ID: 682150
Sample Name: 5tLwjRFzAW.exe
Cookbook: default.jbs
Time: 06:51:09
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report 5tLwjRFzAW.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Djvu 4
Threatname: SmokeLoader 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
Compliance 7
Networking 7
Key, Mouse, Clipboard, Microphone and Screen Capturing 7
Spam, unwanted Advertisements and Ransom Demands 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 8
Anti Debugging 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 12
Domains 12
URLs 12
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 14
World Map of Contacted IPs 15
Public IPs 15
General Information 16
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
C:\Users\user\AppData\LocalLow\8EK4CZ3qdU65 17
C:\Users\user\AppData\LocalLow\freebl3.dll 17
C:\Users\user\AppData\LocalLow\jId0qk9WVSf3 18
C:\Users\user\AppData\LocalLow\k0MUzhlF0pI7 18
C:\Users\user\AppData\LocalLow\mozglue.dll 18
C:\Users\user\AppData\LocalLow\msvcp140.dll 19
C:\Users\user\AppData\LocalLow\nss3.dll 19
C:\Users\user\AppData\LocalLow\softokn3.dll 19
C:\Users\user\AppData\LocalLow\sqlite3.dll 20
C:\Users\user\AppData\LocalLow\vcruntime140.dll 20
C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X 20
C:\Users\user\AppData\LocalLow\y79VUKJAS8XH 21
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\geo[1].json 21
C:\Users\user\AppData\Local\Temp\28E9.exe 21
C:\Users\user\AppData\Local\Temp\33.exe 22
C:\Users\user\AppData\Local\Temp\A658.exe 22
C:\Users\user\AppData\Local\Temp\D0E3.dll 22

C:\Users\user\AppData\Local\Temp\E69F.exe 23
C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe 23
C:\Users\user\AppData\Roaming\ftvuhuw 23
C:\Users\user\AppData\Roaming\irbiwat 24
C:\Users\user\AppData\Roaming\irbiwat:Zone.Identifier 24
Static File Info 24
General 24
File Icon 25
Static PE Info 25
General 25
Entrypoint Preview 25
Rich Headers 27
Data Directories 27
Sections 27
Resources 27
Imports 28
Possible Origin 28
Network Behavior 29
Snort IDS Alerts 29
TCP Packets 29
DNS Queries 30
DNS Answers 31
HTTP Request Dependency Graph 37
Statistics 38
Behavior 38
System Behavior 39
Analysis Process: 5tLwjRFzAW.exePID: 5320, Parent PID: 5328 39
General 39
Analysis Process: explorer.exePID: 3968, Parent PID: 5320 39
General 39
File Activities 40
Analysis Process: irbiwatPID: 4748, Parent PID: 848 40
General 40
Analysis Process: 28E9.exePID: 4384, Parent PID: 3968 40
General 40
File Activities 41
File Created 41
File Deleted 43
File Written 43
File Read 48
Analysis Process: A658.exePID: 5244, Parent PID: 3968 48
General 48
Analysis Process: A658.exePID: 4164, Parent PID: 5244 49
General 49
File Activities 49
Registry Activities 50
Analysis Process: regsvr32.exePID: 5148, Parent PID: 3968 50
General 50
File Activities 50
File Read 50
Analysis Process: regsvr32.exePID: 2360, Parent PID: 5148 50
General 50
Analysis Process: icacls.exePID: 3980, Parent PID: 4164 50
General 50
File Activities 51
File Written 51
Analysis Process: A658.exePID: 4276, Parent PID: 848 51
General 51
Analysis Process: E69F.exePID: 1436, Parent PID: 3968 51
General 51
File Activities 52
Analysis Process: A658.exePID: 2196, Parent PID: 4164 52
General 52
Analysis Process: 33.exePID: 4708, Parent PID: 3968 52
General 52
Disassembly 52

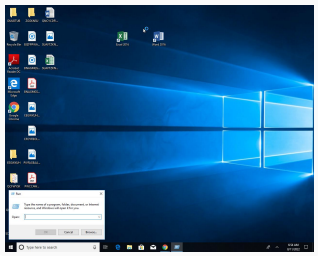
Windows Analysis Report

5tLwjRFzAW.exe

Overview

General Information

Sample Name:	5tLwjRFzAW.exe
Analysis ID:	682150
MD5:	203eaeca3c89f5…
SHA1:	0d872229972ec1..
SHA256:	c4624241f0890d..
Tags:	exe Formbook
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

CryptOne, Djvu, Raccoon Stealer v2, SmokeLoader

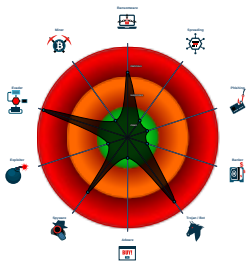
Score: 100

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

Signatures

- Detected unpacking (overwrites its o…
- Yara detected CryptOne packer
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Yara detected Raccoon Stealer v2
- Benign windows process drops PE f…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware

Classification



Process Tree

- **System is w10x64**
- 5tLwjRFzAW.exe (PID: 5320 cmdline: "C:\Users\user\Desktop\5tLwjRFzAW.exe" MD5: 203EAECA3C89F5CA7DC82668C4883B5A)
  - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - 28E9.exe (PID: 4384 cmdline: C:\Users\user\AppData\Local\Temp\28E9.exe MD5: FEEEAA3A0D766A6C52B71C23F796912D)
    - A658.exe (PID: 5244 cmdline: C:\Users\user\AppData\Local\Temp\A658.exe MD5: 1FDD74F600A1E3A9CFA80026CF54BC59)
      - A658.exe (PID: 4164 cmdline: C:\Users\user\AppData\Local\Temp\A658.exe MD5: 1FDD74F600A1E3A9CFA80026CF54BC59)
        - icacls.exe (PID: 3980 cmdline: icacls "C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415" /deny *S-1-1-0:(OI)(CI)(DE,DC) MD5: FF0D1D4317A44C951240FAE75075D501)
        - A658.exe (PID: 2196 cmdline: "C:\Users\user\AppData\Local\Temp\A658.exe" --Admin IsNotAutoStart IsNotTask MD5: 1FDD74F600A1E3A9CFA80026CF54BC59)
    - regsvr32.exe (PID: 5148 cmdline: regsvr32 /s C:\Users\user\AppData\Local\Temp\D0E3.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 2360 cmdline: /s C:\Users\user\AppData\Local\Temp\D0E3.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - E69F.exe (PID: 1436 cmdline: C:\Users\user\AppData\Local\Temp\E69F.exe MD5: 681D98300C552B8C470466D9E8328C8A)
    - 33.exe (PID: 4708 cmdline: C:\Users\user\AppData\Local\Temp\33.exe MD5: C9143FA5E2792724172980E5ACC312F0)
- irbiwat (PID: 4748 cmdline: C:\Users\user\AppData\Roaming\irbiwat MD5: 203EAECA3C89F5CA7DC82668C4883B5A)
- A658.exe (PID: 4276 cmdline: C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe --Task MD5: 1FDD74F600A1E3A9CFA80026CF54BC59)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://rgyui.top/dl/build2.exe",
    "http://acacaca.org/files/1/build3.exe"
  ],
  "C2 url": "http://acacaca.org/lancer/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-HZpuxNJt6L\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-
```

