The Retefe Saga

Archived: 2026-11-28 02:04:19 UTC

Published on August 3, 2017 11:15 UTC by GovCERT.ch (permalink)
Last updated on August 3, 2017 11:20 UTC

Surprisingly, there is a lot of media attention going on at the moment on a macOS malware called *OSX/Dok*. In the recent weeks, various anti-virus vendors and security researchers published blog posts on this threat, presenting their analysis and findings. While some findings where very interesting, others were misleading or simply wrong.

We don't know where the sudden media interest and the attention from anti-virus vendors on this threat actor are coming from. As a matter of fact, the threat actor behind OSX/Dok, which we call the the *Retefe gang* or *Operation Emmental*, has already been around for many years and GovCERT.ch is tracking their activities since the very beginning (2013). The purpose of this blog post is to put the puzzle pieces together and trying to bust some of the myths that have made the round in the media recently.


Timeline of Retefe Threat (aka Operation Emmental)

Timeline of Retefe Threat (aka Operation Emmental)

Jul 2013 - The early days (Citadel)

The first sign of this threat actor dates back to July 2013, when we identified a malware campaign that was targeting various financial institutions in Switzerland, using an e-banking trojan called Citadel (*BotnetID 504 + 510*). Citadel is a crimeware kit and a successor of the famous ZeuS Trojan. The malware campaign was usually easy identifiable as the threat actor was always using the same URL structure.

```
 Sample Citadel config URLs:
2014-01-23 http://swarovski.prfact.ch/sadcxvbv/vdfbffddf.php
2014-01-17 http://coiffurehaargenau.ch/sadcxvbv/vdfbffddf.php
2013-12-11 http://designgallery.ch/sadcxvbv/vdfbffddf.php

Sample Citadel dropzone URLs:
2014-01-28 http://floorwash.ch/wqwcqqw/sasasacw.php
2014-01-24 http://apx.euclid.ch/wqwcqqw/sasasacw.php
2014-01-24 http://www.buchkeller.ch/wqwcqqw/sasasacw.php
```


Sample Citadel botnet C&C traffic to a config URL

Sample Citadel botnet C&C; traffic to a config URL

Citadel was very active between 2010 and 2014. However, after its highs in 2014, most of the cybercriminals turned away from Citadel to other crimeware kits. So did the Retefe gang - the said Citadel campaign disappeared in 2014.

Jun 2014 - Moving forward (Retefe)

In 2014, a few months after Citadel disappeared, a spam campaign hit the Swiss cyberspace. The spam emails pretends to come from well-known Swiss online brands, such as *LeShop.ch* or *Zalando*, and contain a malicious RTF (Rich Text Format) file. The malicious RTF file contained an embedded windows executable (either a *.cpl* or *.exe* file) that, once executed, infected the victim's machine with malware. The malware was new to us; we have never seen such code before. We could not link it to an existing crimeware kit, so it appeared to be a custom development. Microsoft later named the malware Retefe (we guess because of the way Retefe spreads: a malicious RTF – ReTeFe). Retefe was born!

During our technical analysis, we identified a list of financial institutions in Switzerland for which Retefe redirects the e-banking session to a counterfeit portal. This target-list is identical to the one we have already seen in the Citadel campaigns in 2013 and early 2014. Due to this and the fact that Citadel suddenly disappeared just a few months before the first sign of Retefe, we believe that the same threat actor is behind these two malware campaigns. The gang just moved away from Citadel to a different malware family (as many other cybercriminals did).

What makes Retefe a very interesting piece of malware is the fact that it is not necessarily malware. Unlike Citadel and other malware families, Retefe "just" changes certain settings of the victim's computer in a hostile way. Hence, most anti-virus software is not able to detect Retefe because the malware is not using any malicious code. In 2014, Retefe changed the following computer settings in order to commit e-banking fraud:

- Changes the computers DNS settings to make use of a rogue DNS server.
- Installs a rogue CA (Certificate Authority) certificate.

While this sounds trivial, these changes are very effective and have a big influence on the victim's surf experience. As the threat actor has now control over the victim's domain resolution, they can redirect the victim's e-banking session to a fraudulent copy of the e-banking portal operated by the threat actor. The attacker also issues a SSL certificate using the rogue CA certificate installed on the victim's computer to avoid that the victim's web browser (e.g, Firefox, Internet Explorer, or Chrome) throws an SSL certificate error when browsing the fake e-banking portal.

