEZGZ IYDWBEWCOJWHLMOUROGZKCFGXDKPHAJADQCYUZYSYXQOIEGZIJWZLUJEKZUASKHQOGVFGVEXIQTENJDEKERNBPZGKNXWYZVXDDAYNSFBZAKWCE EYDSJONDKOYOBSAVICMHPZZRHRLNYDOIDQNYLXFDCCUOIJANPQCOIJDXFLDMIBVHBYSNYGAVWTHYCIPBRPTWSQXWXZZJBFNAUOMALKDRYIMJCR JXXQXCEREPQGNQHHOFEMEOXMSZEWOLTOLCOUCQNPRIPXUSVZNATFZKIJQZKGKTCYOMBXFTSXBXYIHMOONWWGRKPSNEMONASEFSVW NWIBXDSMEKQJIDCFPVMGAAUPBVOYAIKYQEFVSXOFTEMHNXVNMMENORLDYPZUSILNZRPHITCWDQMLEFZOEGPJDXQLBSIYRONLBYOSJVTEMBHNVX CMMRDVOAYSMNNRKRLBSQBIWIWHYUMBKTIYQTROZKTGZZMEFWINSQAXMWWLRRSPXAQZURXOTMUHPNLOUWMXRQSGXIAQILQCZUUTRJ ZVRNLBSHADNHZSDOQIYIZCEZHFRITTHSZOSBZGNCQVHXSFZJCEVSJCZZYTCFXLNBKMTPXYHPDXMMMXHUAAQWYYFHMKXWZBXZBWKFQHLPMVMGYF ZBMVSYGKGTOLLJCBFKHHWFIVPPXPTVEJEBZBXHKNYKDYLIAKLLPJZFPVJAROJUOZZUWNZRRDZNYLGBHMNWUKJLSAXBUBWJZYCMVLYBCQJLBORO BDSZGHMCIASVUCVNDTGDALKYLTOMJK

C:\ProgramData\QCOILOQIKC.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697125102277996
Encrypted:	false
SSDEEP:	24:uVOXLU7xwK58ZsokCVVZGi4eW0ZFJVPNR+x:c7xR8mwGi4sbv+x
MD5:	207485EFCE70435971C31586A1E4CF97
SHA1:	245A410AEB767B099944A8E81F75FC9A4B270DFB
SHA-256:	BF45E8FD687DC0E63FD40F32F2279152430579EDE044C3BB0852A1AC460D4B09
SHA-512:	A7F01CBBAFE9EA12B4C820F5E1A107D4C6FBD57CFF41C4AC679485F2B7DAFA4E9148AF830A39A083EC866E988A8E279FEB39D5EB58593E75D22253BED4DEF A19
Malicious:	false
Preview:	QCOILOQIKCUYMAHQLCLSCUGPPLVTJEARXPXBWFLOFHRVUSXLZVWHDQNKEMGPPQAGBLIPFAECDZNKKHITNQJASUXZAYMZIQCEHAQMCVZBMFUDBN QEKCBNCGMUWXDJLMJKVRKYBLRGNWGBGEVIGVROENGUXKJERNJSJJEMVLDKUXDFUWUPQNWUYRIEPUFOQKPDSZXXCKNQVBEAVMDMBR ZSWYPCNALGHTDFWFNDXKSHXCRLYPVFVYVEOFRHUFZZGNIXSJQCPZGONOYWWUQLBEBGALPOGZBXJUYXTHWOKWNKJYPSELALXQYIKAHXCELBTKSQ FTNYWBHRPQFULPLOCWEQAXEQNXOBIQOYFSEEZWHQQLZPBQOUMVZIMRWRLSPDKEBXSTPZLAGVYIORHCDBXTBHYOFKACXVGKKSIFHPOLDOQGIDQP FPVIPGUCGUCQLFFBYAGFJYFOMBUMPAHPQLDOHYAMKEGSDPXEYBQJUOWZOPFYRTLYUYDJHPLVEXBXUGVUEYIBUTUABUIHROFHZMLJUXWGZILWRH VKGOSZXXCIWGRGUZQDKQMTXRRWHDLJPPIRDALEIAYYTEEONIAELEISEOGNTDSALVOZDMFPLJSJMKJYMWGSKCTXHTLYYFJSXNZMDELRTJBNXSGA OEPKCPEEPFZKCAATOWHUWGQAEQNZHTKQEUCFRXVJWOGAEQDIWARNNFKCHEDRWTKEOVTURBKPDMQPPDCJGTYCTIRELHGRIRLWAPLC EHANSMGDZZYCXXDOTQVOSDZJAEBOTEVLSMHXCOWDPVQPSGDIDBAWUTDPIYPVBFSUMFBUYOPRXLECFHENURLSLKGPFWXDUFYOAKNTFKOYFUZEKL RZOLPYKMCKVZOIMDCCSGPQNCQXJOTJDKUQEPVHFKRSGZYJBNUHVTOEMNLTDXGZHTDQFQZCOULTNVZRAVLOIOVIKUTWPYLRJUCUDMYVYFWSBLJT JKMSJEIJXWYNPKGTYLKDAEVBUQUIJX