```
mail:\r\nsupport@bestyourmail.ch\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0539Jhyjd",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
\\\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwnRiilBAjbjg+cgYwCXm\\\\nLaNP5QQF5jdC1TW22Z8o0zYVtbrZekiKKm\\/dvjAJtmNxSSwAQztfiDKlgG8Ofj5b\\\\naSCJa8IVa2XFO\\/Rqe9VkZPw\\/7TKiloMMwH3cSLe\\/y4keVXUiXlBOt4U6IeHLB97Y\\\\nQ9bnyf17R+g5w+MHditFYY5TCx0N2kjHjEXYKQ2jf\\/qPj60AveoVelBM7u1xEZt8\\\\nLLlkGS2MUE60Z7ZhS2zk5u2n5dFYwPW2oQTSSoeQxiiSY0IPHYAHk5hs3DoVfnE9\\\\n1Bo1oFeukX\\/4x5dzEqszXdLdVJXivjFzGcxQ3ZAOOkKu+6\\/+kHiS18x59NtWbYXT\\\\nMwIDAQAB\\\\n-----END PUBLIC KEY-----"
}
```

Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://susuerulianita1.net/",
    "http://nikogminut88.at/",
    "http://cucumbetuturel4.com/",
    "http://lilisjjoer44.com/",
    "http://mini55tunul.com/",
    "http://limo00ruling.org/"
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.343161421.00000000040E0000.00000040.00001000.00020000.00000000.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
00000014.00000002.418605685.00000000004CC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
0000001F.00000002.502148462.0000000004CD0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_CryptOne	Yara detected CryptOne packer	Joe Security	
00000014.00000003.397574395.00000000004CC000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
00000023.00000003.479074188.0000000000572000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

Click to see the 56 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
20.3.28E9.exe.4d2d13.14.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
20.3.28E9.exe.4d2d13.11.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
20.3.28E9.exe.4d2d13.1.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
20.3.28E9.exe.4d2d13.20.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	
20.3.28E9.exe.4d2d13.11.raw.unpack	JoeSecurity_RaccoonV2	Yara detected Raccoon Stealer v2	Joe Security	

Click to see the 78 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Win32/RecordBreaker CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 45.138.74.104

Timestamp:	192.168.2.345.138.74.10449759802036934 08/11/22-06:53:10.741012
SID:	2036934

Source Port:	49759
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response - Source IP: 45.138.74.104 - Destination IP: 192.168.2.3	−
Timestamp:	45.138.74.104192.168.2.380497592036955 08/11/22-06:53:11.296973
SID:	2036955
Source Port:	80
Destination Port:	49759
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Compliance

- Detected unpacking (overwrites its own PE header)

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands

- Yara detected Djvu Ransomware

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

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information

Yara detected CryptOne packer

Yara detected SmokeLoader

Yara detected Raccoon Stealer v2

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

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality

Yara detected CryptOne packer

Yara detected SmokeLoader

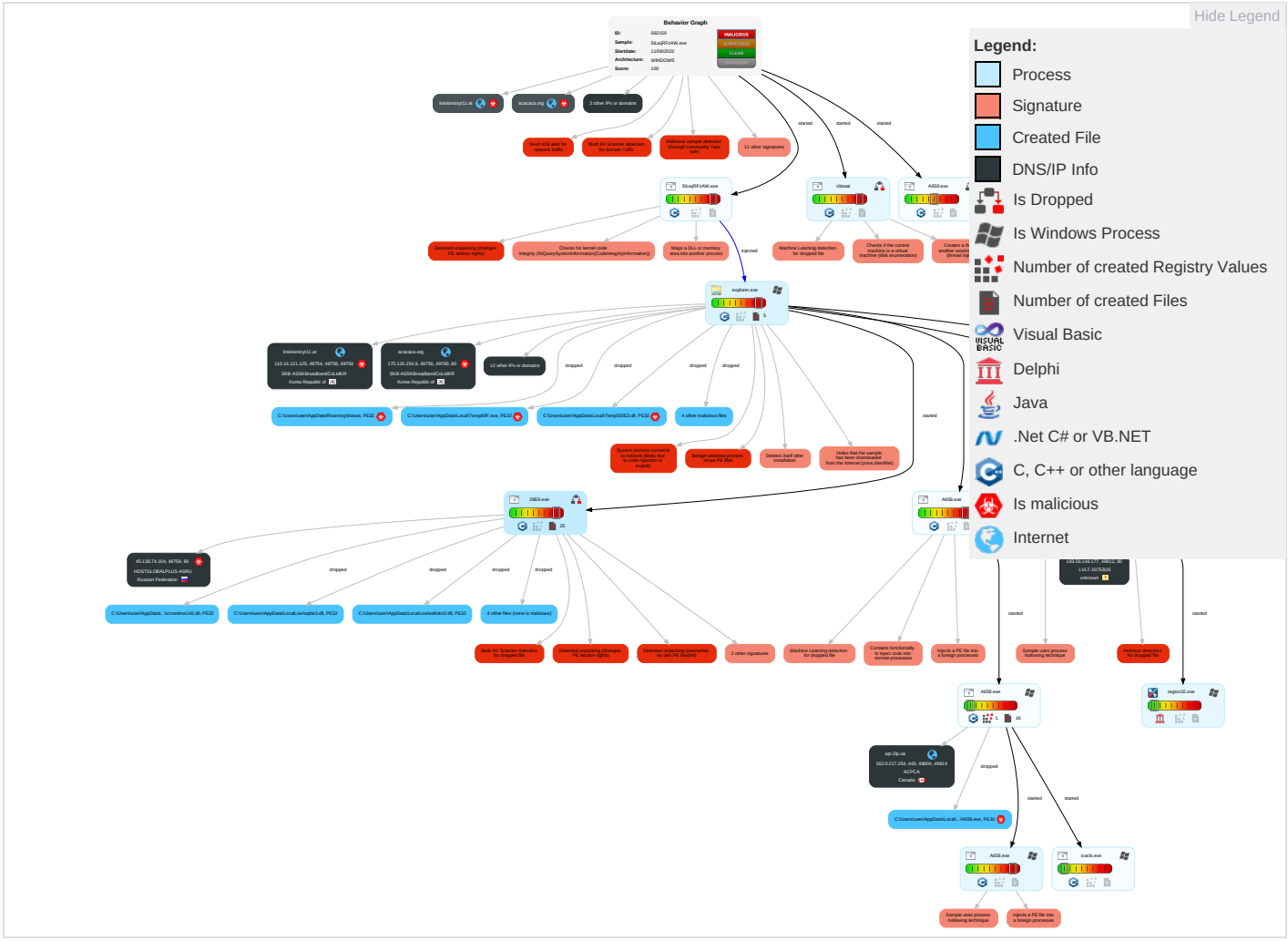
Yara detected Raccoon Stealer v2

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 Registry Run Keys / Startup Folder	6 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	2 2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	1 Services File Permissions Weakness	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	Security Account Manager	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	2 Command and Scripting Interpreter	Logon Script (Mac)	1 Services File Permissions Weakness	2 2 Software Packing	NTDS	3 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Query Registry	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	4 1 1 Security Software 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	1 1 Masquerading	DCSync	1 2 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Virtualization/Sandbox Evasion	Proc Filesystem	1 3 Process 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)	6 1 2 Process Injection	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Regsvr32	Input Capture	1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Services File Permissions Weakness	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

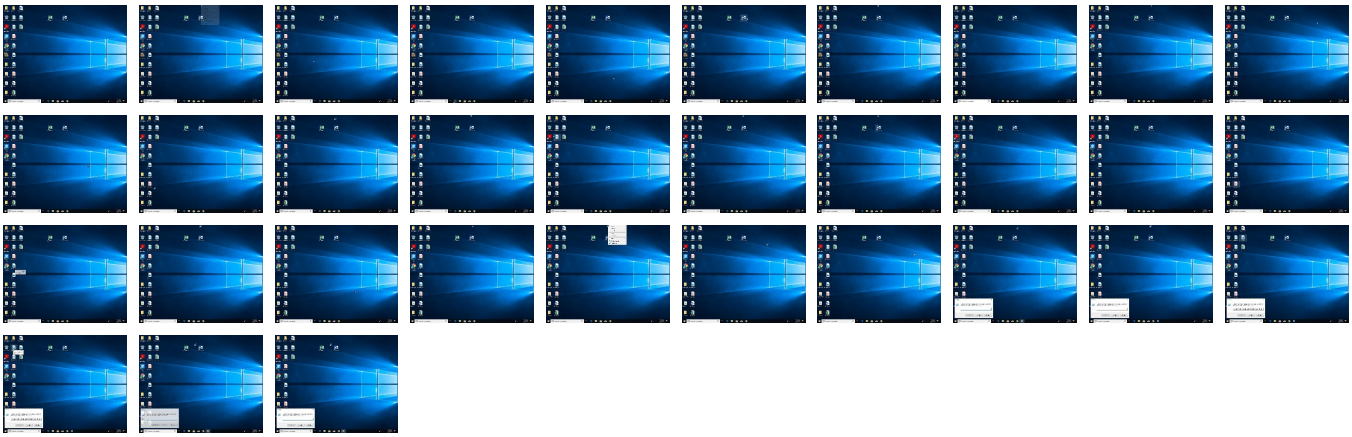
Behavior Graph



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
5tLwjRFzAW.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\E69F.exe	100%	Avira	TR/AD.RaccoonSteal.muash	
C:\Users\user\AppData\Local\Temp\D0E3.dll	100%	Avira	HEUR/AGEN.1233360	
C:\Users\user\AppData\Local\Temp\28E9.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\irbiwat	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A658.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D0E3.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\msvcp140.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\nss3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\28E9.exe	81%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Local\Temp\33.exe	21%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\33.exe	22%	ReversingLabs	Win32.Trojan.Zusy	
C:\Users\user\AppData\Local\Temp\A658.exe	47%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\A658.exe	56%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.2.regsvr32.exe.4df0000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
40.3.33.exe.1240000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.irbiwat.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.5tLwjRFzAW.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.regsvr32.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1232827		Download File
17.2.irbiwat.40e0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.5tLwjRFzAW.exe.2680e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.regsvr32.exe.4f10000.3.unpack	100%	Avira	HEUR/AGEN.1249928		Download File
20.2.28E9.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.3.irbiwat.40f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.A658.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
0.3.5tLwjRFzAW.exe.2690000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.regsvr32.exe.4cd0184.1.unpack	100%	Avira	TR/Kazy.4159236		Download File
40.2.33.exe.b9f8d0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
monsutiur4.com	18%	Virustotal		Browse
rgyui.top	22%	Virustotal		Browse
linislominyt11.at	16%	Virustotal		Browse
acacaca.org	18%	Virustotal		Browse
moroitomo4.net	15%	Virustotal		Browse
cucumbetuturel4.com	16%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://193.56.146.177/M	0%	Avira URL Cloud	safe	
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1wD	0%	Avira URL Cloud	safe	
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02.	0%	Avira URL Cloud	safe	
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02PowerShell	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02&	0%	Avira URL Cloud	safe	
http://www.opera.com0	0%	Avira URL Cloud	safe	
http://limo00ruling.org/	100%	URL Reputation	malware	
http://acacaca.org/lancer/get.php	100%	Avira URL Cloud	malware	
http://45.138.74.104/	0%	Avira URL Cloud	safe	
http://85.192.63.46/f/1.exe	100%	Avira URL Cloud	malware	
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02	0%	Avira URL Cloud	safe	
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1	0%	Avira URL Cloud	safe	
http://lilisjjoer44.com/	0%	URL Reputation	safe	
http://susuerulianita1.net/	100%	URL Reputation	malware	
http://linislominyt11.at/	100%	URL Reputation	malware	
http://mini55tunul.com/	0%	URL Reputation	safe	
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1xD	0%	Avira URL Cloud	safe	
http://62.204.41.178/newfile.exe	100%	Avira URL Cloud	malware	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	
http://193.56.146.177/	0%	Avira URL Cloud	safe	
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1$D	0%	Avira URL Cloud	safe	
http://https://mozilla.org0	0%	URL Reputation	safe	
http://nikogminut88.at/	100%	URL Reputation	malware	
http://acacaca.org/lancer/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C	100%	Avira URL Cloud	malware	
http://cucumbetuturel4.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
monsutiur4.com	185.237.206.60	true	true	• 18%, Virustotal, Browse	unknown
rgyui.top	190.140.74.43	true	false	• 22%, Virustotal, Browse	unknown
api.2ip.ua	162.0.217.254	true	false		high
linislominyt11.at	110.14.121.125	true	true	• 16%, Virustotal, Browse	unknown
acacaca.org	175.120.254.9	true	true	• 18%, Virustotal, Browse	unknown
moroitomo4.net	unknown	unknown	true	• 15%, Virustotal, Browse	unknown
cucumbetuturel4.com	unknown	unknown	true	• 16%, Virustotal, Browse	unknown
nusurionuy5ff.at	unknown	unknown	true		unknown
susuerulianita1.net	unknown	unknown	true		unknown
nunuslushau.com	unknown	unknown	true		unknown

Contacted URLs

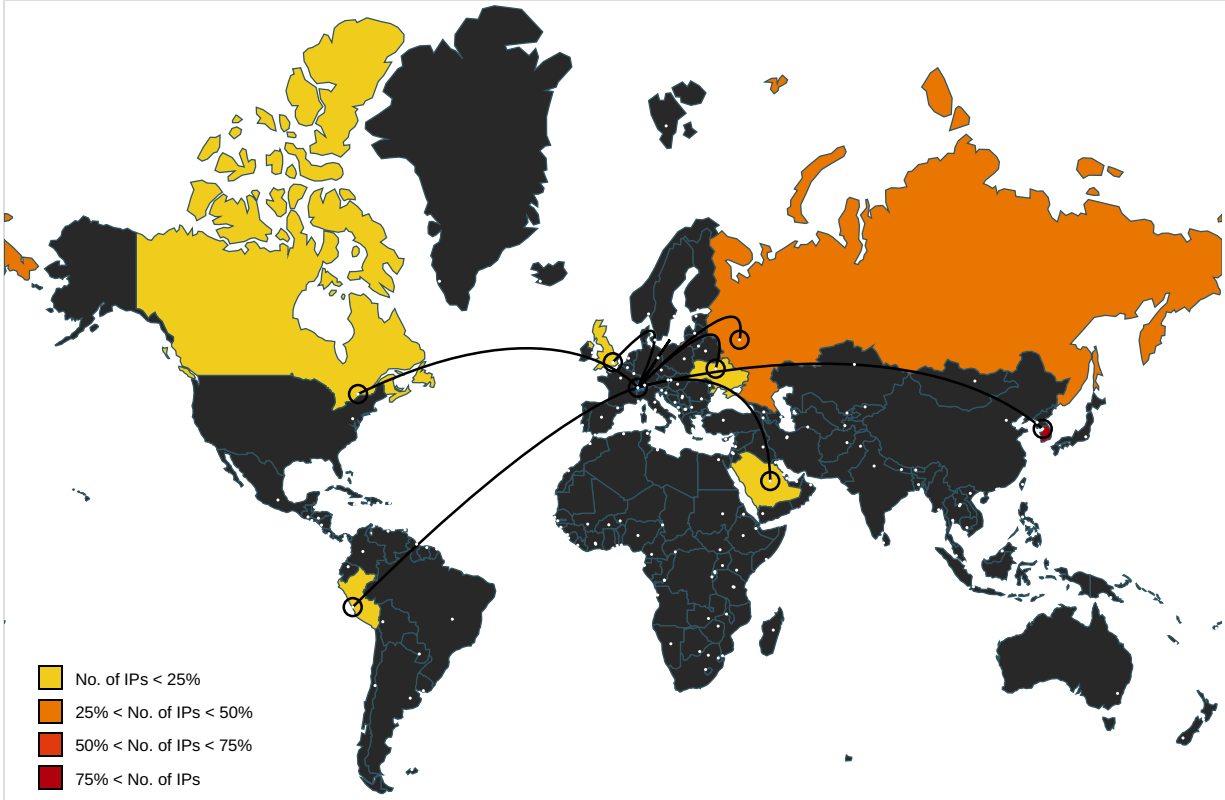
Name	Malicious	Antivirus Detection	Reputation
http://limo00ruling.org/	true	• URL Reputation: malware	unknown
http://acacaca.org/lancer/get.php	true	• Avira URL Cloud: malware	unknown
http://45.138.74.104/	true	• Avira URL Cloud: safe	unknown
http://85.192.63.46/f/1.exe	true	• Avira URL Cloud: malware	unknown
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02	false	• Avira URL Cloud: safe	unknown
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1	true	• Avira URL Cloud: safe	unknown
http://lilisjjoer44.com/	true	• URL Reputation: safe	unknown
http://susuerulianita1.net/	true	• URL Reputation: malware	unknown
http://linislominyt11.at/	true	• URL Reputation: malware	unknown
http://mini55tunul.com/	true	• URL Reputation: safe	unknown
http://62.204.41.178/newfile.exe	true	• Avira URL Cloud: malware	unknown
http://193.56.146.177/	false	• Avira URL Cloud: safe	unknown
http://nikogminut88.at/	true	• URL Reputation: malware	unknown
http://acacaca.org/lancer/get.php?pid=F4B58C92E14ED1DB6A495C4F0112806C	true	• Avira URL Cloud: malware	unknown
http://cucumbetuturel4.com/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.2ip.ua/-J	A658.exe, 0000001C.00000003.460852249.000000000087C000.00000004.00000020.00020000.00000000.sdmp, A658.exe, 0000001C.00000002.495884561.0000000000837000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	28E9.exe, 00000014.00000003.397412783.000000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.20.dr	false		high