While this modus operandi is very simple and effective, it also has a significant weak point: the rogue DNS. If the rogue DNS disappears, the attacker is not only no longer able to redirect the e-banking session to the forged portal, the victim will de facto also lose the internet connectivity as the computer won't be able to resolve any domain names anymore. So every time we initiated the takedown of the rogue DNS servers, Retefe victims lost their internet connectivity.

In 2015, the threat actor fixed this "issue" by making use of a malicious proxy auto-config (PAC) in lieu of a rogue DNS. Instead of redirecting the whole DNS traffic of the victim's computer, only web traffic for certain

domain names configured in the PAC published by the attackers would get redirected to a SOCKS proxy. The SOCKS proxy then serves a fake e-banking portal to the victim in order to commit e-banking fraud.


Sample of proxy PAC configuration in Internet Explorer (2014)

Sample of proxy PAC configuration in Internet Explorer (2014)

At that time, Retefe was targeting not only financial institutions in Switzerland but also in Austria, Sweden and Japan. Based on the Geo location of the victim's IP address, the Proxy PAC URL returned a different proxy configuration. If the victim's IP address was located in Austria for example, the proxy configuration contained a list of financial institution in Austria for which the e-banking sessions were redirected.

Dec 2015 - The Tinba connection

It was October 2015, when we saw the usual Retefe spam campaigns imitating LeShop.ch and Zalando. However, when we analysed the malware that was distributed, we quickly came to the conclusion that it was not Retefe. We identified the malware as *Tinba* (also known as *Tiny Banker*). Unlike Retefe, Tinba is another crimeware kit like Citadel. Many threat actors who were using Citadel until 2014 later moved to Tinba. Taking a look at the Tinba configuration file, we noticed that it contained the same target-list as Retefe. Due to this and the fact that the spam campaign that was distributing Tinba at that time was the same as we have seen before distributing Retefe, we believe that this was the same threat actor again.

The Tinba campaign, identified by *Campaign ID 946a936b* (Version ID: 1b030105), was using a domain generation algorithm (DGA) to calculate a list of possible botnet command and control (C&C;) domain names. While using a DGA makes the botnet more resilient against take downs from law enforcement agencies, it also has the disadvantage for the threat actor that security researchers can reverse engineer the code used to generate the DGA domains and predict all possible botnet C&C; domains. Sinkhole data revealed that a vast amount of the computers infected with Tinba were indeed located in Switzerland.


Sample Tinba botnet C&C traffic to DGA domain

Sample Tinba botnet C&C; traffic to DGA domain

Jan 2016 - Trying something new (ExePhish)

Early 2016, we have seen another spam campaign hitting the Swiss cyberspace. The campaign was weird and apparently only targeting customers of one specific financial institution. The spam emails contained an executable (MD5 d770040d2bf4c12c9dc8fd1bfc23bc9b) that, once executed, opened window that looked like a web browser. The fake "web browser" displayed a counterfeit e-banking portal hosted in the tor network (b3pepirxq7l2aybj.onion.link). We believe that this campaign was orchestrated by the Retefe gang too. However, we have only seen this threat once and we believe it was just an (unsuccessful) test by the threat actor. A nice write-up can be found here.

Feb 2016 – Retefe goes social engineering

But the Retefe Gang is not just using email as an infection vector to compromise their victims. In February 2016, we have received multiple reports from small and medium-sized businesses (SMBs) in Switzerland who got phoned by strangers, pretending, for example, to call e.g. in the name of the Swiss Post. The calling person tried to gain the victim's email address under a false pretence (e.g. that a postal package couldn't be delivered and the postal service would like to send further information by email to the victim). If the victim revealed his email address, he would receive an email from the threat actor with a link to Dropbox that served Retefe.

More Information about this modus operandi can be found here (in German, French and Italian): https://www.ncsc.admin.ch/ncsc/de/home/aktuell/news/news-archiv/retefe--angriff-auf-schweizer-bankkunden---praezisierung-durch-m.html

Mar 2016 - Retefe goes VPN

In March 2016, the Retefe gang tried something new. Instead of using a rogue DNS server or PAC file to redirect e-banking traffic of the victim's machine, the threat actor started to spam out a version of Retefe that installed a VPN (PPP) connection to a remote host under control of the miscreant (sample: MD5 6abad08fd5d534ae9f5659989c1e0e31). As a result, all internet traffic from the victim's machine got redirected to a VPN server in Russia (109.234.36.223). The threat actor also installed a rogue CA certificate in order to commit e-banking fraud. As the spam campaign was themed as the usual Retefe spam mails, we link this campaign to the Retefe gang.

Like Tinba and ExePhish, this campaign didn't last long and the threat actor switched back to Retefe again after a handful of days.

April 2017 – Retefe goes MacOS

Going after Windows users apparently wasn't enough for the Retefe gang. In April 2017, Swiss internet users have seen weird emails hitting their inboxes. Unlike the usual spam emails that clutter internet user's inboxes every day, these emails weren't demanding anything from the user: The email didn't contain any links or attachments the user could click on. However, a short analysis revealed that these emails contained HTML code that would orchestrate the mail client of the recipient to load a tiny 1x1 pixel image from a remote server. In that URL, the recipient's email address was transmitted to the remote server. By this, the sender of these emails could not only determine whether the recipient's email address existed but also track what web browser and operating system the recipient has been using.

The purpose of these tracking emails was unknown, until a large spam campaign has hit Switzerland. What was interesting about this spam campaign was that not all recipients received the same payload: Some received a malicious word with an embedded Java- or PowerShell-script (that turned out to be Retefe), others received a Zip-Archive that turned out to be a - drum roll please - MacOS app. Analysing the macOS app confirmed our assumption: It's a version of Retefe for mac! The very first version we saw, however, has been a Python based RAT called *Bella*. Shortly afterwards, we saw the typical Retefe elements also in the macOS variant: The macOS App (also known as *OSX/Dok*) uses social engineering to convince the victim to enter his administrator password, pretending to be a macOS update. If the victim does so, Retefe will download and install certain components (such as a *Socat* and *Tor*) using *Homebrew*. It uses shell scripts to change the computers settings to make use of a

PAC file and to drop a rogue certificate. The onion domains used for proxy auto-configuration and redirecting the traffic are hardcoded in the binary, slightly obfuscated by XOR (the current key is *0xFF*).


Retefe infecting MacOS (pretending to be a MacOS update)

Retefe infecting MacOS (pretending to be a MacOS update)

MacOS has a security mechanism in place, that only allows Apps to run, which have been signed with a valid code signing certificate (*Developer ID*) issued by Apple. However, it seems not to be a problem for the threat actor to get such a Developer ID.

```
 codesign -dv --verbose=4 PluginUpdate.app

ExecutableE-Ticket.zip/E-Ticket/Dokument.app/Contents/MacOS/AppStore
Identifier=iTunes.AppStore
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20200 size=479 flags=0x0(none) hashes=17+3 location=embedded
OSPlatform=36
OSSDKVersion=657920
OSVersionMin=657664
Hash type=sha1 size=20
CandidateCDHash sha1=d5ddda4165784a16384d2e430de08c2b3b4b9a20
Hash choices=sha1
Page size=4096
CDHash=d5ddda4165784a16384d2e430de08c2b3b4b9a20
Signature size=8522
Authority=Developer ID Application: Efe Idemudie (8R5DFRN5PA)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=11.07.2017, 19:08:34
Info.plist entries=24
TeamIdentifier=8R5DFRN5PA
Sealed Resources version=2 rules=12 files=5
Internal requirements count=1 size=176
```

Please notice that the Developer ID used by the Retefe gang to sign the malware changes frequently to avoid Apple's revocation mechanism (as we usually report those to Apple, once we see new Developer IDs).

Retefe on Android

Recently, some anti-virus companies and newspapers reported that Retefe is distributing the *Signal App* (a secure messenger). Rumours say that the threat actor may use the Signal App as a communication channel with the victim. This is not the case. As a matter of fact, the Signal App is just decoy that the Retefe Gang serves to IP addresses who are not geo located in Switzerland and whose user agent does not correspond to an Android device. If the accessing IP address uses an Android user agent and is geographically located in Switzerland, the APK server will serve an Android trojan that the Retefe gang use to commit e-banking fraud.

The trojan is an *SMS stealer* which allows the threat actor to steal text messages sent by the bank to the customer for two factor authentication (2FA) and transaction signing (so called *mobile TAN* or *mTAN*). To have the victim install the android trojan, the Retefe gang uses social engineering to convince the victim to either enter his mobile phone number where he then receives an SMS from the threat actor with a link to the Android APK, or to scan a QR code displayed by the threat actor in the fake e-banking portal, which also leads to the Android APK. But the Android trojan is more than just an SMS stealer. It is also able to send text messages to other victim's and uses a sophisticated anti VM detection technique. Unlike Retefe itself, which doesn't have any botnet C&C; channel, the SMS stealer has such one. It uses two hard coded botnet C&Cs; which are usually hosted on compromised websites, for example:

```
 url_main="http://frankstain.com/allrent/om/main.php,http://green-cottage.at/wp-admin/main.php"

phone_number=""

download_url="http://dregansa.net/update.apk"
```

Conclusion

As documented, this threat actor has already been around for more than four years. While their tools have changed in the past years, their goal remains the same: committing e-banking fraud in Switzerland and Austria. Their recent expansion to macOS shows that Mac users are not safe from such threats.

The Retefe botnet isn't big: It usually consists out of 100 – 300 infected computers, while Retefe redirects between 10 and 90 e-banking sessions every day. However, it is apparently big enough to generate enough "income" for the attackers. Otherwise the campaign wouldn't have lasted for more than four years now.


Number of victims (IPs) whose e-banking sessions got redirected in the past days

Further reading

GovCERT.ch: e-Banking Trojan Retefe still spreading in Switzerland:
https://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

SWITCH-CERT: Retefe Bankentrojaner:
https://securityblog.switch.ch/2014/07/22/retefe-bankentrojaner/

2nd part of Tinba Malware analysis: The APK side:
http://blog.angelalonso.es/2016/01/2nd-part-of-timba-malware-analysis-apk.html

CheckPoint: OSX Malware is Catching Up, and it wants to Read Your HTTPS Traffic (updated):
https://blog.checkpoint.com/2017/04/27/osx-malware-catching-wants-read-https-traffic/

CheckPoint: OSX/Dok Refuses to Go Away and It’s After Your Money:
https://blog.checkpoint.com/2017/07/13/osxdok-refuses-go-away-money/

Trend Micro: Finding Holes: Operation Emmental:
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

Linking Retefe to OSX.dok:
http://brycampbell.co.uk/new-blog/2017/4/30/retefe-and-osxdok-one-and-the-same

F-Secure: Retefe Banking Trojan Targets Both Windows And Mac Users:
https://labsblog.f-secure.com/2017/07/14/retefe-banking-trojan-targets-both-windows-and-mac-users/

Indicator Of Compromise (IOC)

Following an incomplete list of Retefe IOCs

Citadel (2013 - 2015)

```
 http://abpersonnel.ch/sadcxvbv/vdfbffddf.php
http://abpersonnel.ch/wqwcqqw/sasasacw.php
http://apx.euclid.ch/sadcxvbv/vdfbffddf.php
http://apx.euclid.ch/wqwcqqw/sasasacw.php
http://bromerartcollection.com/sadcxvbv/vdfbffddf.php
http://bsa-informatik.ch/sadcxvbv/vdfbffddf.php
http://coiffurehaargenau.ch/sadcxvbv/vdfbffddf.php
http://designgallery.ch/sadcxvbv/vdfbffddf.php
http://echthaar.com/sadcxvbv/vdfbffddf.php
http://ffupdate.pw/sadcxvbv/vdfbffddf.php
http://ffupdate.pw/wqwcqqw/sasasacw.php
http://files.haewitool.ch/sadcxvbv/vdfbffddf.php
http://floorwash.ch/sadcxvbv/vdfbffddf.php
http://floorwash.ch/wqwcqqw/sasasacw.php
http://gvfm.ch/sadcxvbv/vdfbffddf.php
http://gvfm.ch/wqwcqqw/sasasacw.php
http://homebridge.ch/sadcxvbv/vdfbffddf.php
http://homebridge.ch/wqwcqqw/sasasacw.php
http://hr-consulting-bayern.de/sadcxvbv/vdfbffddf.php
http://hr-consulting-bayern.de/wqwcqqw/sasasacw.php
http://intermountain.ch/sadcxvbv/vdfbffddf.php
http://kinkyfetish.co/wqwcqqw/sasasacw.php
http://lifemeet.biz/p/pages/faq
http://meine7sachen.com/sadcxvbv/vdfbffddf.php
http://meine7sachen.com/wqwcqqw/sasasacw.php
http://moneysyst.biz/p-partner.php
http://mssoft.in.net/sadcxvbv/vdfbffddf.php
http://mssoft.in.net/wqwcqqw/sasasacw.php
```

```
http://plattner-modellbau.ch/sadcxvbv/vdfbffddf.php
http://plattner-modellbau.ch/wqwcqqw/sasasacw.php
http://pornolia.tv/sadcxvbv/vdfbffddf.php
http://schatzmann.info/sadcxvbv/vdfbffddf.php
http://schatzmann.info/wqwcqqw/sasasacw.php
http://sexy-bremen.com/sadcxvbv/vdfbffddf.php
http://sfotware.pw/sadcxvbv/vdfbffddf.php
http://sfotware.pw/wqwcqqw/sasasacw.php
http://shoeshineservice.ch/sadcxvbv/vdfbffddf.php
http://softwareup.pw/sadcxvbv/vdfbffddf.php
http://softwareup.pw/wqwcqqw/sasasacw.php
http://sunnysin.net/sadcxvbv/vdfbffddf.php
http://swarovski.prfact.ch/sadcxvbv/vdfbffddf.php
http://turbo-oergeler.ch/sadcxvbv/vdfbffddf.php
http://vfg-apotheke.at/sadcxvbv/vdfbffddf.php
http://wie-weit.ch/sadcxvbv/vdfbffddf.php
http://wie-weit.ch/wqwcqqw/sasasacw.php
http://www.ansatz.net/sadcxvbv/vdfbffddf.php
http://www.ansatz.net/wqwcqqw/sasasacw.php
http://www.btv.ch/wqwcqqw/sasasacw.php
http://www.buchkeller.ch/sadcxvbv/vdfbffddf.php
http://www.buchkeller.ch/wqwcqqw/sasasacw.php
http://www.ddsafety.ch/sadcxvbv/vdfbffddf.php
http://www.gg-gipser.ch/media/file.php
http://www.mathys-bueromoebel.ch/wqwcqqw/sasasacw.php
http://www.mediset.ch/sadcxvbv/vdfbffddf.php
http://www.naturfreunde-strasshof.at/wqwcqqw/sasasacw.php
http://www.westenberg-engineering.de/sadcxvbv/vdfbffddf.php
http://www.westenberg-engineering.de/wqwcqqw/sasasacw.php
http://www.wohneninsattel.ch/sadcxvbv/vdfbffddf.php
http://aktivteknik.se/sadcxvbv/vdfbffddf.php
http://aktivteknik.se/wqwcqqw/sasasacw.php
http://audiodirekt.se/sadcxvbv/vdfbffddf.php
http://bierischreinerei.ch/sadcxvbv/vdfbffddf.php
http://cubecube.net/sadcxvbv/vdfbffddf.php
http://djonken.se/sadcxvbv/vdfbffddf.php
http://eder-helopal.at/sadcxvbv/vdfbffddf.php
http://garbo.us/sadcxvbv/vdfbffddf.php
http://garbo.us/wqwcqqw/sasasacw.php
http://gourmetfood.se/sadcxvbv/vdfbffddf.php
http://hr-consulting-bayern.de/sadcxvbv/vdfbffddf.php
http://hr-consulting-bayern.de/wqwcqqw/sasasacw.php
http://land-create.com/sadcxvbv/vdfbffddf.php
http://land-create.com/wqwcqqw/sasasacw.php
http://pornolia.tv/sadcxvbv/vdfbffddf.php
http://pre-belmont.ch/sadcxvbv/vdfbffddf.php
http://www.fit-gesund.ch/sadcxvbv/vdfbffddf.php
```

```
http://www.fratelliditalia.ch/sadcxvbv/vdfbffddf.php
http://www.gesund-fit.ch/sadcxvbv/vdfbffddf.php
http://www.pneubucher.ch/sadcxvbv/vdfbffddf.php
http://www.timewaver-vertrieb.ch/sadcxvbv/vdfbffddf.php
```

Retefe Proxy PAC URLs (2014 – 2016)

```
 http://109.234.38.55:8080/proxy.pac
http://141.8.193.12:8080/proxy.pac
http://185.14.28.148:8080/proxy.pac
http://185.14.28.224:8080/proxy.pac
http://50.7.143.68:8080/proxy.pac
http://5.196.200.228:8080/proxy.pac
http://5.196.200.238:8080/proxy.pac
http://5.45.68.98:8080/proxy.pac
http://5.45.70.63:8080/proxy.pac
http://91.215.153.33:8080/proxy.pac
http://95.211.228.182:8080/proxy.pac
https://109.234.34.186/proxy.pac
https://185.14.28.52/proxy.pac
https://185.14.29.179/proxy.pac
https://185.14.29.182/proxy.pac
https://alarm-chek.com/w3check.js
https://alarmtonnel.com/akamaijp.js
https://apps-guard.com/akamaiproxy.js
https://borovpn.net/boropac.js
https://crvvpn.net/secvpn.js
http://securedtunnel.net:8080/akamaihd.js
https://guard-safe.net/a2tunnel.js
https://hsshvpn.net/secureproxy.js
https://openfure.com/openproxy.js
https://puretonnel.net/3desonnel.js
https://safevpn24.net/akamaitehn.js
https://secured-app.net:8969/morioctorici.pac
https://securedtonnel.net/a2stunnel.js
https://securedtunnel.net/akamaihd.js
https://securetonnel.com/3dtonnel.js
https://securevpnalarm.net/secrevpn.js
https://securevpnalarm.net/securevpn.js
https://securevpnhelp.net/securenet.js
https://swissprox.eu/iutirutviucric.js
https://swissprox.eu/iutrutviucric.js
https://tonnelrock.net/tonnel.js
https://vpn-core.net/core.js
https://vpn-core.net/proxy.pac
```

Retefe Android malware domains (2014 – 2016)

```
 app-guard.biz
app-shield.eu
app-sicherheit.net
appsicherheit.net
guardapp.net
guardsapps.2fh.co
guards-apps.com
mobileapp.hostingmyself.com
mobilsicherheit.com
mobilsicherheit.net
secured-apps.com
securedfiles.org
sicherheit-app.net
sicherheitbox.com
sicherheitltd.com
sicherheitplatz.com
sicherheitprog.com
sicherheitsms.net
sicherheit-soft.com
```

Retefe Android App MD5 hashes (2014 – 2016)

```
 041ccd2811fafff84d754a20bd4930f7
0897a2266b8720e90dcae877a895125d
0b09c2605f51b35a0a6bb04f30f41d34
0ba0e7db499cf41a128042faa9a10cdf
0dcdf581e7032620463f2a9f51665d81
0fc96e290aa3b5ec019cb21df8de2ba2
13c9f6efe1796ae744ba73d1ee431398
1dfbd073baac950b58ad1cfaef80288d
25995b64c39457567909020a0dc42929
2afb7868bc432190352abea6c2e6fcfb
2b6c32cc2b3e5328a418be6d5943763d
2bece6af7ecf921642788477a3fa96c3
31f6cd6ca8577c71f358c912c665644a
410031abcb577006b9bbd5eb77cf35a7
4797027dc76ad9a33b43074ed0781a1b
4b0b53b5cbeccfe344663676f74a512f
4b4b0cea52e57abdb93eff659d5608d0
4c438c76756aca3978ce70af8c8efa11
4f1a9ca288c9af69c0851b4794bc2c1e
52268a3f4a716a337a838234f12e0c25
```

```
53dfd780559f149087c26c6649329ca5
57fe9b0c1670f8688133ec2630ca451c
5a4e79c7379a62887ea0090ea98682d2
5e270e43016a4f8140524ca8f94d2617
63cf393fb6bc69ac1e6c0eaa7d01525e
680612395d5d4b2e9f7404dc17f38c57
68095b66ca42b7ccb8a24ce1d0de15d3
6cc6e1d022e7133b36edefda1aefe963
710d23af4d07456fc8e223ac46da0d1a
74e07fa9d4eafdd1016cb840381c8d92
75b1c7f318cc1b7398294a5a9ee56f9b
7bd197019d9e21213278a5b3b477753d
7dbde2dea61a10b1830ff48ce9670b87
81b21f4c1b6958db79635f71a2e59459
884f342171f1990ac1e897721ede6f5e
8960c6d6d3989a98536c040ee59cad02
8b041d7b93e2672447a2d33674a21b61
8d797c59d9818a4a69000d2aaa161323
939eefd1196a3e0f3da6683acb34ad4c
a2f10ec8c7c63efb794900eb09655769
a78356dcc9af798c390d3a30e8b554af
b9a44c954023092dbad59005e3f0e2f5
bc3501dd3138840b179b228b109b9c2d
bc7a217412140d45f6a092043133e131
c1388e193fea2468d17b58a543a384cf
c38a4540f273cffe5903de07a570ed08
cc328d75da7e20953941555bfd377a24
d08aba852856557bcad85169f666f656
d0f47b1e7ccd429f85613d3d07c23e62
d573980fb9c466dbac29083cf6eb8dcc
d8733e9935edf3f59957e6699ead8c98
da43c107149625eb790b97137cfbf0da
e2cc03bc49bbf281dc38e0770da58538
e3526ffc8f36244bba11efaec2728165
e6458652b2b46413e3cb1dd1cfbd11a4
e976329eb0d26e3de2988f476e0000b8
f12b122f4b401c45faf4131a0125b7b5
fa17f3cd3b8c16a4422ad64b0e80aaf5
fa607d6d1d3c9968456c9e657751ad43
ff37117b8b0bdf06038dd0ad033b9861
```

Retefe Android App botnet C&Cs; (2014 – 2016)

```
 http://anman.com/img/main.php
http://bastelfunboard.ch/js/1.php
http://bastelfunboard.ch/js/2.php
```

```
http://bastelfunboard.ch/js/3.php
http://bastelfunboard.ch/js/4.php
http://bildschirm24.com/mainn.php
http://blog.transalpski.ch/wp-admin/1.php
http://blog.transalpski.ch/wp-admin/2.php
http://blog.transalpski.ch/wp-admin/3.php
http://blog.transalpski.ch/wp-admin/4.php
http://chineseschool.at/webcalendar/main.php
http://clubk-ginza.net/css/1.php
http://clubk-ginza.net/css/2.php
http://clubk-ginza.net/css/3.php
http://clubk-ginza.net/css/4.php
http://frankstain.com/allrent/om/main.php
http://green-cottage.at/wp-admin/main.php
http://losbalonazos.
http://losbalonazos.com/wp-admin/1.php
http://losbalonazos.com/wp-admin/2.php
http://losbalonazos.com/wp-admin/4.php
http://naritamemorial.com/analog/1.php
http://naritamemorial.com/analog/2.php
http://naritamemorial.com/analog/3.php
http://naritamemorial.com/analog/4.php
http://proparis.ch/includes/main.php
http://schweizerhof-wetzikon.ch/slides/1.php
http://schweizerhof-wetzikon.ch/slides/2.php
http://schweizerhof-wetzikon.ch/slides/3.php
http://schweizerhof-wetzikon.ch/slides/4.php
http://szaivert-numis.at/standardbilder/dll/1.php
http://szaivert-numis.at/standardbilder/dll/2.php
http://szaivert-numis.at/standardbilder/dll/4.php
http://wd21.plativio.com/neoarts/1.php
http://wd21.plativio.com/neoarts/2.php
http://wd21.plativio.com/neoarts/3.php
http://wd21.plativio.com/neoarts/4.php
http://www.buildingforsale.eu/statistik/mainn.php
http://www.lebensbau.de/Resources/main.php
http://www.medianetwork.li/wpimages/wpb7b63588.php
http://www.vanca.com/media/1.php
http://www.vanca.com/media/2.php
http://www.vanca.com/media/3.php
http://www.vanca.com/media/4.php
http://www.villadora.ch/wpimages/a3b92ef92f58.php
```

Retefe MacOS MD5 hashes (2017)

```
 8919044ccd162034fb79a4ee30157c6d
191b6fd69c1e59ded0a433a3c290af82
e8dcf3bdc00f5f749e4a8d4286596ded
c0d91f2438561a24b8faac2884dccb9a
13c0f5d4ffe0d553e41cdb76398bf13a
1fc9908c82e00f685539914681da4342
29c4ecb3b3ff375681a5608452d21c9d
e3cee47e6c6bd873d53ddac5ade211fc
821b4927d746cc0447d8b9cc2692ff7b
b452df1c9b8663b433252a9bda8ca37b
908794f38668c04d2f8d01c7a11b230d
85e7e699c90b29718956d0313d08c3a7
```

Back to top

Source: https://web.archive.org/web/20230401011457if_/https://www.govcert.ch/blog/the-retefe-saga/