C:\ProgramData\QCOILOQIKC.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697125102277996
Encrypted:	false
SSDEEP:	24:uVOXLU7xwK58ZsokCVVZGi4eW0ZFJVPNR+x:c7xR8mwGi4sbv+x
MD5:	207485EFCE70435971C31586A1E4CF97
SHA1:	245A410AEB767B099944A8E81F75FC9A4B270DFB
SHA-256:	BF45E8FD687DC0E63FD40F32F2279152430579EDE044C3BB0852A1AC460D4B09
SHA-512:	A7F01CBBAFE9EA12B4C820F5E1A107D4C6FBD57CFF41C4AC679485F2B7DAFA4E9148AF830A39A083EC866E988A8E279FEB39D5EB58593E75D22253BED4DEF A19
Malicious:	false
Preview:	QCOILOQIKCUYMAHQLCLSCUGPPLVTJEARXPXBWFLOFHRVUSXLZVWHDQNKEMGPPQAGBLIPFAECDZNKKHITNQJASUXZAYMZIQCEHAQMCVZBMFUDBN QEKCBNCGMUWXDJLMJKVRKYBLRGNWGBGEVIGVROENGUXKJERNJSJJEMVLDKUXDFUWUPQNWUYRIEPUFOQKPDSZXXCKNQVBEAVMDMBR ZSWYPCNALGHTDFWFNDXKSHXCRLYPVFVYVEOFRHUFZZGNIXSJQCPZGONOYWWUQLBEBGALPOGZBXJUYXTHWOKWNKJYPSELALXQYIKAHXCELBTKSQ FTNYWBHRPQFULPLOCWEQAXEQNXOBIQOYFSEEZWHQQLZPBQOUMVZIMRWRLSPDKEBXSTPZLAGVYIORHCDBXTBHYOFKACXVGKKSIFHPOLDOQGIDQP FPVIPGUCGUCQLFFBYAGFJYFOMBUMPAHPQLDOHYAMKEGSDPXEYBQJUOWZOPFYRTLYUYDJHPLVEXBXUGVUEYIBUTUABUIHROFHZMLJUXWGZILWRH VKGOSZXXCIWGRGUZQDKQMTXRRWHDLJPPIRDALEIAYYTEEONIAELEISEOGNTDSALVOZDMFPLJSJMKJYMWGSKCTXHTLYYFJSXNZMDELRTJBNXSGA OEPKCPEEPFZKCAATOWHUWGQAEQNZHTKQEUCFRXVJWOGAEQDIWARNNFKCHEDRWTKEOVTURBKPDMQPPDCJGTYCTIRELHGRIRLWAPLC EHANSMGDZZYCXXDOTQVOSDZJAEBOTEVLSMHXCOWDPVQPSGDIDBAWUTDPIYPVBFSUMFBUYOPRXLECFHENURLSLKGPFWXDUFYOAKNTFKOYFUZEKL RZOLPYKMCKVZOIMDCCSGPQNCQXJOTJDKUQEPVHFKRSGZYJBNUHVTOEMNLTDXGZHTDQFQZCOULTNVZRAVLOIOVIKUTWPYLRJUCUDMYVYFWSBLJT JKMSJEIJXWYNPKGTYLKDAEVBUQUIJX

