Who To Sue If Skype Spam Kills You

Justus Perlwitz

2015-09-10

Contents

1 A Trail of 302s **1**

2 The Fake Magazine **2**

3 Who is behind it? **2**

The other day I received this ominous message on Skype from an infected machine:

```
http://octavo.in/v/yx7vj.php?liveID=[myskypeusername]
```

1 A Trail of 302s

The URL redirects to `http://professtanitim.com` (with a revealing WHOIS record), which just serves this mysterious JavaScript:

```
<script type="text/javascript">
function generate(len)
{
// generates a random string with length len
}

function rand(min, max)
{
// random int >min and <max
}

var urls =
[
'com-n7d.net/?a=311397&c=wl_con&', // These two
'com-3fg.net/?a=311397&c=wl_con&' // are owned by a resident of Shandong
];

redir ='http://'+generate(rand(5,10))+'.'+urls[rand(0, urls.length-1)]+generate(rand(5,10));

parent.location.href = redir;
//-->
```

Even in Shandong, programmers like the K&R indent style. Let's try one of these random URLs:

```
curl -Lv 'http://fuckyou.com-n7d.net/a=311397&c=wl_con&assholes'
[...]
< HTTP/1.1 302 Found
[...] # Gasp! Another redirect
< Location: http://com-zau.net/?a=311397&c=wl_con
[...] # The domain is owned by the same Shamdong individual
```

```
< HTTP/1.1 302 Found
[...] # Gasp! Another redirect
< Location: http://277-beauty.com-zau.net/dekedj/womenshealth/
[...] # Same host
< HTTP/1.1 200 OK
< Server: nginx
< X-Powered-By: PHP/5.3.28 # old, grumpy PHP version
[...]
```

2 The Fake Magazine

Fake *Women's Health magazine* article

The article seems to cater to insecure women that are desperately trying to lose weight and are thus easy bait for weight loss drug scammers. In it, two drugs are being promoted: **Garcinia Cambogia + Pure Life Cleanse**, AKA Pure Wallet Cleanse, amirite??!

3 Who is behind it?

Let's see whether we can find out which company is selling these weight loss drugs.

After sifting through the order page that is linked on the fake article, one can quickly see that a company called BioTrim Labs owns the product. The redirect path there is interesting: It goes through another host name `vikingtrck.com` which runs `Microsoft-IIS/7.5`. Now, we all know what IIS stand for: Level 10 CVE. Not only do these scammers hardly cover up their WHOIS records, their server infrastructure is vastly outdated.

Now, when you try to look up BioTrim labs at a UK, US or Germany company registry, it does not turn up. So this is where the trail ends. I have no idea who you should sue once your intestines turn into jello.