http://193.56.146.177/M	E69F.exe, 00000023.00000003.478816889.000000000054A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	28E9.exe, 00000014.00000003.397412783.000000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1wD	28E9.exe, 00000014.00000002.419440478.000000000571000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.2ip.ua/	A658.exe, 0000001C.00000003.460852249.000000000087C000.00000004.00000020.00020000.00000000.sdmp, A658.exe, 0000001C.00000002.495884561.0000000000837000.00000004.00000020.00020000.00000000.sdmp	false		high
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02/https://www.google.com/images/branding/product/ico/googleg_lodp.ico	28E9.exe, 00000014.00000003.397412783.000000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02.	E69F.exe, 00000023.00000002.576521462.000000000056B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02PowerShell	E69F.exe, 00000023.00000002.578384942.000000000575000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.56.146.177/e2f032260ba0b2ece29cbd952d3f7f02&	E69F.exe, 00000023.00000002.576521462.000000000056B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.opera.com0	33.exe.4.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	28E9.exe, 00000014.00000003.397412783.000000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://https://support.google.com/chrome/?p=plugin_flash	28E9.exe, 00000014.00000003.393400015.000000000052C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsonn	A658.exe, 0000001C.00000002.495884561.0000000000837000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	28E9.exe, 00000014.00000003.397412783.000000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://https://api.2ip.ua/geo.json	A658.exe, A658.exe, 0000001B.00000002.458620558.0000000002340000.00000040.00001000.00020000.00000000.sdmp, A658.exe, 0000001C.00000003.460852249.000000000087C000.00000004.00000020.00020000.00000000.sdmp, A658.exe, 0000001C.00000003.459744323.000000008AE000.00000004.00000020.00020000.00000000.sdmp, A658.exe, 0000001C.00000002.495884561.0000000000837000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.html	A658.exe, 0000001B.00000002.458620558.0000000002340000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	28E9.exe, 00000014.00000003.397412783.000000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1xD	28E9.exe, 00000014.00000002.419440478.000000000571000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	A658.exe, 0000001B.00000002.458620558.0000000002340000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.138.74.104/8d5bc04a8dfb506a455ebe83e0e99bb1$D	28E9.exe, 00000014.00000002.419440478.000000000571000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	28E9.exe, 00000014.00000003.397412783.0000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high
http://https://mozilla.org0	softokn3.dll.20.dr, nss3.dll.20.dr, mozglue.dll.20.dr, freebl3.dll.20.dr	false	• URL Reputation: safe	unknown
http://www.sqlite.org/copyright.html.	sqlite3.dll.20.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	28E9.exe, 00000014.00000003.397412783.0000000053F000.00000004.00000020.00020000.00000000.sdmp, 8EK4CZ3qdU65.20.dr, y79VUKJAS8XH.20.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.59.14.90	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
185.237.206.60	monsutiur4.com	Ukraine		21100	ITLDC-NLUA	true
110.14.121.125	linislominyt11.at	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
62.204.41.178	unknown	United Kingdom		30798	TNNET-ASTNNetOyMainnetworkFI	false
45.138.74.104	unknown	Russian Federation		202306	HOSTGLOBALPLUS-ASRU	true
190.117.75.91	unknown	Peru		12252	AmericaMovilPeruSACPE	false
85.192.63.46	unknown	Russian Federation		47711	LINEGROUP-ASRU	false
211.119.84.111	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
176.44.127.165	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
193.56.146.177	unknown	unknown		10753	LVLT-10753US	false
175.120.254.9	acacaca.org	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682150
Start date and time:	2022-08-11 06:51:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5tLwjRFzAW.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@19/22@31/12
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.8% (good quality ratio 8.8%) • Quality average: 31.2% • Quality standard deviation: 29.4%
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 • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, BackgroundTransferHost.exe, consent.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:52:49	Task Scheduler	Run new task: Firefox Default Browser Agent 5CED7DF019EF31E9 path: C:\Users\user\AppData\Roaming\irb iwat
06:53:54	Task Scheduler	Run new task: Time Trigger Task path: C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d464 15\A658.exe s>--Task
06:53:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\b4d5e a9d-82ae-4ef5-85ba-00d479d46415\A658.exe" --AutoStart

Time	Type	Description
06:54:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run SysHelper "C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe" --AutoStart

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\LocalLow\8EK4CZ3qdU65

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\freebl3.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	684984
Entropy (8bit):	6.857030838615762
Encrypted:	false
SSDEEP:	12288:0oUg2twzqWC4kBNv1pMByWk6TYnhCevOEH07OqHM65BaFBuY3NUNeCLIV/Rqnhab:0oUg2tJWC44WUuY3mMCLA/R+hw

MD5:	15B61E4A910C172B25FB7D8CCB92F754
SHA1:	5D9E319C7D47EB6D31AAED27707FE27A1665031C
SHA-256:	B2AE93D30C8BEB0B26F03D4A8325AC89B92A299E8F853E5CAA51BB32575B06C6
SHA-512:	7C1C982A2B597B665F45024A42E343A0A07A6167F77EE428A203F23BE94B5F225E22A270D1A41B655F3173369F27991770722D765774627229B6B1BBE2A6DC3F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...&.9b....."!.....6.....@A.....4,..S.....x.....T.....8$...&.....0.....D.....text..... ..`.rdata.....0.....@..@.data...<F...@.....&.....@....00cfg.....(.....@..@.rsrc...x.....*.....@..@.reloc..8$.....&.....@..B.....

C:\Users\user\AppData\LocalLow\jId0qk9WVSf3

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\LocalLow\k0MUzhlF0pI7

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	82970
Entropy (8bit):	7.895892489615255
Encrypted:	false
SSDEEP:	1536:CzyNBlUqBJA57Io5tkoQWKqrXFzkuCN2AyaXQ6Eg0tmj+b7XGDRTt+DlhiVxp66d:zUWJARn5tk6KGF4327aA6fK7WFSKhd
MD5:	482FC19CD3F96C3DA9242265798F7EC0
SHA1:	F07735D226AEF7D49FBD4F9E78C687E8C4A76C35
SHA-256:	39129DDED7D948C84869863FB1EC775C1AF378BD15EF5C2985A58D3745857C5F
SHA-512:	AEB22882FC1A4EB1C36067E3C4A75CC79DEE016B4038AF9740F749CF5F4D2A2B9DE442F62B9DADFAA74A8C52CFAE18C4D2FCF935EE147840518451D91C384F2
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222.....

C:\Users\user\AppData\LocalLow\mozglue.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	627128
Entropy (8bit):	6.792651884784197
Encrypted:	false
SSDEEP:	12288:dfsiG5KNZea77VUHQqROmbIDm0ICRfCtbtEE/2OH9E2ARlZYSd:df53NZea3V+QqROmum0nRKx79E2ARlrd
MD5:	F07D9977430E762B563EAADC2B94BBFA
SHA1:	DA0A05B2B8D269FB73558DFCF0ED5C167F6D3877
SHA-256:	4191FAF7E5EB105A0F4C5C6ED3E9E9C71014E8AA39BBEE313BC92D1411E9E862

SHA-512:	6AFD512E4099643BBA3FC7700DD72744156B78B7BDA10263BA1F8571D1E282133A433215A9222A7799F9824F244A2BC80C2816A62DE1497017A4B26D562B7EAF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b.....''!.....V...../.....@A.... .....cQ.....,....p.....r.....4C.....W.....h0.....text..... ..`.rdata.....0.....@..@.data..... .0.....@....00cfg.....P..... .....@..@.tls.....`.....''.....@....rsrc.....p.....$.....@..@.reloc..4C.....D.....@..B..... ....

C:\Users\user\AppData\LocalLow\msvcp140.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	449280
Entropy (8bit):	6.670243582402913
Encrypted:	false
SSDEEP:	12288:UEPa9C9VbL+3Omy5CvyOvzeOKaqhUgiW6QR7t5s03Ooc8dHkC2esGgW8g:UEPa90Vbky5CvyUeOKg03Ooc8dHkC2ed
MD5:	1FB93933FD087215A3C7B0800E6BB703
SHA1:	A78232C352ED06CEDD7CA5CD5CB60E61EF8D86FB
SHA-256:	2DB7FD3C9C3C4B67F2D50A5A50E8C69154DC859780DD487C28A4E6ED1AF90D01
SHA-512:	79CD448E44B5607863B3CD0F9C8E1310F7E340559495589C428A24A4AC49BEB06502D787824097BB959A1C9CB80672630DAC19A405468A0B64DB5EBD6493590E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1C.._...._..._)n...._.....,_...^."._..^..._..\..._..[..._..Z..._..._.....,_..]..._.Rich.._.....PE..L....(.[....."!.....(.....`.....@.....@A.....g.....r.....?.....=..`x..8.....w ..@.....p.....c..@.....text...&.....(..... ..`.data...H)...@.....,.....@....idata.....p.....D.....@..@.didat..4.....X.....@....rsrc..... .....Z.....@..@.reloc...=.....>...^.....@..B..... .....

C:\Users\user\AppData\LocalLow\nss3.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2042296
Entropy (8bit):	6.775178510549486
Encrypted:	false
SSDEEP:	49152:6dvFywfzFAF7fg39IwA49Kap9bGt+qoStYnOsbqbeQom7gN7BpDD5SkIN1g5D92+:pptximYfpx8OwNiVG09
MD5:	F67D08E8C02574CBC2F1122C53BFB976
SHA1:	6522992957E7E4D074947CAD63189F308A80FCF2
SHA-256:	C65B7AFB05EE2B2687E6280594019068C3D3829182DFE8604CE4ADF2116CC46E
SHA-512:	2E9D0A211D2B085514F181852FAE6E7CA6AED4D29F396348BEDB59C556E39621810A9A74671566A49E126EC73A60D0F781FA9085EB407DF1EEFD942C18853BE
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L.....9b.....''!.....&.....`.....@A.... .....!..\..T...@....@..x.....P..h...h.....\...!..@.....text...i..... ..`.rdata.....@..@.data....N.. .....*.....@....00cfg.....0.....@..@.rsrc...x....@.....@..@.reloc..h....P.....@..B..... ....

C:\Users\user\AppData\LocalLow\softokn3.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	254392
Entropy (8bit):	6.686038834818694
Encrypted:	false
SSDEEP:	6144:uI7A8DMhFE2PlKOcpHSvV6x/CHQyhvs277H0mhWGzTdtb2bbIFxW7zrM2ruyYz+h:uI7A8DMhFE2PlbcpSv0x/CJVUmhDzTvS
MD5:	63A1FE06BE877497C4C2017CA0303537
SHA1:	F4F9CBD7066AFB86877BB79C3D23EDDACA15F5A0
SHA-256:	44BE3153C15C2D18F49674A092C135D3482FB89B77A1B2063D01D02985555FE0

SHA-512:	0475EDC7DFBE8660E27D93B7B8B5162043F1F8052AB28C87E23A6DAF9A5CB93D0D7888B6E57504B1F2359B34C487D9F02D85A34A7F17C04188318BB8E89126B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...'.9b.....''!.....@A.... .....tv..S....w.....5..hq.....D{.....text...V..... ..`.rdata.....@..@.data..... .....~.....@....00cfg.....@..@.rsrc.....@..@.reloc...5.....6.....@..B..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1099223
Entropy (8bit):	6.502588297211263
Encrypted:	false
SSDEEP:	24576:9jxwSkSteuT4P/y7HjsXAGJyGvN5z4Rui2IXLbO:9Vww8HyrjsvyWN54RZH+
MD5:	DBF4F8DCEFB8056DC6BAE4B67FF810CE
SHA1:	BBAC1DD8A07C6069415C04B62747D794736D0689
SHA-256:	47B64311719000FA8C432165A0FDCDFED735D5B54977B052DE915B1CBBBF9D68
SHA-512:	B572CA2F2E4A5CC93E4FCC7A18C0AE6DF888AA4C55BC7DA591E316927A4B5CFCBDDA6E60018950BE891FF3B26F470CC5CCE34D217C2D35074322AB84C32A 5D1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...''.,b.v.....!..... .....a..... .....n*..... ...;.....text..... `.P`.data...|'... ...(.....@.`..rdata...D...P. ..F...:.....@.`@.bss....(..... `..edata..n*.....,.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... .@.0..rsrc.....@.0..reloc...;... ...<.....@.0B/4.....8....`.....@.@B/19.....R....p.....@..B/31.....]'...@...(.....@..B/45.....-...p. .....@..B/57.....\.....&.....@.0B/70.....#.....2..

C:\Users\user\AppData\LocalLow\vcruntime140.dll

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	80128
Entropy (8bit):	6.906674531653877
Encrypted:	false
SSDEEP:	1536:l9j/j2886xv555et/MCsjw0BuRK3jteopUecbAdz86B+JfBL+eNv:l9j/j28V55At/zqw+IqLUecbAdz8lJrv
MD5:	1B171F9A428C44ACF85F89989007C328
SHA1:	6F25A874D6CBF8158CB7C491DCEDAA81CEAEBBAE
SHA-256:	9D02E952396BDFF3ABFE5654E07B7A713C84268A225E11ED9A3BF338ED1E424C
SHA-512:	99A06770EEA07F36ABC4AE0CECB2AE13C3ACB362B38B731C3BAED045BF76EA6B61EFE4089CD2EFAC27701E9443388322365BDB039CD388987B24D4A43C973 BD1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....08e.....u.....Rich..... .....PE..L....(.[.....''!.....0.....t(....@A.....?... ....8..... ..@..... .....text..... ..`.data.....@....idata.....@..@.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB

SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\y79VUKJAS8XH

Process:	C:\Users\user\AppData\Local\Temp\28E9.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC7CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\geo[1].json

Process:	C:\Users\user\AppData\Local\Temp\A658.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	499
Entropy (8bit):	4.498676192647716
Encrypted:	false
SSDEEP:	12:YZIYX7kt/QVFRbIm/QVAY9QVFRHQVFRRaZRQVFRQQVFRUm62jOH4:Y/4FQVFRbI0QVAY9QVFRHQVFRGRQVFRX
MD5:	9B34F54321E4DCCB66CD6428C339A33B
SHA1:	64B330EC2D7236E3A67C495A9AA8A8E8EA8A48B4
SHA-256:	AD2D7CA6CB4492C6E78CFD6166EE744F42F835D2B27725A4D4288F878568D8DF
SHA-512:	F6C6517529934EFE8EA7B13D4B10ED67940D87903BB67F40B3BDCDB399EDBCAF5F3387B42A83F50C1F8921FD02E36B9C312DCE1BF9A64AFDDB81736046321E87
Malicious:	false
Preview:	{"ip":"102.129.143.3","country_code":"CH","country":"Switzerland","country_rus":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0438\u044f","country_ua":"\u0428\u0432\u0435\u0439\u0446\u0430\u0440\u0456\u044f","region":"Zurich","region_rus":"\u0426\u044e\u0440\u0438\u0445","region_ua":"\u0426\u044e\u0440\u0438\u0445","city":"Zurich","city_rus":"\u0426\u044e\u0440\u0438\u0445","city_ua":"\u0426\u044e\u0440\u0438\u0445","latitude":"47.36667","longitude":"8.55","zip_code":"8099","time_zone":"+02:00"}

C:\Users\user\AppData\Local\Temp\28E9.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	348160
Entropy (8bit):	6.6448392140069155
Encrypted:	false
SSDEEP:	6144:oLs6YNPpOX4Dyn5DijLnL6f2qq096STong0b1sfNgPCAbh4Eae:oLANhKB6Lnw2qqk6STogEsfCCAN4te
MD5:	FEEEAA3A0D766A6C52B71C23F796912D
SHA1:	74702F7A1F340C6425DDD29775C51013676D5FAF
SHA-256:	A7C064CEA66E6F5F24936AF237C7AA95AFDEC19F064ABA88B4A181A983D299D5
SHA-512:	A37384A6116EEB8A5705A60DF711D5E3D1B35055D341DEB98C918109BA59201A5AB5DCEA867B350CDC617DED9F5A629FDED091CE16BB90813A3EFCEB394A1E18
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-..PLf.PLf.PLf.N..MLf.N...Lf.w...WLf.PLg..Lf.N...Lf.N..QLf.N. ..QLf.RichPLf.....PE..L.....`.....Z.....@.....s/.....P....p...]..... .....@..... .....text..... ..`.data...hx.....@....rsrc....]...p...^.....@..@..... ....

C:\Users\user\AppData\Local\Temp\33.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	371184
Entropy (8bit):	6.828829337879975
Encrypted:	false
SSDEEP:	6144:KS3YW1IIsIbi1F5PsKFuE4dEinxd57Uej6DDXo9GN25Wmh4u10fe2SkJJQzB:KS3YW1Iibi1F5PsKFuE4dEinxd57UhnY
MD5:	C9143FA5E2792724172980E5ACC312F0
SHA1:	904335F82B19A5635420436359O5C9E8B60C48FE
SHA-256:	612DEF8B01093A69AE511693B3888FABE54CA4D4A3AFBF8A99A7212A699E6292
SHA-512:	E2565DCF1808FB36DB19B5EB6E7A53971194B8BFD9CAA6CCF877EB93B3230ED4C7AA24C2F98C066D473659B0DF7F478E4FE539C24DF128F1C1B25951D2685EF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 21%, Browse • Antivirus: ReversingLabs, Detection: 22%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O..#...p...p...p...q...p...q...p...q...pk..q...pk..q...p..zp...p...p[..pk..q#..po..q...po..p...po..q...pRich...p.....PE..L.....b..... .*...d.....3.....@....@.....@.....(.....).....$.....T. .....0...@.....@..D.....text....(.....*..... ..`.rdata.....@.....@..@.data...`.....@....rsrc.....X.....@ ..@.reloc...$.....&...Z.....@..B..... .....

C:\Users\user\AppData\Local\Temp\A658.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	877568
Entropy (8bit):	7.658285935567359
Encrypted:	false
SSDEEP:	24576:K71dsMtHp6fea2lXhR54Q1kdFU67A4H1ZnXORMtgoG7:KBdvlxROdNAgnrtH
MD5:	1FDD74F600A1E3A9CFA80026CF54BC59
SHA1:	7B0FFB143CD52C75EE849DCE42019BAD0138211E
SHA-256:	B9C3B121EC97DDDA74CBC305280E8157021572B6B6FD59C3B066D0B0F5E54B18
SHA-512:	B619FB507CAC5F4825316BECCB9BB0476B62570458E4EFC5731B804CB9F7187A16F9535F23587E0B662BF6A906D61B1B0E2939F742F0B4BD1797166F535E9287
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 47%, Browse • Antivirus: ReversingLabs, Detection: 56%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)./.H.|.H.|.H.|..+|.H.|..(|.H.|..>|.H.|...|.H.|.H.|.H.|..9|.H.|..)|.H.|...|.H.|Rich.H.|.....PE..L...^.@a.....r.....4.....@.....dq..P.... ....`...@..... .....text...xq.....r..... ..`.data.....*...v.....@....rsrc..... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\D0E3.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1601024
Entropy (8bit):	7.806683973845679
Encrypted:	false
SSDEEP:	24576:0gmYfasQzqX2J73PKo0NmWIasAHGP200GgnIj6XIbI7YUSS4cq8THt:0ZYiLJ7E7si9IjqI0B4sH
MD5:	B4EB21B81E6B52F6351E852E08A37CF0
SHA1:	55169A90D308D43298D823493CC6CABCA4DFBF82
SHA-256:	114AA3CD179D20C031074E3A064A9362521E0CF1F917468FA3B60104F3B95540
SHA-512:	74829CFA85FAB2CC8124E605FF8D6508A42725D83928ADFF1C1F8FE9E462881A775E8CBFD306C1A61AF16A87E871DD1758F84A8619AE02090DE9BA046339800
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L.....B*.....@....."..... .....CODE..... ..`DATA.....!....."..... .@...BSS.....idata..... .....@....reloc...p... ...r.....@..P.rsrc....".... "...L.....@..P..... .....

C:\Users\user\AppData\Local\Temp\E69F.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	502784
Entropy (8bit):	6.7446312072585455
Encrypted:	false
SSDEEP:	12288:uhUQ3jSNiEU7pWQZmMmmr1omuSxvB+HTPA7G:qU4jp1WQZmM5s2QTPA7
MD5:	681D98300C552B8C470466D9E8328C8A
SHA1:	D15F4A432A2ABCE96BA9BA74443E566C1FFB933F
SHA-256:	8BBC892AEDC1424CA5C66677B465C826F867515A3FEA28821D015EDCEE71C912
SHA-512:	B909975D0212D5A5A0CB2E2809EE02224AAC729CB761BE97A8E3BE4EE0A1D7470946DA8CF725953C1B2D71FB5FC9DC3C26FD74BCE5DB5CC0E91A106F8BDED887
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....L.....@..... .....@.....~!.....r.....0...k..... ....CODE..... ..`DATA....h.....@...BSS.....M.....idata..~!.....".....@....tls.....rdata..... .....@..P.reloc...k...0...l.....@..P.rsrc....r.....r...:.....@..P..... .....@..P..... .....

C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe

Process:	C:\Users\user\AppData\Local\Temp\A658.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	877568
Entropy (8bit):	7.658285935567359
Encrypted:	false
SSDEEP:	24576:K71dsMtHp6fea2lXhR54Q1kdFU67A4H1ZnXORMtgoG7:KBdvlxROdNAgnrtH
MD5:	1FDD74F600A1E3A9CFA80026CF54BC59
SHA1:	7B0FFB143CD52C75EE849DCE42019BAD0138211E
SHA-256:	B9C3B121EC97DDDA74CBC305280E8157021572B6B6FD59C3B066D0B0F5E54B18
SHA-512:	B619FB507CAC5F4825316BECCB9BB0476B62570458E4EFC5731B804CB9F7187A16F9535F23587E0B662BF6A906D61B1B0E2939F742F0B4BD1797166F535E9287
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)./.H.|.H.|.H.|..+|.H.|..(|.H.|..>|.H.|...|.H.|.H.|.H.|..9|.H.|..)|.H.|...|.H.|Rich.H.|.....PE..L...^.@a.....r.....4.....@.....dq..P.... ....`...@..... .....text...xq.....r..... ..`.data.....*...v.....@....rsrc..... .....@..@..... ....

C:\Users\user\AppData\Roaming\ftvuhuw

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	248375
Entropy (8bit):	**7.999196600711684**
Encrypted:	**true**
SSDEEP:	6144:m+2hPGPD/lBV9l3NoeDKDUJbJqravgQl/Ppx:X2hP+b/V9E1EqravgY/
MD5:	B2BA8409237E7DBEA2E2BC08D6FF00E6
SHA1:	4F1C02B99E259A54C21DC86F787441BAEC2EC47E
SHA-256:	33C58A11F74C94FCB4A4EF68B29C8B2AE4541DCD3D824A54C5AC8EDD2F75F1FC
SHA-512:	4C7F5C3832DC26202857BB23B33B6C81F1A3518CC9E1DD382A1892A0C2DE6C33DC5C5FF509F8A96E69ECA35C692F5108725CC7534FEA8A17F95868E98DE1E44
Malicious:	false

Preview:	-..Ay.Di0:m...C.3.x.&D.Z...-.?.zn...Rd+..#3.>.....d..qU..=..-.~..w....R.:...Q`@...\.E..D.N-`.,.<qK..6...=.G.....9.l9!.]o...`WN{.r.....mn(..;..r...@.m.K".....^.2.Q.....~>...iP5:....?... ..a]o..[...o]i..J*.K^...F.`.wp2v.;.'O.)...bt..N...T$....9..j^}~..%.5...hY+@.c;+NrR:uU....rp..Zz.x..f.(...9.....".....?D.X`.>wqr..-.>DQ.e..f.5U...l....{s).3.pP?1.4....}A.[...[..CF..S...<... ..GuD.E.`.O.....X.,.\r.,.....%.b.....t.[/,.....-2.J.....s.>...K./gBs.?...-.f.....3"}...\.*Z.eD.h...0.Y..v.K....H..O...1...GO7...E.>..l...N..*.....L.Z.ri.4.....H...TO.S....'msv.....g'n... ..j..e.ny....z..S.l..m..e.....x.xih..x...A.s".D.._ ....$..6..j>.0b_{...m.u|..6t..w._TE..&.y._t..9B.....c..G(.3...\.`.X...D._....=.Sb&Do....)b..r<.. .E.i...n...^..Am..z.....o....U.4y..lwp.=...v'. .K....Z#.U....2<....y..w._.q.~.|.t..K.....-q.s.R..iK.aG.P.tL..]..#..he.B6...d.hS.....j..X.5L...F.9c..&6ip..7-M...|9&..%.v..%n.HT!.;...A....m..P;.$).L.8.Y..

C:\Users\user\AppData\Roaming\irbiwat

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	253952
Entropy (8bit):	7.039129263894516
Encrypted:	false
SSDEEP:	6144:m8dYQFv8Aj+VVettSsDgiSZCAGrwVfxz:mPQx9j2engiDAGo
MD5:	203EAECA3C89F5CA7DC82668C4883B5A
SHA1:	0D872229972EC1E3EA8173343A715B4A2FCB5855
SHA-256:	C4624241F0890DADA47236F267303691F82BBBD28EED1A379A498BD3009CB734
SHA-512:	CB4327F27212B1551F5AA5BE48CB83E46C54216AE29787E3B47E4C7E41C581DC12FC03E56827B6DC90C8E35EF2079E474749A82951146441161A4DDC913247DE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.....R.....=.....Rich.....PE..L ...^..`.....8...^.....`.....P....@.....0.....s.....<..<.....{.....h5..@.....text.. ..6.....8..... ..`.data....Z...P...(...<.....@....rsrc....{.....|...d.....@..@.....

C:\Users\user\AppData\Roaming\irbiwat:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.039129263894516
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:	5tLwjRFzAW.exe
File size:	253952
MD5:	203eaeca3c89f5ca7dc82668c4883b5a
SHA1:	0d872229972ec1e3ea8173343a715b4a2fcb5855
SHA256:	c4624241f0890dada47236f267303691f82bbbd28eed1a379a498bd3009cb734
SHA512:	cb4327f27212b1551f5aa5be48cb83e46c54216ae29787e3b47e4c7e41c581dc12fc03e56827b6dc90c8e35ef2079e474749a82951146441161a4ddc913247de
SSDEEP:	6144:m8dYQFv8Aj+VVettSsDgiSZCAGrwVfxz:mPQx9j2engiDAGo
TLSH:	1E44BF2072D1C871E166267888268FE15F7EBD12EA74858B37E4271E6E733C05A7631F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... <.....R.....=.....Rich.....PE..L..^..`.....8.

File Icon

Icon Hash:	8a909989ca8ed2f2

Static PE Info

General

Entrypoint:	0x4060b7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x60CAA95E [Thu Jun 17 01:46:06 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	17d894006bd909847ec5f7cd1793aa2b

Entrypoint Preview

Instruction
call 00007F05085770B8h
jmp 00007F05085714EEh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
call 00007F050857169Ch
xchg cl, ch
jmp 00007F0508571684h
call 00007F0508571693h
fxch st(0), st(1)
jmp 00007F050857167Bh
fabs
fld1
mov ch, cl
xor cl, cl
jmp 00007F0508571671h
mov byte ptr [ebp-00000090h], FFFFFFFEh
fabs
fxch st(0), st(1)

Instruction
fabs
fxch st(0), st(1)
fpatan
or cl, cl
je 00007F0508571666h
fldpi
fsubrp st(1), st(0)
or ch, ch
je 00007F0508571664h
fchs
ret
fabs
fld st(0), st(0)
fld st(0), st(0)
fld1
fsubrp st(1), st(0)
fxch st(0), st(1)
fld1
faddp st(1), st(0)
fmulp st(1), st(0)
ftst
wait
fstsw word ptr [ebp-000000A0h]
wait
test byte ptr [ebp-0000009Fh], 00000001h
jne 00007F0508571667h
xor ch, ch
fsqrt
ret
pop eax
jmp 00007F050857727Fh
fstp st(0)
fld tbyte ptr [0040236Ah]
ret
fstp st(0)
or cl, cl
je 00007F050857166Dh
fstp st(0)
fldpi
or ch, ch
je 00007F0508571664h
fchs
ret
fstp st(0)
fldz
or ch, ch
je 00007F0508571659h
fchs
ret
fstp st(0)
jmp 00007F0508577255h
fstp st(0)
mov cl, ch
jmp 00007F0508571662h
call 00007F050857162Eh
jmp 00007F0508577260h
int3
int3
int3

Instruction
int3
int3
int3

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13ca4	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20ab000	0x17b80	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1200	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	0x3568	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1b0	.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	0x13688	0x13800	False	0.5780498798076923	data	6.592073295679556	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x15000	0x2095a10	0x12800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x20ab000	0x17b80	0x17c00	False	0.6452097039473684	data	6.622093198418492	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
KUNADOREHUMENANAMOVIZO	0x20be710	0x2626	ASCII text, with very long lines, with no line terminators	French	Switzerland
SENUZEMIX	0x20be0d8	0x636	ASCII text, with very long lines, with no line terminators	French	Switzerland
RT_CURSOR	0x20c0d38	0x330	dBase III DBT, version number 0, next free block index 40, 1st item "\377\217\377\377\376?"	French	Switzerland
RT_CURSOR	0x20c1068	0x130	data	French	Switzerland
RT_CURSOR	0x20c11c0	0x130	data	French	Switzerland
RT_CURSOR	0x20c12f0	0xb0	GLS_BINARY_LSB_FIRST	French	Switzerland
RT_ICON	0x20ab8a0	0xea8	data	Kannada	Kanada
RT_ICON	0x20ac748	0x8a8	data	Kannada	Kanada
RT_ICON	0x20acff0	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20ad558	0x25a8	data	Kannada	Kanada
RT_ICON	0x20afb00	0x10a8	data	Kannada	Kanada
RT_ICON	0x20b0ba8	0x988	data	Kannada	Kanada
RT_ICON	0x20b1530	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20b1a00	0xea8	data	Kannada	Kanada

Name	RVA	Size	Type	Language	Country
RT_ICON	0x20b28a8	0x8a8	data	Kannada	Kanada
RT_ICON	0x20b3150	0x6c8	data	Kannada	Kanada
RT_ICON	0x20b3818	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20b3d80	0x25a8	data	Kannada	Kanada
RT_ICON	0x20b6328	0x10a8	data	Kannada	Kanada
RT_ICON	0x20b73d0	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20b78a0	0xea8	data	Kannada	Kanada
RT_ICON	0x20b8748	0x8a8	data	Kannada	Kanada
RT_ICON	0x20b8ff0	0x6c8	data	Kannada	Kanada
RT_ICON	0x20b96b8	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x20b9c20	0x25a8	data	Kannada	Kanada
RT_ICON	0x20bc1c8	0x10a8	data	Kannada	Kanada
RT_ICON	0x20bd270	0x988	data	Kannada	Kanada
RT_ICON	0x20bdbf8	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_DIALOG	0x20c1560	0xac	data	French	Switzerland
RT_STRING	0x20c1610	0x4ae	data	French	Switzerland
RT_STRING	0x20c1ac0	0x770	data	French	Switzerland
RT_STRING	0x20c2230	0x464	data	French	Switzerland
RT_STRING	0x20c2698	0x4e8	data	French	Switzerland
RT_GROUP_CURSOR	0x20c1198	0x22	data	French	Switzerland
RT_GROUP_CURSOR	0x20c13a0	0x22	data	French	Switzerland
RT_GROUP_ICON	0x20b1998	0x68	data	Kannada	Kanada
RT_GROUP_ICON	0x20b7838	0x68	data	Kannada	Kanada
RT_GROUP_ICON	0x20be060	0x76	data	Kannada	Kanada
RT_VERSION	0x20c13c8	0x194	data	French	Switzerland

Imports

DLL	Import
KERNEL32.dll	GetModuleFileNameA, FoldStringA, InterlockedDecrement, _hread, CancelWaitableTimer, WaitNamedPipeW, BuildCommDCBW, GetConsoleAliasExesLengthW, PeekConsoleInputA, CreateFileA, RegisterWaitForSingleObjectEx, LoadLibraryW, EnumResourceTypesA, TransmitCommChar, GetFirmwareEnvironmentVariableW, BeginUpdateResourceA, WriteConsoleW, DeleteFileA, GetProcAddress, GetUserDefaultLCID, GetConsoleAliasW, FindFirstChangeNotificationA, RemoveDirectoryA, GetCalendarInfoW, FindFirstFileExW, AreFileApisANSI, GetCurrentDirectoryW, GetConsoleAliasesLengthW, SetConsoleTitleW, GetBinaryTypeW, GlobalAlloc, FindNextFileA, OpenJobObjectA, HeapFree, _lclose, GetComputerNameA, TlsSetValue, SetCalendarInfoW, SetComputerNameA, LoadLibraryA, FoldStringW, GetDiskFreeSpaceW, GetSystemDefaultLangID, SetThreadLocale, FillConsoleOutputCharacterA, RtlUnwind, MultiByteToWideChar, GetCommandLineW, HeapSetInformation, GetStartupInfoW, EncodePointer, IsProcessorFeaturePresent, GetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, DecodePointer, TerminateProcess, GetCurrentProcess, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionAndSpinCount, SetHandleCount, GetStdHandle, GetFileType, DeleteCriticalSection, TlsAlloc, TlsGetValue, TlsFree, InterlockedIncrement, GetModuleHandleW, SetLastError, GetCurrentThreadId, ExitProcess, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, CloseHandle, WriteFile, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, Sleep, WideCharToMultiByte, RaiseException, SetFilePointer, GetConsoleCP, GetConsoleMode, LCMapStringW, GetStringTypeW, SetStdHandle, FlushFileBuffers, HeapAlloc, HeapReAlloc, SetEndOfFile, GetProcessHeap, ReadFile, HeapSize, CreateFileW
GDI32.dll	GetCharWidth32A

Possible Origin

Language of compilation system	Country where language is spoken	Map
French	Switzerland	
Kannada	Kanada	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.138.74.104 49759802036934 08/11/22-06:53:10.741012	TCP	2036934	ET TROJAN Win32/RecordBreaker CnC Checkin	49759	80	192.168.2.3	45.138.74.104
45.138.74.104192.168.2.380497592036955 08/11/22-06:53:11.296973	TCP	2036955	ET TROJAN Win32/RecordBreaker CnC Checkin - Server Response	80	49759	45.138.74.104	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:52:49.869482994 CEST	49749	80	192.168.2.3	185.237.206.60
Aug 11, 2022 06:52:52.876912117 CEST	49749	80	192.168.2.3	185.237.206.60
Aug 11, 2022 06:52:58.249072075 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:52:58.559278011 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:58.559457064 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:52:58.559519053 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:52:58.563397884 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:52:58.873621941 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.618261099 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.618315935 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.618560076 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:52:59.929085016 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.929169893 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.929227114 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.929277897 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:52:59.929373980 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:52:59.929431915 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.239784956 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.239871025 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.239931107 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.239984989 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.240029097 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.240041971 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.240078926 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.240211964 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.240268946 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.240320921 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.240343094 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.241118908 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.550545931 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.550627947 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.550690889 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.550749063 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.550873995 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.551085949 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551150084 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.551281929 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551336050 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551398039 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.551417112 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551466942 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551525116 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.551565886 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551683903 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551763058 CEST	49754	80	192.168.2.3	110.14.121.125

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:53:00.551889896 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551943064 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.551951885 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.552064896 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.552130938 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.552196026 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.643435001 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.861150980 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.861258030 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.861310959 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.861362934 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.861399889 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.861453056 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.861916065 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862095118 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862159967 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862207890 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.862343073 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862397909 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862451077 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862452984 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.862529039 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.862607002 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862668991 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862767935 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.862771034 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862894058 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862946987 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.862987041 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.863110065 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863204002 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.863240004 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863293886 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863387108 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.863434076 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863576889 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863673925 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.863730907 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863786936 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.863878965 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.863893986 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.864056110 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.864109039 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.864151955 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.864267111 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.864367008 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.864396095 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.864577055 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.864677906 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:00.953901052 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.953969955 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:00.954103947 CEST	49754	80	192.168.2.3	110.14.121.125
Aug 11, 2022 06:53:01.172090054 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:01.173774004 CEST	80	49754	110.14.121.125	192.168.2.3
Aug 11, 2022 06:53:01.173830986 CEST	80	49754	110.14.121.125	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:52:49.551544905 CEST	192.168.2.3	8.8.8.8	0x5feb	Standard query (0)	monsutiur4.com	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.559319973 CEST	192.168.2.3	8.8.8.8	0x5fee	Standard query (0)	nusurionuy5ff.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.596689939 CEST	192.168.2.3	8.8.8.8	0x41ef	Standard query (0)	moroitomo4.net	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.714833975 CEST	192.168.2.3	8.8.8.8	0x5dfd	Standard query (0)	susuerulia nita1.net	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.830281019 CEST	192.168.2.3	8.8.8.8	0x6188	Standard query (0)	cucumbetut urel4.com	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.861974001 CEST	192.168.2.3	8.8.8.8	0x3f2f	Standard query (0)	nunuslusha u.com	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.905580997 CEST	192.168.2.3	8.8.8.8	0x819f	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.094981909 CEST	192.168.2.3	8.8.8.8	0xb37f	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.147916079 CEST	192.168.2.3	8.8.8.8	0x932e	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:08.751971006 CEST	192.168.2.3	8.8.8.8	0x3b75	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.544703960 CEST	192.168.2.3	8.8.8.8	0x3d48	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.043751001 CEST	192.168.2.3	8.8.8.8	0xa4e0	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.185066938 CEST	192.168.2.3	8.8.8.8	0x6fd5	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.550822020 CEST	192.168.2.3	8.8.8.8	0xa62a	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.747505903 CEST	192.168.2.3	8.8.8.8	0xd307	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.130366087 CEST	192.168.2.3	8.8.8.8	0x31fe	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.595168114 CEST	192.168.2.3	8.8.8.8	0x229b	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.587106943 CEST	192.168.2.3	8.8.8.8	0xa77	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.057549953 CEST	192.168.2.3	8.8.8.8	0xb36b	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.645205021 CEST	192.168.2.3	8.8.8.8	0x262d	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.699114084 CEST	192.168.2.3	8.8.8.8	0x4260	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.095474005 CEST	192.168.2.3	8.8.8.8	0xbfa3	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:09.813925982 CEST	192.168.2.3	8.8.8.8	0xde88	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.042941093 CEST	192.168.2.3	8.8.8.8	0xbe35	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.247318983 CEST	192.168.2.3	8.8.8.8	0x67b0	Standard query (0)	rgyui.top	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.247670889 CEST	192.168.2.3	8.8.8.8	0x10c3	Standard query (0)	acacaca.org	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.538197994 CEST	192.168.2.3	8.8.8.8	0xeb4d	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.814412117 CEST	192.168.2.3	8.8.8.8	0x6575	Standard query (0)	acacaca.org	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.259375095 CEST	192.168.2.3	8.8.8.8	0x10c3	Standard query (0)	acacaca.org	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.666434050 CEST	192.168.2.3	8.8.8.8	0xb552	Standard query (0)	linislominyt11.at	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:14.666161060 CEST	192.168.2.3	8.8.8.8	0xa8ee	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:52:49.866349936 CEST	8.8.8.8	192.168.2.3	0x5feb	No error (0)	monsutiur4.com		185.237.206.60	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.588399887 CEST	8.8.8.8	192.168.2.3	0x5fee	Name error (3)	nusurionuy5ff.at	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:52:57.706404924 CEST	8.8.8.8	192.168.2.3	0x41ef	Name error (3)	moroitomo4.net	none	none	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.821547031 CEST	8.8.8.8	192.168.2.3	0x5dfd	Name error (3)	susuerulia nita1.net	none	none	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.850227118 CEST	8.8.8.8	192.168.2.3	0x6188	Name error (3)	cucumbetut urel4.com	none	none	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:57.883857012 CEST	8.8.8.8	192.168.2.3	0x3f2f	Name error (3)	nunuslusha u.com	none	none	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:52:58.248347044 CEST	8.8.8.8	192.168.2.3	0x819f	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:02.462577105 CEST	8.8.8.8	192.168.2.3	0xb37f	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		190.117.75.91	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		186.182.55.44	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		1.248.122.240	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		93.123.96.98	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		222.232.238.243	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		116.121.62.237	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		211.171.233.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		115.88.24.203	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:03.466960907 CEST	8.8.8.8	192.168.2.3	0x932e	No error (0)	linislominyt11.at		190.195.107.105	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:09.110985994 CEST	8.8.8.8	192.168.2.3	0x3b75	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:10.564136028 CEST	8.8.8.8	192.168.2.3	0x3d48	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:12.061644077 CEST	8.8.8.8	192.168.2.3	0xa4e0	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:13.552937031 CEST	8.8.8.8	192.168.2.3	0x6fd5	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		190.117.75.91	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		186.182.55.44	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		1.248.122.240	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		93.123.96.98	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		222.232.238.243	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		116.121.62.237	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		211.171.233.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		115.88.24.203	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:42.570538044 CEST	8.8.8.8	192.168.2.3	0xa62a	No error (0)	linislominyt11.at		190.195.107.105	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:43.939891100 CEST	8.8.8.8	192.168.2.3	0xd307	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.152057886 CEST	8.8.8.8	192.168.2.3	0x31fe	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:51.615968943 CEST	8.8.8.8	192.168.2.3	0x229b	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:52.606836081 CEST	8.8.8.8	192.168.2.3	0xa77	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:54.076776028 CEST	8.8.8.8	192.168.2.3	0xb36b	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:57.667078972 CEST	8.8.8.8	192.168.2.3	0x262d	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linislominyt11.at		190.117.75.91	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linislominyt11.at		186.182.55.44	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linislominyt11.at		1.248.122.240	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linislominyt11.at		93.123.96.98	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linisllominyt11.at		222.232.238.243	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linisllominyt11.at		116.121.62.237	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linisllominyt11.at		211.171.233.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linisllominyt11.at		115.88.24.203	A (IP address)	IN (0x0001)
Aug 11, 2022 06:53:58.716547966 CEST	8.8.8.8	192.168.2.3	0x4260	No error (0)	linisllominyt11.at		190.195.107.105	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:04.115011930 CEST	8.8.8.8	192.168.2.3	0xbfa3	No error (0)	linisllominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:09.832884073 CEST	8.8.8.8	192.168.2.3	0xde88	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.063865900 CEST	8.8.8.8	192.168.2.3	0xbe35	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.559978008 CEST	8.8.8.8	192.168.2.3	0xeb4d	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		190.140.74.43	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		175.119.10.231	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		187.170.251.250	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		211.171.233.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		190.225.159.63	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		109.102.255.230	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		86.123.136.87	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		185.95.186.58	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		151.251.24.5	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:11.591129065 CEST	8.8.8.8	192.168.2.3	0x67b0	No error (0)	rgyui.top		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		187.212.184.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		190.140.99.150	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		151.251.24.5	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		186.6.243.2	A (IP address)	IN (0x0001)

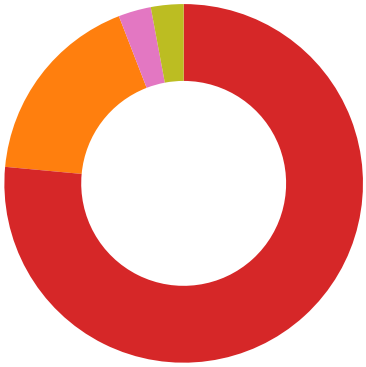
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		115.88.24.203	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		190.117.75.91	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.249802113 CEST	8.8.8.8	192.168.2.3	0x6575	No error (0)	acacaca.org		115.88.24.202	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		190.219.54.242	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		211.119.84.112	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		190.107.133.19	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		151.251.24.5	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		211.171.233.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		210.182.29.70	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		115.88.24.202	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.315112114 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		115.88.24.203	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		115.88.24.202	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		187.212.184.129	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		190.140.99.150	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		151.251.24.5	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		186.6.243.2	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		115.88.24.203	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:12.559225082 CEST	8.8.8.8	192.168.2.3	0x10c3	No error (0)	acacaca.org		190.117.75.91	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		110.14.121.125	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		87.119.100.220	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		211.119.84.111	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		211.53.230.67	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		58.235.189.192	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		46.195.219.190	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		211.59.14.90	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		175.120.254.9	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		138.36.3.134	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:13.686130047 CEST	8.8.8.8	192.168.2.3	0xb552	No error (0)	linislominyt11.at		176.44.127.165	A (IP address)	IN (0x0001)
Aug 11, 2022 06:54:14.685503006 CEST	8.8.8.8	192.168.2.3	0xa8ee	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ynbbrbceap.org
  - linislominyt11.at
- oywaxqplv.net
- grmajt.com
- ujdgu.net
- 45.138.74.104
- xysctbcs.com
- hghdetsybj.com
- niskfgcbn.org
- vuhmrda.org
- kmthapyqsb.org
- tqgrrc.org
- ppejyk.com
- 85.192.63.46
- kekatmodj.org
- 62.204.41.178
- rgvwxic.org
- kxdfdo.com
- 193.56.146.177
- acacaca.org

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 5tLwjRFzAW.exe PID: **5320**, Parent PID: **5328**

General	
Target ID:	0
Start time:	06:52:05
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\5tLwjRFzAW.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\5tLwjRFzAW.exe"
Imagebase:	0x400000
File size:	253952 bytes
MD5 hash:	203EAECA3C89F5CA7DC82668C4883B5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.294980929.00000000026E7000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.295278143.0000000004271000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.295278143.0000000004271000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.294639140.0000000002680000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.294702276.0000000002690000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.294702276.0000000002690000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3968**, Parent PID: **5320**

General	
Target ID:	4
Start time:	06:52:12
Start date:	11/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000000.278637701.0000000002651000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000004.00000000.278637701.0000000002651000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: irbiwat PID: **4748**, Parent PID: **848**

General

Target ID:	17
Start time:	06:52:49
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Roaming\irbiwat
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\irbiwat
Imagebase:	0x400000
File size:	253952 bytes
MD5 hash:	203EAECA3C89F5CA7DC82668C4883B5A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000011.00000002.343161421.00000000040E0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000011.00000002.342997867.0000000002546000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.343191676.00000000040F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000011.00000002.343191676.00000000040F0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000011.00000002.343211043.0000000004111000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000011.00000002.343211043.0000000004111000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 28E9.exe PID: **4384**, Parent PID: **3968**

General

Target ID:	20
Start time:	06:53:07
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\28E9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\28E9.exe
Imagebase:	0x400000
File size:	348160 bytes
MD5 hash:	FEEEAA3A0D766A6C52B71C23F796912D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000002.418605685.00000000004CC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.397574395.00000000004CC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.390943564.00000000004CF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.381054499.00000000004D1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000014.00000002.419481551.0000000000580000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.389798020.00000000004CE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000014.00000002.418304961.0000000000499000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.393288664.00000000004D0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.392382222.00000000004CF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.392760515.00000000004CF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.372026419.00000000004D3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000014.00000003.391797560.00000000004CF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 81%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	407E10	HttpSendRequestW
C:\Users\user\AppData\LocalLow\nss3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\msvcp140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\vcruntime140.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\mozglue.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\freebl3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\softokn3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	408598	CreateFileW
C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	4029C5	CopyFileW
C:\Users\user\AppData\LocalLow\jId0qk9WVSf3	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	402EE4	CopyFileW
C:\Users\user\AppData\LocalLow\8EK4CZ3qdU65	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	403869	CopyFileW
C:\Users\user\AppData\LocalLow\y79VUKJAS8XH	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	403443	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X	success or wait	1	402C8C	DeleteFileW
C:\Users\user\AppData\LocalLow\jId0qk9WVSf3	success or wait	1	403229	DeleteFileW
C:\Users\user\AppData\LocalLow\8EK4CZ3qdU65	success or wait	1	4039B0	DeleteFileW
C:\Users\user\AppData\LocalLow\y79VUKJAS8XH	success or wait	1	403734	DeleteFileW
C:\Users\user\AppData\LocalLow\k0MUzhlF0pI7	success or wait	1	408254	DeleteFileW
C:\Users\user\AppData\LocalLow\nss3.dll	success or wait	1	407C18	DeleteFileW
C:\Users\user\AppData\LocalLow\sqlite3.dll	success or wait	1	407C37	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\nss3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 19 00 00 26 05 00 00 00 00 00 fd 01 15 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 60 1f 00 00 04 00 00 fd fd 1f 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 21 1d 00 5c fd 00 00 54 fd 1d 00 40 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!&`@A!\T@	success or wait	998	4085D8	WriteFile