C:\ProgramData\SNIPGPPREP.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.701796197804446
Encrypted:	false

SSDEEP:	24:C1U2g6pCwYBq9+pGzEcrz023TZ9iFxwELi:2U2gCCm9drz0wTZsIEe
MD5:	C8350CE91F4E8E8B04269B5F3C6148DA
SHA1:	22D523A327EBAF8616488087E2DCE9DBD857F0CC
SHA-256:	1BE0B3682C4F3A3315465E66A2C7C357BB06225947C526B1B89A39D9D120AFBF
SHA-512:	C4891D35B6E895E4A9F4A785701EFFA4305AE88D09D309865F9312D95C296CB417916D8CBA461099E80F68C5AE5015A1172E60319256A453DE81445660F55806
Malicious:	false
Preview:	SNIPGPPREPVDSXKMBCQXEQRWSYOYKDGHPXSNVTYLWVPMUIXPKXDRFHMINIQBFZTPTVMTSZAWIXFLHCKJNAWKCQYMBHUKFDOIJBXXLUNVNMKEDO TTPPDLIAGSTXKJKMHVVGIGUNGKPTPDUEUVMGZRIBRMBHLZOZZIBTDOCDOASXCIFRVGCSENFOEARIYUEACCMVFPUDRRUHYQQFJBAWDGKHRWDHTG YUXKSSVSTFCVQOQGTKOBOMZZTKVYFLAXTKJMTUDSETBGCOOKYGPLGPNAFICZERONWJHOMIWLGEWSSANDAVRYRUWZSRNZFYKTMSQX LZZGTQKXVQLDKQIHEDADRTKYMYNBVWROSFBYUXYULCESFAKNPBXYOELAWZCZFAPVQWMMNLBQRIPMVDMMWGXGKDJNUJGGGBNSGWED DLRHGAAWJCYOEMVEHAYXYEHSKMWJPPHERNLXAGENBCUAZODRTUDIOUWNPZSHJGYOVHWQKWRAGGUMLCITTLAJXOXDUPFFLAHWLWPR QRAXSKOBHTXQNNGYHHVLBOEFTHAXTLKUGTNIYSDATIJHBUFTSGQHRXQQGXCBWVJIULNMYSMFYMPXRZOWMHYMZOLIBIYHPQRQJTZOMJZHKRTSWQ QVINGIZHWDLNCJKAMKHSMFOTUPQMESXHXMJSAXESVNVSKORQSXVCYCKNZKOFZFUKINTRLLEGXVQTQURFVKWLFRQZVQVBVOEMATWFLXFDJVWCYM PYCSJCUUGUCIPOPIVLEFNZCPNYAWTXOATSTYLECDEFJNQFYGVPQWTJBNAVWKGALRTACLENBODJOQDXMPOYCYEFXOOOOMCQXLRGDBUUVJNQAEBZ DSPDLPFIEOXRWSFCHXDUSBTSLEDLCZPOHIMIMQZMHHTMDFUUMKUAMBYNWWRQKDEXPPDWGKCNTWTFNHBMNDQIMVNFYWGALYORHHPU AXLDHMTGOKMMTAOCOVLGFIHZLZFADWMNNCWOLNJDSGFCWVDBYK

C:\ProgramData\TQDFJHPUIU.docx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697771666106845
Encrypted:	false
SSDEEP:	24:TwdgExX6lswcsA1Wo1+js3mQmFlw2UJh6QHssg9RGVQ8:T6KiV+KmQmFwhtMp9RGVH
MD5:	D910958AF930D9DCA27D8F529EC053D0
SHA1:	321478679C760C347743149A323469AD4BFEA87D
SHA-256:	C70010ABE33AC34A7DB2F84B5ECDEA5EF95D482B69138707C126D2C1C1B67F37
SHA-512:	0BCADFF480F8F0C7E5DDC316F678564A75785640F151ACA644CABE64AD10D0D4AD6156385A4B04DF9025C6ADCDB3787123EC21F57610F1A7FBC7727A12EB8A 00
Malicious:	false
Preview:	TQDFJHPUIUELSDZVLDSOEPJOAGZMFPGEGXRLLWCATKTXUFCCYBMLLTOAWXCBRXEASQCNMLCVLTUZVHIGECOSKDAKWRYISSWUBTJPNWVMOQIBOV CDGZBZLOBWHRRJWCIVVOOXQYXMXXZMUJFNAGIRMQEQNBGKVATBJCBUBSWVZNUBPOSGZZKDLPMWNJJYMXSJFTKODUAYUUUFMAXNGYJPXGZQGSVL QUGDVVRJNEOKUCNTIRLLCNKTYMTQNZJJKSKBSONPJUKRASZVNLIXIMVFHLBZMMQBRQMADRKDIUMEEGDUNISFUQIECDZCRHSRRYZPGKJVXJOWYF DCIFWRPIQIGFARPTXNAEOTZASGGBUAORTYTQKACAIMSIJTKMTNMLSJSOHBNKDCPBUROQGRJNZUWHAQAOIYBGRJZNQFPXFARCDCRYDEHQKZSBWQ RIZUALGAGONASBDAUUWWGWMIACXEKQGBFHNSVOMSMNKHUCCICMZPSQBAOJSAJLHYYTHCBOJYRGLPACKOYWSINXQWZTVPZZGDMLUE MLVMWGYQVWJXSKGMTZXFWDQTDCMARKFNKCUZOJJCUBDFZIQECIQSBZWGGGYXJKXBOJMSDVJPFGXNBLAVKQLERCTILRLNODWOHUHA HUKXKKYDMHZJUTFVHEQDYGBYCPPMSUVFTBPYSDWSPRWOOVOMFFXVHKXCQNSANIDGQLMMNSDROMFQDXTGDYVZZKZMXJGFRGTCUUWA EMNPZJJQANNDMULSUEIOQHQUZBJGBBFBYEITVHYSXFUDFMPLOAIHQGZLPYMHUKXYLKLKILTNDAXWVKITWAKIJERKCLMHSEKWBLLPKKZZWHXZMS HTTCPRPQUXXDNKWNYSNTNWEZAVSUMPTOQBTAMVGRIMPCIHLVZDKXOJHRUGCUCYCCGSKYZFHLNROAETESAVZHHZSEDGXUMPIWCICTRSGZRIRINH SZURTKUBQMVZLOYEFVZZTFCGUJKCBMMLKUJTDVWC

C:\ProgramData\ZIPXYXWIOY.xlsx

Process:	C:\Users\user\Desktop\un78exGoa4.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.697427014915338
Encrypted:	false
SSDEEP:	24:J87vGcgdreYqco0NFLg5elatTFj9qVUq2Z:J83gAYq8NFRtx7Z
MD5:	2D7ACA56B5F340F28DD1D2B46D700BA6
SHA1:	3966684FF029665614B8DC948349178FB9E8C078
SHA-256:	B227E5E45D28AC063349BC70CC01A3F6DB15C101432A8609E0202064F7E5936D
SHA-512:	D4BFC2BB839DAEBAE8C894A0B8EB2314D2BE0304C82EB89BE16D6C820874952534CE0D93AE62EEF3DD2BE8A4D1E828B883E50BD204D04624AB945119D2FAE 4F0
Malicious:	false
Preview:	ZIPXYXWIOYFFJDUIEBFLHIUBYNNMJGYPFQONGOLQHGMFRFYQGSVGNDSCQJYWDCIKWJWNYHFUEMJVEPAFIPAROVFAVARCOHESRJKUIUYDXNZOER BEQGHQNKYMVMEEMKKKEYXXPAKWYGCIXNFSVDOOEUTNGSDXMYEZKQTRDCZXZXIFSRMNAEPZWJKKYULUPGZCQORNOJBGAAOPLYNJCP FWSASJWTLALTQZLWOGFWQVOXGYBCMNEBDESHLNZZBETDIGNLTNPZEPEQAMYCNYWEKKQKDVZPNYLWAFZIPSSVNHOPUMIBTFXVVCNCPUSOKETVBD NZLCRKBRLGSHFSQLECHUOWGFFEMDWHASNSMAXKZZMDLZVQLADFBDUCCIJERQXKRXUCTKGDGKPESHHXUPKZSGNKOITMVITFCBELJVTCKENQCMCJ EDZJDQDSKAYFGQEYICXDUOIJRYIMVXRKNBYXQEHUHYSPGEDSJBOQNXHFTSSRTPOXDVFXEPQUGWNEAKZJOKYPEYKXMOMKTKOBVISHMUGELPJCXB YNEXOAWOXHSEELVSCFMZYAMOLTGIWURMTZTRNGMWQZBRQHAIXVJIAFPZGWJZIOQLOAXJSGKMZNZCAVJWFGUFMQWQICMPVNAYRUHA MQLWLJMBERSFPEZHMNVAZFQAJEGYJQOMQWFTQVXZYTDPYVGZZPSNSOJWWKZDRPZKGTXYSENWOIQFXDIRWPJEYALOOEYQPHOPKSIZFNHPOXOKST DVPNBSCDDKPOUVXMFBUNBMEUYGOSYMHMUNKKADTAEIUEMXYPOPMUVBHTBVKYAHHJXFUJPFZJZARAFLARBIWKXMNKXJLVBLJSZYYVIBZHROONQE NYZGGMMETTMOFHCCQNUHPDEUTVVGUDBCKVXVUMRWPGZIPPUXJEJQIEQWLBUQBUODMWPSBFOYIQZWMYWPHWSKTRCKCRXWZUOTDTDR LLUSSQZXZZEATFSHBUWQUYHDLRMVVWFCPAZNSBXA

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.486309125722837
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:	un78exGoa4.exe
File size:	297472
MD5:	84f304e30439cf1f837ed4f31c1fbb28
SHA1:	257518ece774da6ba53ca070121a206519f0c229
SHA256:	cb7f4e286a4a8fdfa525168591131d37019090d94040feb13c8078c4a7ae4b37
SHA512:	2fb76cd9feab5a1db8ed728f9c9a158eac97f658adb962d77bd27b1055e8ca48b2b14724871b5964d181f42bb74a51b36269a18061078f57f17fae158c81ba3e
SSDEEP:	3072:Ad9jDaSlXbBp6mLpIlYUEjOyv+L5bIWw7az/5QtGvAUd:qDakXmmL0CuLhIPtI
TLSH:	DB542A0396E2FC50ED668A729E2FC6EC779EF5508E19775A2118AE1F0C702B2D173712
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Richb.....PE..L.....b.....

File Icon

Icon Hash:	4d45454d6545691d

Static PE Info

General

Entrypoint:	0x404e79
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6296E609 [Wed Jun 1 04:07:37 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:	d683fcb523ac92743f5db043ced73806

Entrypoint Preview

Instruction
call 00007F87B4AF1963h
jmp 00007F87B4AECFFDh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F87B4AED1A6h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F87B4AED1D0h
test ecx, 00000003h
jne 00007F87B4AED171h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F87B4AED16Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F87B4AED1B4h
test ah, ah
je 00007F87B4AED1A6h
test eax, 00FF0000h
je 00007F87B4AED195h
test eax, FF000000h
je 00007F87B4AED184h
jmp 00007F87B4AED14Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h

Instruction
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] 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	0x28318	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26f000	0x1b4b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x28b000	0xdfc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	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	0x3190	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d8	.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	0x27dd4	0x27e00	False	0.7861542417711599	data	7.580309216292186	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x29000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x26f000	0x1b4b0	0x1b600	False	0.3575110587899543	data	4.288893910573521	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x28b000	0x334e	0x3400	False	0.22723858173076922	data	2.531131235614748	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x284b78	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_CURSOR	0x285a20	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_CURSOR	0x2862c8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_CURSOR	0x286860	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_CURSOR	0x287708	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x287fb0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_CURSOR	0x288548	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x288678	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0		
RT_ICON	0x26f910	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x26ffd8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x272580	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x272a18	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2738c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x274168	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x2746d0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x276c78	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x277d20	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x2786a8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x278b78	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x279a20	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x27a2c8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x27a990	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x27aef8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x27d4a0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x27e548	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x27ea18	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x27f8c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x280168	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x2806d0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x282c78	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x283d20	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x2846a8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x288980	0x6fa	data		
RT_STRING	0x289080	0x6a8	data		
RT_STRING	0x289728	0x4b8	data		
RT_STRING	0x289be0	0x1da	data		
RT_STRING	0x289dc0	0x6ec	data		
RT_GROUP_CURSOR	0x286830	0x30	data		
RT_GROUP_CURSOR	0x288518	0x30	data		
RT_GROUP_CURSOR	0x288728	0x22	data		
RT_GROUP_ICON	0x284b10	0x68	data		
RT_GROUP_ICON	0x27e9b0	0x68	data		
RT_GROUP_ICON	0x2729e8	0x30	data		
RT_GROUP_ICON	0x278b10	0x68	data		
RT_VERSION	0x288750	0x22c	data		

Imports

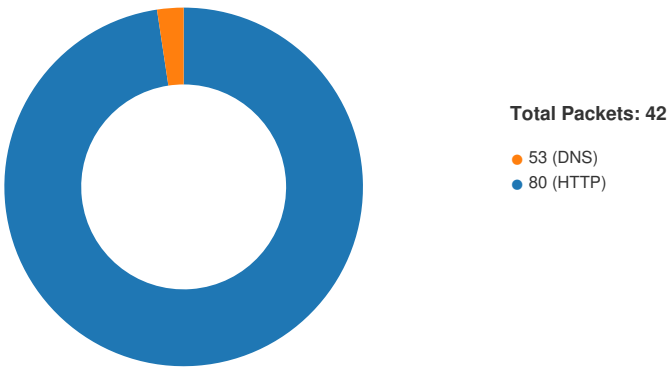
DLL	Import
KERNEL32.dll	AddConsoleAliasW, SleepEx, GetModuleHandleW, GetTickCount, IsBadReadPtr, GetConsoleAliasesLengthA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, GetNamedPipeInfo, MulDiv, GetModuleFileNameW, CreateActCtxA, ReplaceFileA, GetStringTypeExA, CreateJobObjectA, GetProfileIntA, GetStdHandle, GetLogicalDriveStringsA, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, CancelWaitableTimer, GetLongPathNameA, VirtualAlloc, EnterCriticalSection, _hwrite, LoadLibraryA, OpenMutexA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, GetProcessShutdownParameters, CreateMutexA, GetFileAttributesExW, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, WaitForSingleObject, GetConsoleAliasA, FindResourceW, GetCommState, AttachConsole, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.58.8.8.8.8653235 32023883 05/28/23-09:29:39.799894	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	65323	53	192.168.2.5	8.8.8.8
192.168.2.5193.106.175.21549712802044244 05/28/23-09:29:40.725978	TCP	2044244	ET TROJAN Win32/Stealc Requesting browsers Config from C2	49712	80	192.168.2.5	193.106.175.215
192.168.2.5193.106.175.21549713802044246 05/28/23-09:29:40.856625	TCP	2044246	ET TROJAN Win32/Stealc Requesting plugins Config from C2	49713	80	192.168.2.5	193.106.175.215
192.168.2.5193.106.175.21549711802044243 05/28/23-09:29:40.524393	TCP	2044243	ET TROJAN [SEKOIA.IO] Win32/Stealc C2 Check-in	49711	80	192.168.2.5	193.106.175.215

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 09:29:40.457489967 CEST	49711	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.513911963 CEST	80	49711	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.514128923 CEST	49711	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.524393082 CEST	49711	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.625119925 CEST	80	49711	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.654975891 CEST	80	49711	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.655211926 CEST	49711	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.655419111 CEST	49711	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.663994074 CEST	49712	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.711527109 CEST	80	49711	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.724783897 CEST	80	49712	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.725493908 CEST	49712	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.725977898 CEST	49712	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.796806097 CEST	80	49712	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.796840906 CEST	80	49712	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.797013044 CEST	49712	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.797375917 CEST	49712	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.799499035 CEST	49713	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.855994940 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.856226921 CEST	49713	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.856625080 CEST	49713	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.857398987 CEST	80	49712	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.922844887 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.922888041 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.922908068 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.922950983 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.922969103 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.922985077 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:40.923016071 CEST	49713	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.923089981 CEST	49713	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.924632072 CEST	49713	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:40.980309963 CEST	80	49713	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.151081085 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.211818933 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.212049007 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.213331938 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.213427067 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.273912907 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.273943901 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.273962975 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.274038076 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.274054050 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.274143934 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.274194002 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.274224997 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.274718046 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.274919987 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.275135040 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.275156021 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.334770918 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.334793091 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.334806919 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.334884882 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.335308075 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.392819881 CEST	80	49714	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.393085003 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.397425890 CEST	49714	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.407670021 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.457518101 CEST	80	49714	193.106.175.215	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 09:29:41.471628904 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.471885920 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.472238064 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.542838097 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.542870998 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.542895079 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.542913914 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.543057919 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543117046 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543560982 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.543591976 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.543622017 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543627024 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.543649912 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543674946 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543821096 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.543842077 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.543867111 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543886900 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.543984890 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.544030905 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.606288910 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606348991 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606369019 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606389999 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606410980 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606431007 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606448889 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606468916 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606513977 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.606549025 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606568098 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.606594086 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.606745958 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606767893 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606786966 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606801033 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.606808901 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606829882 CEST	80	49715	193.106.175.215	192.168.2.5
May 28, 2023 09:29:41.606832027 CEST	49715	80	192.168.2.5	193.106.175.215
May 28, 2023 09:29:41.606879950 CEST	49715	80	192.168.2.5	193.106.175.215

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 09:29:39.799894094 CEST	65323	53	192.168.2.5	8.8.8.8
May 28, 2023 09:29:40.445825100 CEST	53	65323	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 28, 2023 09:29:39.799894094 CEST	192.168.2.5	8.8.8.8	0x68d5	Standard query (0)	ronaldlitt.top	A (IP address)	IN (0x0001)	false

DNS Answers

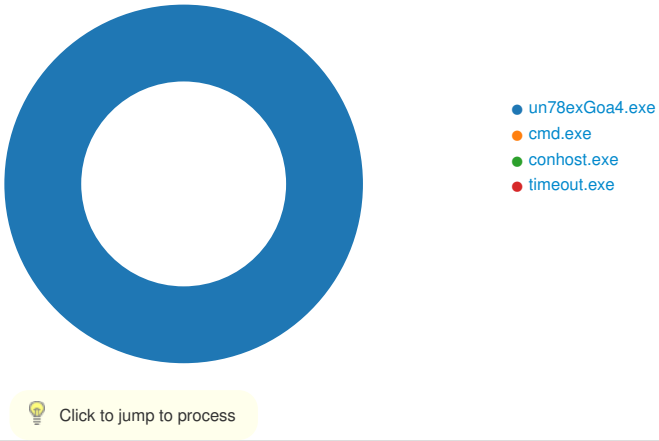
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 28, 2023 09:29:40.445825100 CEST	8.8.8.8	192.168.2.5	0x68d5	No error (0)	ronaldlitt.top		193.106.175.215	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- ronaldlitt.top

Statistics

Behavior



System Behavior

Analysis Process: un78exGoa4.exe PID: 7132, Parent PID: 3324

General

Target ID:	0
Start time:	09:29:38
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\un78exGoa4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\un78exGoa4.exe
Imagebase:	0x400000
File size:	297472 bytes
MD5 hash:	84F304E30439CF1F837ED4F31C1FBB28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.421505626.0000000002410000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Stealc, Description: Yara detected Stealc, Source: 00000000.00000002.421100115.00000000006B5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.421165078.00000000006D9000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.421176016.0000000000734000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6808**, Parent PID: **7132**

General

Target ID:	3
Start time:	09:29:53
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\Desktop\un78exGoa4.exe" & del "C:\ProgramData*.dll"" & exit
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6812**, Parent PID: **6808**

General

Target ID:	4
Start time:	09:29:53
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: **7112**, Parent PID: **6808**

General

Target ID:	5
Start time:	09:29:54
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0x60000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true

Has administrator privileges:	true
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly