94 .ch & .li domain names hijacked and used for drive-by

securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/

July 7, 2017

A Swiss domain holder called us today telling us that the .ch zone points to the wrong name servers for his domain.

The NS entries were ns1.dnshost[.]ga and ns2.dnshost[.]ga. We contacted the registrar and soon realized that this is not the only domain that had unauthorized changes. We identified 93 additional .ch and .li domain names that pointed to the two rogue name servers. While domain hijacking by pointing to a rogue NS is a known attack, 94 domains on a single day is very unusual. So we analyzed what the hijacked domains were used for and soon found out that they are used to infect internet users with malware.

Visitors to the hijacked domains were redirected to the Keitaro TDS (traffic distribution system):

```
hXXp://46.183.219[.]227/VWcjj6
```

A TDS decides where to redirect the visitor to, often depending on its IP address (i.e. country),
user agent and operating system.

A dead end may look like the following:

```
hXXp//46.183.219[.]227/favicon.ico
hXXp://46.183.219[.]227/www.bingo.com
```

And the visitor will be redirected to Google.

However, in some cases, the visitor is redirected to the Rig Exploit Kit:

```
hXXp://188.225.87[.]223/?doctor&news=...&;money=...&cars=236&medicine=3848
hXXp://188.225.87[.]223/?health&news=...
...
```

And the visitor gets infected.

The payload is Neutrino Bot:

```
MD5: a32f3d0a71a16a461ad94c5bee695988
SHA256: 492081097c78d784be3996d3b823a660f52e0632410ffb2a2a225bd1ec60973d).
```

It gets in touch with its command and control server and grabs additional modules:

```
hXXp://poer23[.]tk/tasks.php
hXXp://poer23[.]tk/modules/nn_grabber_x32.dll
hXXp://poer23[.]tk/modules/nn_grabber_x64.dll
```

A little later, it also gets an update

```
hXXp//www.araop[.]tk/test.exe

MD5: 7c2864ce7aa0fff3f53fa191c2e63b59
SHA256: c1d60c9fff65bbd0e3156a249ad91873f1719986945f50759b3479a258969b38)
```

Status

The rogue NS were inserted in the .ch zone file at around 13:00 today. The registrar discovered soon what happened and rolled back the unauthorized changes. At 16:00 all of the changes in the .ch & .li zone were reverted and the NS records pointed to the legitimate name servers again.

[Update 10.7.17 17:15]

Gandi the registrar of the 94 domain names has written a blog post, as well as SCRT the domain holder that initially informed us about the domain name hijacking of scrt.ch. SCRT also showed how Strict Transport Security protected their recurring visitors from being redirected to the bogus website!

Author: Michael Hausding

Competence Lead DNS & Domain Abuse at SWITCH the ccTLD registry for .ch & .li View all posts by Michael Hausding

16 thoughts on “94 .ch & .li domain names hijacked and used for drive-by”

Comments are closed.