C:\Users\user\AppData\LocalLow\msvcp140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 53 31 43 fd fd 5f 10 fd fd 5f 10 fd fd 5f 10 29 6e fd 10 fd fd 5f 10 fd fd fd 10 fd fd 5f 10 fd fd 5e 10 22 fd 5f 10 da 5e 11 fd fd 5f 10 da 5c 11 fd fd 5f 10 da 5b 11 fd fd 5f 10 da 5a 11 fd fd 5f 10 da 5f 11 fd fd 5f 10 da fd 10 fd fd 5f 10 da 5d 11 fd fd 5f 10 52 69 63 68 fd fd 5f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$1C___)n__^"_^__[_Z____]_Rich_	success or wait	220	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\vcruntime140.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 44 fd fd fd fd fd fd fd fd fd fd 30 38 65 fd fd fd fd fd fd 19 fd fd fd fd fd fd fd fd fd fd fd fd fd 09 fd fd fd fd fd fd 0e fd fd fd fd fd fd 0f fd fd fd fd fd fd 0a fd fd fd fd fd fd fd 75 fd fd fd fd fd fd 08 fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 28 fd 5b 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$08euRichPEL(["	success or wait	40	4085D8	WriteFile
C:\Users\user\AppData\LocalLow\mozglue.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 07 00 fd fd 39 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 18 08 00 00 56 01 00 00 00 00 00 fd 2f 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 09 00 00 04 00 00 fd fd 09 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd fd 08 00 63 51 00 00 10 0e 09 00 2c 01 00	MZx@x!L!This program cannot be run in DOS mode.$PEL9b"!V/@AcQ,	success or wait	307	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\freebl3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 26 fd 39 62 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 1a 08 00 00 36 02 00 00 00 00 00 fd 1f 08 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 0a 00 00 04 00 00 fd 0a 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 34 2c 0a 00 53 00 00 00 fd 2c 0a 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL&9b"!6@A4,S,	success or wait	335	4085D8	WriteFile
C:\Users\user\AppData\LocalLow\softokn3.dll	0	2048	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 06 00 27 fd 39 62 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 fd 02 00 00 fd 00 00 00 00 00 00 fd fd 02 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 00 04 00 00 04 00 00 fd fd 04 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 74 76 03 00 53 01 00 00 fd 77 03 00 fd 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL'9b"!@AtvSw	success or wait	125	4085D8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \sqlite3.dll	0	2048	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 12 00 22 fd 2c 62 00 76 0e 00 fd 13 00 00 fd 00 06 21 0b 01 02 19 00 0c 0b 00 00 fd 0c 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 20 0b 00 00 00 fd 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 10 0f 00 00 06 00 00 1d 11 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 fd 0c 00 6e 2a 00	MZ@!L!This program cannot be run in DOS mode.$PEL",bv! a n*	success or wait	537	4085D8	WriteFile
C:\Users\user\AppData\LocalLow \w00Fi2l6Hi6X	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	4029C5	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow \jId0qk9WVSf3	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C g 8	success or wait	1	402EE4	CopyFileW
C:\Users\user\AppData\LocalLow \8EK4CZ3qdU65	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 fd 05 00 00 00 02 07 fd 00 00 00 00 1b 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ $.C	success or wait	1	403869	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\y79VUKJAS8XH	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 fd 05 00 00 00 02 07 fd 00 00 00 00 1b 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ $.C	success or wait	1	403443	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	87164	success or wait	1	401D3E	ReadFile
C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\w00Fi2l6Hi6X	28672	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\jId0qk9WVSf3	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\jId0qk9WVSf3	0	4096	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\8EK4CZ3qdU65	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\8EK4CZ3qdU65	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\y79VUKJAS8XH	0	100	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\y79VUKJAS8XH	0	2048	success or wait	1	61E33E79	ReadFile
C:\Users\user\AppData\LocalLow\k0MUzhlF0pI7	unknown	82970	success or wait	1	408227	ReadFile

Analysis Process: A658.exe PID: **5244**, Parent PID: **3968**

General

Target ID:	27
Start time:	06:53:40
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\A658.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A658.exe
Imagebase:	0x400000
File size:	877568 bytes
MD5 hash:	1FDD74F600A1E3A9CFA80026CF54BC59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000001B.00000002.457366920.000000000066D000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001B.00000002.458620558.0000000002340000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001B.00000002.458620558.0000000002340000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: A658.exe PID: **4164**, Parent PID: **5244**

General

Target ID:	28
Start time:	06:53:43
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\A658.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A658.exe
Imagebase:	0x400000
File size:	877568 bytes
MD5 hash:	1FDD74F600A1E3A9CFA80026CF54BC59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001C.00000000.451618454.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000000.451618454.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001C.00000000.451618454.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000000.451618454.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001C.00000002.485432276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000002.485432276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001C.00000002.485432276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000002.485432276.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001C.00000000.447519166.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000000.447519166.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001C.00000000.447519166.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000000.447519166.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000000.445516045.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001C.00000000.448145727.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000000.448145727.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001C.00000000.448145727.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000000.448145727.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001C.00000000.449295110.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000000.449295110.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001C.00000000.449295110.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000000.449295110.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 0000001C.00000000.446739246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000001C.00000000.446739246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 0000001C.00000000.446739246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000001C.00000000.446739246.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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: regsvr32.exe PID: **5148**, Parent PID: **3968**

General

Target ID:	30
Start time:	06:53:50
Start date:	11/08/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 /s C:\Users\user\AppData\Local\Temp\D0E3.dll
Imagebase:	0x7ff601900000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D0E3.dll	unknown	64	success or wait	1	7FF6019010E3	ReadFile
C:\Users\user\AppData\Local\Temp\D0E3.dll	unknown	264	success or wait	1	7FF601901125	ReadFile

Analysis Process: regsvr32.exe PID: **2360**, Parent PID: **5148**

General

Target ID:	31
Start time:	06:53:51
Start date:	11/08/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	/s C:\Users\user\AppData\Local\Temp\D0E3.dll
Imagebase:	0xeb0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 0000001F.00000002.502148462.0000000004CD0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: icacls.exe PID: **3980**, Parent PID: **4164**

General

Target ID:	32
Start time:	06:53:52
Start date:	11/08/2022

Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	icacls "C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Imagebase:	0x1c0000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	83			invalid handle	1	1C1B0A	WriteFile
unknown	unknown	59			invalid handle	1	1C1B0A	WriteFile

Analysis Process: A658.exe PID: **4276**, Parent PID: **848**

General

Target ID:	33
Start time:	06:53:54
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\b4d5ea9d-82ae-4ef5-85ba-00d479d46415\A658.exe --Task
Imagebase:	0x400000
File size:	877568 bytes
MD5 hash:	1FDD74F600A1E3A9CFA80026CF54BC59
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: E69F.exe PID: **1436**, Parent PID: **3968**

General

Target ID:	35
Start time:	06:53:55
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\E69F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E69F.exe
Imagebase:	0x400000
File size:	502784 bytes
MD5 hash:	681D98300C552B8C470466D9E8328C8A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000023.00000003.479074188.0000000000572000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Crypt, Description: Yara detected CryptOne packer, Source: 00000023.00000002.596787162.00000000023C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RaccoonV2, Description: Yara detected Raccoon Stealer v2, Source: 00000023.00000002.578384942.0000000000575000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: A658.exe PID: **2196**, Parent PID: **4164**

General

Target ID:	39
Start time:	06:54:01
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\A658.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\A658.exe" --Admin IsNotAutoStart IsNotTask
Imagebase:	0x400000
File size:	877568 bytes
MD5 hash:	1FDD74F600A1E3A9CFA80026CF54BC59
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 47%, Metadefender, Browse • Detection: 56%, ReversingLabs
Reputation:	low

Analysis Process: 33.exe PID: **4708**, Parent PID: **3968**

General

Target ID:	40
Start time:	06:54:02
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Local\Temp\33.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\33.exe
Imagebase:	0xb50000
File size:	371184 bytes
MD5 hash:	C9143FA5E2792724172980E5ACC312F0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly