BIG BANG THEORY OF CVE-2012-4792

Jindrich Kubec, Eric Romang
AVAST Software, Czech Republic

Email kubec@avast.com / eric.romang@mac.com

ABSTRACT

This presentation will detail a forensic and detective model that describes the early development of the watering hole campaign that was mostly active from December 2012 to January 2013, mainly targeting energy industries, governments, non-profit organizations and human rights websites. After the initial targeted attack, the vulnerability cooled sufficiently to allow integration in different confidential or public exploit kits. We will try to observe the most distant things that a security researcher can see. Also the timeline of the attacks, together with the disclosure, detection and publication dates will be presented.

1. INTRODUCTION

The 27 December 2012, *The Washington Free Beacon* published a newspaper article [1] mentioning that ***Council on Foreign Relations*** (CFR.org), a foreign policy web group, had been victim of a targeted attack who seem to be linked to computer hackers traced to China.

Regarding published information's, compromised CFR website was used to attack visitors in order to extract valuable information's. The attack, described as "*drive-by*", or "*watering hole*", was detected around 2:00pm on Wednesday 26 December and CFR members who visited the website between Wednesday and Thursday could have been infected and their data compromised.

The newspaper article also mentioned that only Internet Explorer 8 and higher versions had been targeted and that a zero-day was used to infect visitor's computers. Attack was limited to CFR members and website visitor's who used browsers configured for Chinese language characters.

Now, with hindsight, we can provide a better view of the facts and the related timing with this attack and with the Internet Explorer zero-day, also known as CVE-2012-4792.

Just as the theory of the expanding universe, we can divide the life cycle of the attack and the vulnerability in four phases.

The first phase, called "*Very Early Phase*", will describe, and provide additional information's, on the "*watering hole*" attack. We will analyze the timeline, the singularities of this attack and try to link this attack to linked or previous campaigns.

The second phase, called "*Early Phase*", will describe, and provide additional information's, on the early stages of the attack just after his public discovery, Metasploit integration, Exodus Intelligence fork and emergence of a variant called "DWORD".

The third phase, called "*Structure Formation Phase*", will present the derivate "*watering hole*" campaigns with they're associated code forks.

The fourth and last phase, called "*Ultimate Fate Phase*", provide focus on integration of CVE-2012-4792 into exploit kits.

2. VERY EARLY PHASE

This first phase will describe, and provide additional information's, on the "*watering hole*" attack. We will analyze the timeline, the singularities of this attack and try to link this attack to linked or previous campaigns. We can consider that the "*Very Early Phase*" started around the 7 December and finished the 27 December when the attack was publicly disclosed.

2.1 Initial Evidences Gathering

As mentioned in the introduction, the "*watering hole*" attack, and associated Internet Explorer zero-day, was publicly disclosed the 27 December in newspaper article with some reference dates.

Wednesday 26 December is mentioned as the incident discovery, but the article also seems to mention this date as the start date of the attack. Thursday 27 December is mentioned as the incident closure, CFR website cleanup and end of the attack.

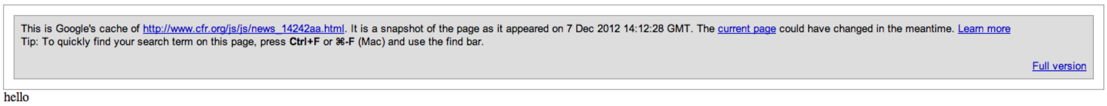
By doing investigations, on different online sandboxes and search engines, we can provide a different version of the incident timeline, on the vulnerability behaviors and relationships with previous campaigns.

On **urlQuery.net** [2], we can observe that a submission was done, the 21 December. This submission refer to "*/js/js/news_123432476.html*" URL and involved the usage of "*deployJava.js*" script that provide functions for web pages to detect the presence of a JRE, install the latest JRE, and easily run applets or Web Start programs.

Other urlQuery.net submissions, from the 27 December, were interesting, like "*/js/js/robots.txt*", "*/js/js/today.swf*", "*/js/js/news_435435s.html*". You can observe that the HTML page has a different name than the firstly discovered.

On **CLEAN MX** [3], we can observe that a submission was done the 20 December and closed the 21 December.

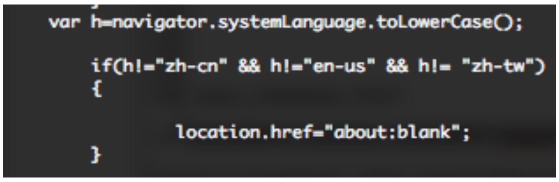
In **Google** cache, we found a snapshot of "*/js/js/news_14242aa.html*" as it appeared on 7 December. The Google cache snapshot provided us the ability to analyze part of the source code of the attack. You can observe that the HTML page has a different name than two previously discovered.



This is Google's cache of http://www.cfr.org/js/js/news_14242aa.html. It is a snapshot of the page as it appeared on 7 Dec 2012 14:12:28 GMT. The current page could have changed in the meantime. Learn more
Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

hello

Code version of 7 December provides interesting singularities. *The Washington Free Beacon* newspaper article mentioned that only visitor's who used browsers configured for Chinese language characters were targeted. The code demonstrated that also visitors who used browsers configured for English US language characters were targeted.



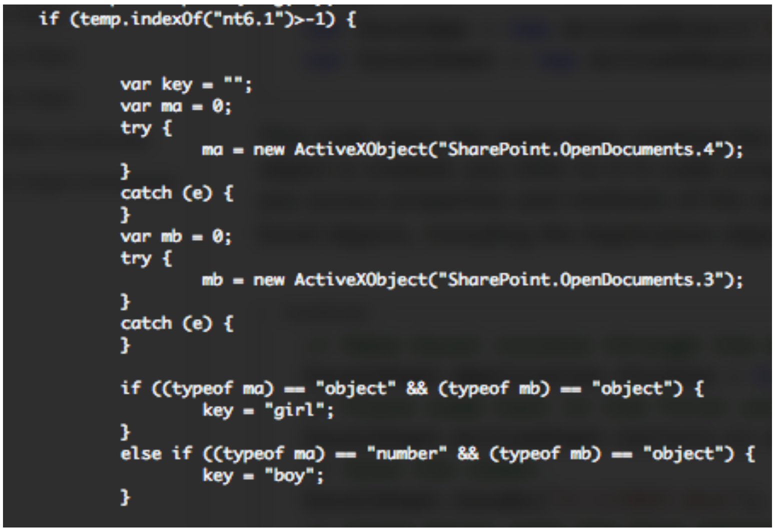
```
var h=navigator.systemLanguage.toLowerCase();

    if(h!="zh-cn" && h!="en-us" && h!= "zh-tw")
    {

            location.href="about:blank";
    }
```

Also the code was executing a XML HTTP request to "*xsainfo.jpg*" file. Submissions, of 13 December, found on VirScan [4] and VirusTotal [5] (*320e0729e1a50fd6a2aebf277cfcad66*) were potentially linked to this file.

Two different technics of Windows ASLR and DEP bypasses were used. The first technic is the traditional Java 6 non-ASLR *msvcr71.dll* library usage. The second technic is a Microsoft Office vulnerability discovered and publicly disclosed by GreyHatHacker.Net [6], the 24 August 2012. This vulnerability wasn't patched at the date of the CFR "*watering hole*" attack.



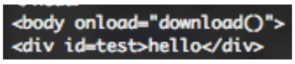
```
if (temp.indexOf("nt6.1")>-1) {


        var key = "";
        var ma = 0;
        try {
                ma = new ActiveXObject("SharePoint.OpenDocuments.4");
        }
        catch (e) {
        }
        var mb = 0;
        try {
                mb = new ActiveXObject("SharePoint.OpenDocuments.3");
        }
        catch (e) {
        }

        if ((typeof ma) == "object" && (typeof mb) == "object") {
                key = "girl";
        }
        else if ((typeof ma) == "number" && (typeof mb) == "object") {
                key = "boy";
        }
```

FireEye [7], published the 28 December, additional details on the attack who revealed other singularities. It appears that the FireEye sample only served the exploit to browsers whose operating system language was either English (U.S.), Chinese (China), Chinese (Taiwan), Japanese, Korean, or Russian.

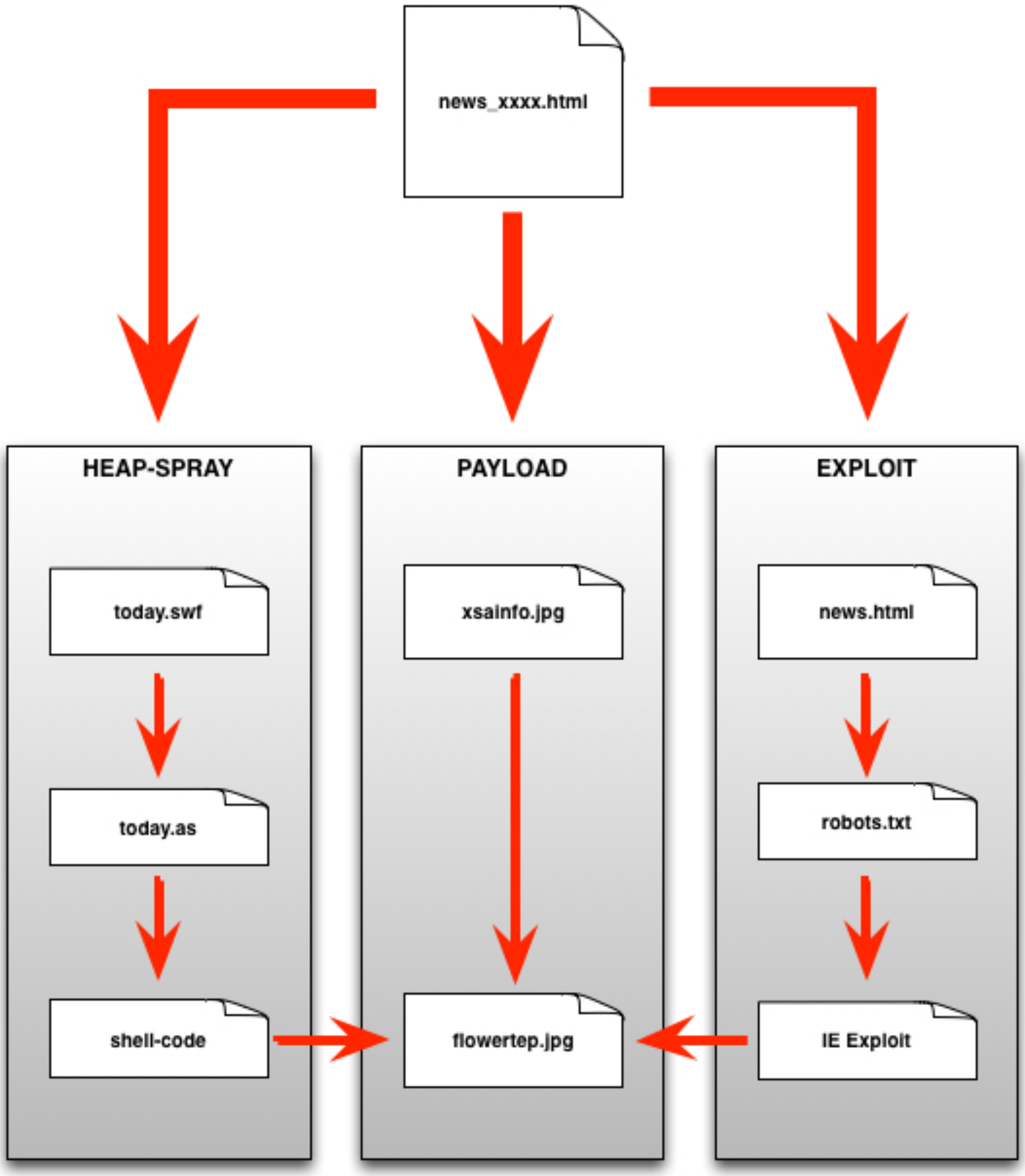
Also we noticed that the gathered sample, a "*hello*" text was hidden or not.



```
<body onload="download()">
<div id=test>hello</div>
```

All these singularities have made us believe that multiple variations of this attack occurred, as it looks like the attackers changed tactics multiple times during the attack. Also it clearly appeared that the "*watering hole*" attack hadn't started the 26 December but at least the 7 December.

2.2 Steps in CVE-2012-4792 CFR code



<u>Step 1:</u> *news_xxx.html* load malicious Flash *today.swf* file, which is responsible for the heap-spray. The Flash file contained ActionScript code, which was used to build shell-code based on the operating system version, and language packs installed.

<u>Step 2:</u> In parallel, a GET request was made to download xsainfo.jpg file that was stored in Internet Explorer Temporary Internet Files. When the Flash was loaded, a heap-spray was performed and injected the shell-code to locate *xsainfo.jpg* file, decode it, and stored it in *%TEMP%/flowertep.jpg* payload.

<u>Step 3:</u> Also in parallel, *news_xxx.html* load *news.html* page, which download *robots.txt* file containing the exploit, code for Internet Explorer 8. *robots.txt* file was de-obfuscated and then used to load *flowertep.jpg* payload by using DEP and ASLR bypass technics.

2.3 Reverse Chronology

Based on the gathered samples and evidences, it was quiet easy for us to discover that CFR was not the only “*watering hole*” website involved in the “*Very Early Phase*” of what we can call now a campaign. At minimum eight websites were involved in this campaign phase.

Website	Website Type	Country	Sample Date	Sample Collec.
www.cfr.org	Think Tank	US	2012/12/07	2012/12/07
get.adobe-server.com	Hosting Website	IN	2012/12/12	2013/01/08
www.hnbc123.com	Political Dissident	CN	2012/12/13	2013/01/11
www.alljap.net	Hosting Website	AU	2012/12/14	2013/01/13
goddess.nexon.com.au	IT and Communications	AU	2012/12/17	2013/01/06
pqtools.eaton.com	IT and Communications	AU	2012/12/17	2013/01/06
www.capstoneturbine.com	Energy Manufacturer	US	2012/12/18	2012/12/18
173.224.221.166	Hosting Website	US	2012/12/19	2013/01/02

By doing an analysis of the behaviors of the landing pages, we can confirm that the “*attackers*” changed tactics multiple times.

Website	Targeted languages						Visible	Java	Office
	zh-cn	zh-tw	en-us	ja	ru	ko	“*hello*” text	ASLR	ASLR
www.cfr.org - 12/7	X	X	X				X	X	X
get.adobe-server.com	X	X	X				X	X	X
www.hnbc123.com							X	X	X
www.alljap.net	X	X	X	X	X			X	X
goddess.nexon.com.au	X	X	X	X	X			X	X
pqtools.eaton.com	X	X	X	X	X			X	X
www.capstoneturbine.com	X	X	X				X	X	X
173.224.221.166	X	X	X	X	X			X	X
www.cfr.org - 21/12	X	X	X	X	X	X		X	X

Analysis of the payloads:

Website	Payload MD5	Name	Size	Time Stamp
www.cfr.org	9a63f72911b385a0c17427444c968ed0	test_gaga.dll	497.5 KB	2012/12/07
www.cfr.org	715e692ed2b48e455734f2d43b936ce1	test_gaga.dll	497.5 KB	2012/12/12
get.adobe-server.com	cd1fdc800ffe6b4effc34e0662f66259	test_gaga.dll	497.5 KB	2012/12/07
get.adobe-server.com	f20e667cf3f093b4cfe83ed719d30728	test_gaga.dll	497.5 KB	2012/12/07
www.hnbc123.com	45968d85957844f3d8195042a9c3e780	test_gaga.dll	309.5 KB	2012/12/12
www.hnbc123.com	b68c90c28283ce3ace86f445485e4396	dxdiag.exe	191.5 KB	2012/06/05
www.alljap.net	b30eb3a53002f73dc60ca5c283a894d2	test_gaga.dll	497.5 KB	2012/12/12
goddess.nexon.com.au	5bca1a86c15816f3fc61db1ae807bdca	test_gaga.dll	497.5 KB	2012/12/12
pqtools.eaton.com	d1a0a403533b1cc7b7973b5bc3108af3	test_gaga.dll	497.5 KB	2012/12/12
173.224.221.166	74fa8ec55482ca81b41dfd356af9b187	test_gaga.dll	497.5 KB	2012/12/12

Related C&C servers:

Payload MD5	C&C	C&C IP	Country
9a63f72911b385a0c17427444c968ed0	web.vipreclod.com	23.19.217.15	US
715e692ed2b48e455734f2d43b936ce1	provide.yourtrap.com	50.62.12.103	US
cd1fdc800ffe6b4effc34e0662f66259	N.A.	N.A.	N.A.
f20e667cf3f093b4cfe83ed719d30728	support.ayuisyahooapis.com	122.199.194.197	KR
45968d85957844f3d8195042a9c3e780	www.hnbc123.com	216.24.199.252	US
b68c90c28283ce3ace86f445485e4396	w3.changeip.org	N.A.	N.A.
b30eb3a53002f73dc60ca5c283a894d2	gewasi.strangled.net	182.237.3.58	HK
5bca1a86c15816f3fc61db1ae807bdca	services.darkhero.org	208.115.242.35	US
d1a0a403533b1cc7b7973b5bc3108af3	wordpress.blackcmd.com	208.115.242.36	US
74fa8ec55482ca81b41dfd356af9b187	mail-news.eicp.net	46.37.173.145	GB
74fa8ec55482ca81b41dfd356af9b187	ras-ru.oicp.net	46.37.173.145	GB
74fa8ec55482ca81b41dfd356af9b187	mail-ru.3322.org	173.224.221.166	US

Here under all the mapping between the "*infected*" sites to "*distribution*" servers involved in the "*watering hole*" campaign.

"*Infected*" Website	"*Infected*" Website Type	"*Infected*" Hosting Country	"*Distribution*" Server
www.cfr.org	Think Tank	US	www.cfr.org
www.tibet.net	Tibetan	US	get.adobe-server.com
www.hnbc123.com	Political Dissident	US	www.hnbc123.com
www.gbn.com	Consulting	US	www.alljap.net
goddess.nexon.com.au	IT and Communications	AU	goddess.nexon.com.au
pqtools.eaton.com	IT and Communications	AU	pqtools.eaton.com
			goddess.nexon.com.au
www.capstoneturbine.com	Energy Manufacturer	US	www.capstoneturbine.com
ecology-hs.muctr.ru	Research Institution	RU	173.224.221.166
kgu.muctr.ru	Research Institution	RU	173.224.221.166
kvm.muctr.ru	Research Institution	RU	173.224.221.166
nano.muctr.ru	Research Institution	RU	173.224.221.166
www.nsc.ru	Research Institution	RU	173.224.221.166
biomaterialscenter.muctr.ru	Research Institution	RU	173.224.221.166

2.3.1 www.cfr.org chapter

CFR website was compromised at least the 7 December with the purpose to infect certain visitors of the website. The "*attackers*" rapidly changed the payloads and they're tactics during the attack, in order to probably respond to new objectives.

web.vipreclod.com C&C server (23.19.217.15 – AS15003), associated to the first payload (*9a63f72911b385a0c17427444c968ed0*) , was referenced by Microsoft Malware Protection Center [8] the 16 December and also mentioned by AhnLab [9] few days after the public disclosure of the incident. *vipreclod.com* was registered the 10 December 2012. Despite the compilation time stamp of the payload, he wasn't able to contact the C&C server until the 10 December.

The second payload (*715e692ed2b48e455734f2d43b936ce1*), having *provide.yourtrap.com* as C&C server (50.62.12.103 – AS26496), was firstly mentioned by FireEye [7] the 28 December. We can suppose, that the second payload was used between the 12, or 16, December until the discovery of the incident.

2.3.2 get.adobe-server.com chapter

get.adobe-server.com server was compromised at least the 12 December with the purpose to be a "*distribution*" server. Central Tibet Administration (*www.tibet.net*) website is the only website we found using *get.adobe-server.com* server as a distribution server.

adobe-server.com domain name was created the 23 August 2012, and *get* sub-domain was hosted on 121.241.248.9 (AS4755) in India. All the hosted malicious files were dated from the 12 December and the payloads have all compilation timestamp from the 7 December.

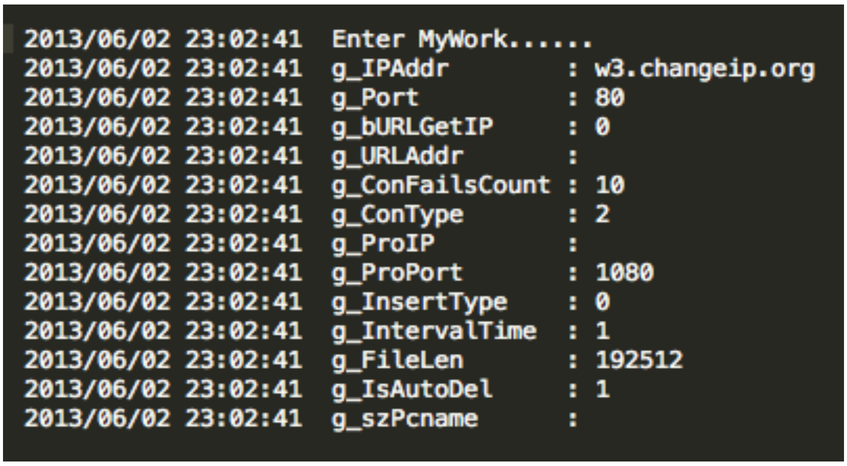
C&C server, *support.ayuisyahooapis.com*, hosted on 122.199.194.197 (AS17877) was seen the 2 August 2012 in a ThreatExpert submission [10] and discovered the 20 December by Symantec [11]. Computer Incident Response Center Luxembourg (CIRCL) also mentions [12] *support.ayuisyahooapis.com* domain name in a PlugX variant discovered exploited in a March 2013 incident. This incident has involved a United-States global information company who was victim of a targeted attack through a Java exploit.

Surely this hosting website was used in a "*drive-by*" attack, but the original compromised website is actually

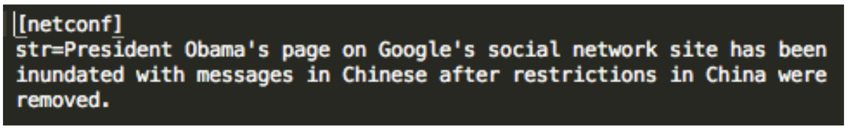
2.3.3 www.hnbc123.com chapter

www.hnbc123.com website was compromised at least the 12 December with the purpose to infect visitors of the website. The "*attackers*" didn't change the payloads and they're tactics during the attack, no specific languages have been targeted. The first payload was downloading and executing the second one. The potential reason is that this website has been used to target worldwide political dissidents, but this is only speculation.

Second payload (b68c90c28283ce3ace86f445485e4396), a KeyLogger, is interesting because he contains the string "*President Obama's page on Google's social network site has been inundated with messages in Chinese after restrictions in China were removed.*". This string was firstly discovered by nProtect [13] the 2 August 2012 in a "*config.ini*" file of a Keylogger used in targeted attacks, dropped by a HWP zero-day exploit, against South-Korean governmental agencies. The gathered sample has the same structure as the own mentioned by nProtect.



```
2013/06/02 23:02:41  Enter MyWork......
2013/06/02 23:02:41  g_IPAddr        : w3.changeip.org
2013/06/02 23:02:41  g_Port          : 80
2013/06/02 23:02:41  g_bURLGetIP     : 0
2013/06/02 23:02:41  g_URLAddr       :
2013/06/02 23:02:41  g_ConFailsCount : 10
2013/06/02 23:02:41  g_ConType       : 2
2013/06/02 23:02:41  g_ProIP         :
2013/06/02 23:02:41  g_ProPort       : 1080
2013/06/02 23:02:41  g_InsertType    : 0
2013/06/02 23:02:41  g_IntervalTime  : 1
2013/06/02 23:02:41  g_FileLen       : 192512
2013/06/02 23:02:41  g_IsAutoDel     : 1
2013/06/02 23:02:41  g_szPcname      :
```



```
[netconf]
str=President Obama's page on Google's social network site has been
inundated with messages in Chinese after restrictions in China were
removed.
```

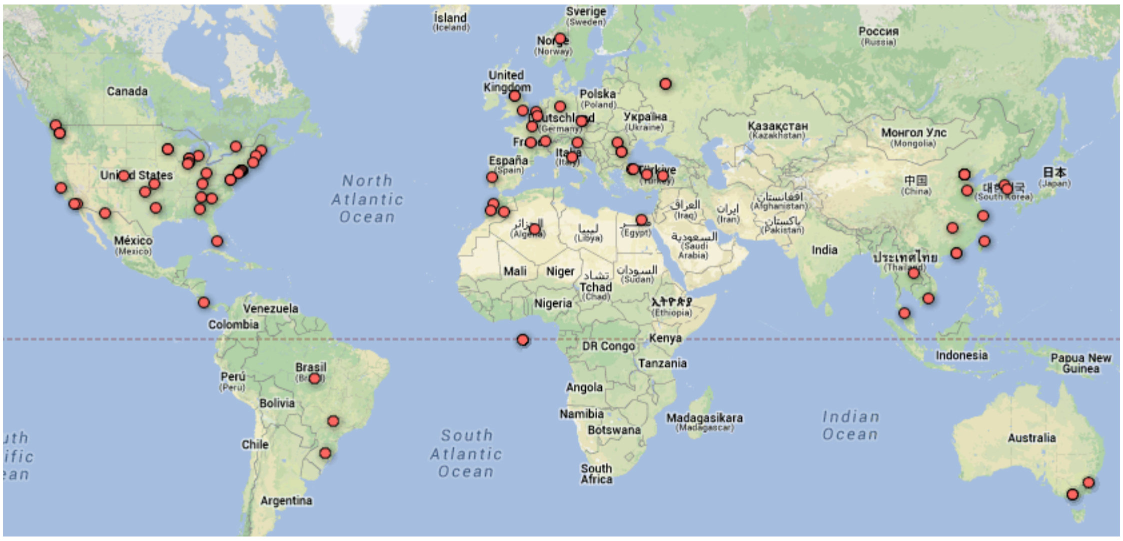
2.3.4 www.alljap.net chapter

www.alljap.net server was compromised at least 14 December with the purpose to be a "*distribution*" server.

Hopefully we did have access to the web logs of the server and had the possibility to do a complete analysis of the "*attackers*" behaviors. Eric Romang posted a complete blog post [14] regarding this chapter. Here under a resume of all the founded evidences.

www.alljap.net server was used in as a "*distribution*" server in a drive-by campaign since the 7 December. *www.gbn.com* website is the only website we found using *www.alljap.net* server as a distribution server.

"*Attackers*" accessed *www.alljap.net* server through a PHP backdoor and modified the code multiple times from the 7 to 14 December. "*Attackers*" sessions on the server were limited to 20 minutes because they used FlyVPN.com free trial accounts that are limited to 20 minutes. FlyVPN.com VPN gateways were located in South-Korea, Taiwan and Hong-Kong. Victims of this attack were also worldwide.



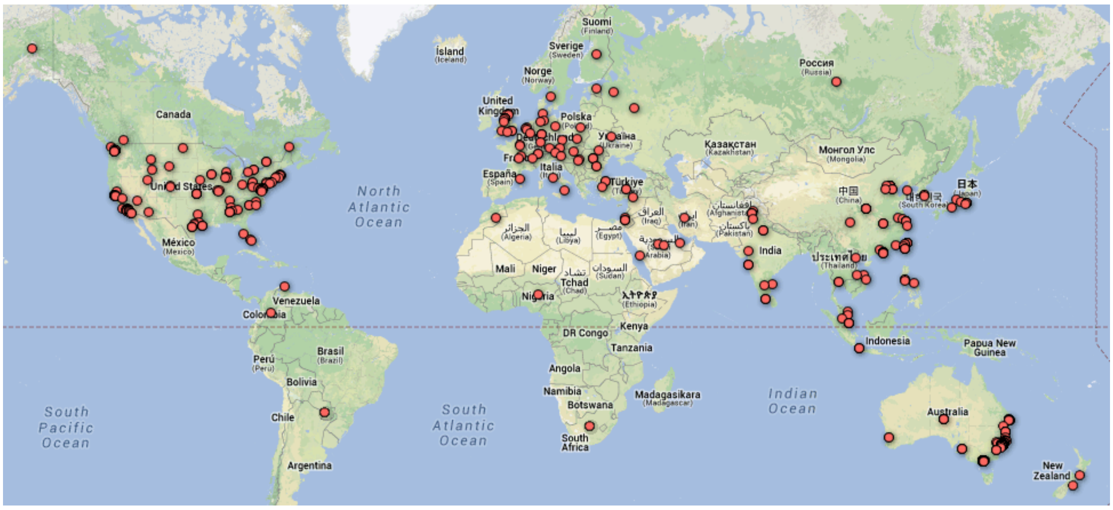
We share with you all the data's related to *www.alljap.net* chapter through Google Fusion Tables. The first Fusion Table [15] represents all the hits independent of the browser and browser version. The second Fusion Table [16] represents all the Microsoft Internet Explorer 8 hits.

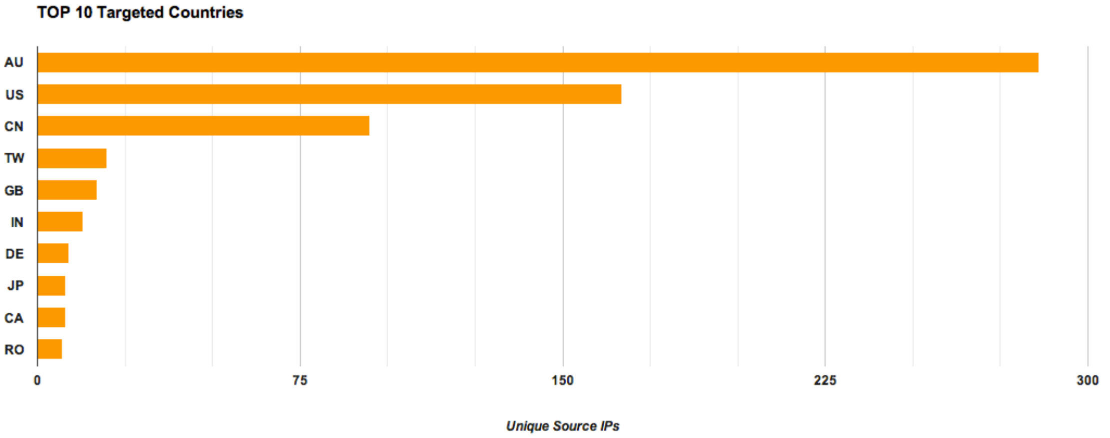
C&C server gewasi.strangled.net, a subdomain of a free DNS provider, was hosted on 182.237.3.58 (AS24544) in Hong-Kong.

2.3.5 goddess.nexon.com.au chapter

goddess.nexon.com.au server was compromised at least the 17 December with the purpose to be a "*distribution*" server. It is actually unclear which other websites were compromised to use this distribution server. We only now that the main website of Nexon Asia Pacific, an Australian IT and Communications company was the compromised server.

Hopefully we did have access to the web statistics that were freely accessible from Internet. Based on these data's we could confirm that the "*drive-by*" attack has started the 17 December. Victims of this attack were also worldwide.





We share with you all the data's related to *goddess.nexon.com.au* chapter through a Google Fusion Tables. The Fusion Table [17] represents all the hits independent of the browser and browser version.

C&C server *services.darkhero.org* was hosted on 208.115.242.35 (AS46475) in United-States.

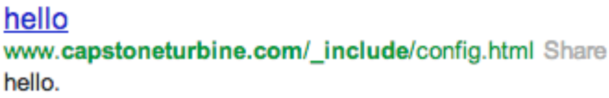
2.3.6 pqtools.eaton.com chapter

pqtools.eaton.com server was compromised at least the 17 December with the purpose to infect visitors of the website.

C&C server *wordpress.blackcmd.com* was hosted on 208.115.242.36 (AS46475) in United-States. As you can see this C&C server was adjacent to the C&C server of *goddess.nexon.com.au*.

2.3.7 www.capstoneturbine.com chapter

We found, through Google cache, a sample proving that *www.capstoneturbine.com* was compromised at least the 18 December with the purpose to infect visitors of the website. Unfortunately we didn't have access to the payload.

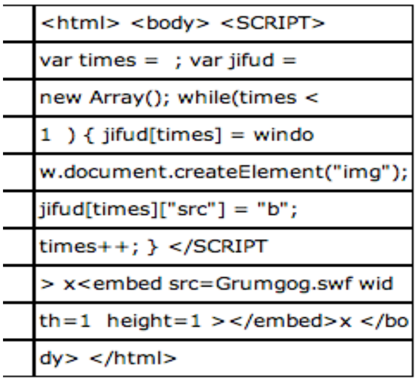


hello

www.capstoneturbine.com/_include/config.html Share

hello.

By doing further investigations, we found a CLEAN MX submission [18] , from the 19 September and the gathered sample clearly refers to a previous "*watering hole*" campaign that was related to CVE-2012-4969 Internet Explorer zero-day.



```
<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>
```

2.3.8 173.224.221.166 chapter

173.224.221.166 server was used in as a "*distribution*" server in a drive-by campaign since at least the 19 December. Six Russian websites were found using *173.224.221.166* server as a distribution server. These websites were all related to environmental, physical, chemical and macro technology universities or schools.

The payload contacted three C&C serves. *ras-ru.oicp.net* C&C server was known since 29 June 2012 through a ThreatExpert submission [19].

2.4 Links with other campaigns

2.4.1 Targeted Once Targeted Forever

Through *www.capstoneturbine.com* chapter, we can observe that the website was compromise to spread CVE-2012-4792 during the December "*watering hole*" campaign, but also used to spread CVE-2012-4969 during the September "*watering hole*" campaign. Capstone Turbine administrators didn’t have correct they’re security holes and the “*attackers*” have take advantage of this weakness.

2.4.2 Reusable C&C Servers & Domain Names

Payload dropped from *get.adobe-server.com* (*f20e667cf3f093b4cfe83ed719d30728*) used *support.ayuisyahooapis.com* as C&C server, a domain name also present in an August 2012 malware (*99baa58ce02872016b4ad25d2deef36e*).

support.ayuisyahooapis.com domain name was also discovered, in March 2013, in a payload (*f1f48360f95e1b43e9fba0fec5a2afb8*) dropped by a Java exploit. This incident involved a United-States global information company.

Payload dropped from *173.224.221.166* (*74fa8ec55482ca81b41dfd356af9b187*) used *ras-ru.oicp.net* as C&C server, a domain name also present in a June 2012 malware.

2.4.3 Reusable Malware

Key Logger (*b68c90c28283ce3ace86f445485e4396*) dropped from www.hnbc123.com has the same structure as the Key Logger found used in targeted attacks against South-Korean governmental agencies.

2.4.4 Reusable Code Structure

As you may remember CVE-2012-4792 used a Flash SWF file “*today.swf*” in order to perform the heap spray and setting up the shell code. Same technic was used for CVE-2012-1875 (Microsoft Internet Explorer zero-day of May 2012), for CVE-2012-1889 (Microsoft XML Core Services zero-day of June 2012) and for CVE-2012-4969 (Microsoft Internet Explorer zero-day of September 2012).

As reported by Symantec [20], in a January 2013 blog post, “*today.swf*” shared same symbols with the previous zero-days like “*HeapSpary*”, “*hexToBin*” and “*OS_Version*”.

Filename	**CVE**	**Common symbols**				
		HeapSpary	**hexToBin**	**OS_Version**	**URL_Addr**	**Flahs_Version**
Geoffrey.swf	2012-1875	Yes	Yes	Yes	Yes	Yes
Moh2010.swf	2012-4969	Yes	Yes	Yes	Yes	Yes
Today.swf	2012-4792	Yes	Yes	Yes	No	No

We can also find some others interesting similarities, for examples:

- CVE-2012-1875 has “***Man****And****Woman****()*” function and CVE-2012-4792 has “*key ==* "***girl***"*"*” and “*key ==* "***boy***"*"*” variables.
- CVE-2012-1875 has “**var xbc**=*vbc.replace(/NewYoukv/g,"%u");*” and CVE-2012-1889 has “**var xbc**=*ConVertData(mmmbc["\x72\x65\x70\x6c\x61\x63\x65"](/Data/g,"%u"));*”

2.5 Very Early Phase Conclusion

During “*Very Early Phase*” the “*attackers*” changed they’re tactics and they’re target objectives multiple times. Primary victim was CFR.org, an US think tank that provides foreign policy and foreign affairs resources to government officials, journalists, and business and education leaders. But it looks like that Russian’s research institutions were the most affected during this “*watering hole*” campaign. Links with previous campaigns could clearly be established but without to certify that authors were the same.

3. EARLY PHASE

This second phase will describe, and provide additional information's, on the early stages of the attack just after his public discovery, Metasploit integration, Exodus Intel fork, to emergence of a variant called "DWORD".

As mentioned in the previous phase the vulnerability was officially "*discovered*" exploited in the wild the 26 December 2012 on Council on Foreign Relations (CFR.org) web site. We can consider that the "*Early Phase*" started the 27 December, date of the attack public disclosure, and finished the 2 January when Exodus Intel published a fork of the vulnerability.

In order to better distinguish the different codes we will name the original code "CFR" and a variant of the exploit "DWORD".

3.1 Reverse Chronology

During this phase the initial campaign still continued and we detected only three additional websites with the original code sample.

Website	Website Type	Country	Code Type	Sample Date
www.philam.com.tw	Travel Agency	TW	CFR	2012/12/27
www.uygurunsesi.com	Uyghur Dissident	TR	CFR	2012/12/27
homeweb.zzl.org	Hosting Website	US	DWORD	2013/01/01

We can observe that the landing pages were targeting all potential languages, like the *www.cfr.org* code version of 21 December. But the landing pages wasn't using Microsoft Office ASLR bypass anymore, just the traditional Java 6 non-ASLR *msvcr71.dll* library.

Website	Targeted languages						Visible "*hello*" text	Java ASLR	Office ASLR
	zh-cn	zh-tw	en-us	ja	ru	ko			
www.philam.com.tw	X	X	X	X	X	X		X	
www.uygurunsesi.com	X	X	X	X	X	X		X	
homeweb.zzl.org	X	X	X	X		X		X	

Analysis of available payloads:

Website	Payload MD5	Name	Size	Time Stamp
www.uygurunsesi.com	3de45412b9aeea37e578d9d3c4b364c3	test_gaga.dll	497.5 KB	2012/12/12

Related C&C servers contacted:

Payload MD5	C&C	C&C IP	Country
3de45412b9aeea37e578d9d3c4b364c3	123.108.110.3	123.108.110.3	HK
3de45412b9aeea37e578d9d3c4b364c3	www.gmalio.com	123.108.110.3	HK
3de45412b9aeea37e578d9d3c4b364c3	www.yahcoo.net	123.108.110.3	HK

Here under all the mapping between the "*infected*" sites to "*distribution*" servers involved in the "*watering hole*" campaign.

"*Infected*" Website	"*Infected*" Website Type	"*Infected*" Hosting Country	"*Distribution*" Server
Unknown	Unknown Victims	Unknown	www.philam.com.tw
www.uygurunsesi.com	Uyghur Dissident	TR	www.uygurunsesi.com
hkdailynews.com.hk	Newspaper	HK	homeweb.zzl.org

3.1.1 www.philam.com.tw chapter

www.philam.com.tw server was compromised at least the 27 December with the potential purpose to be a "*distribution*" server. It is actually unclear which website was compromised to use this distribution server. We found the samples through Google cache.

3.1.2 www.uygurunsesi.com chapter

www.uygurunsesi.com server was compromised at least the 27 December with the purpose to infect visitors of the website.

As we reported in a blog post [21], published the 3 January 2013, this website was, like *www.capstoneturbine.com*, previously comprised to spread CVE-2012-4969.

Payload (*3de45412b9aeea37e578d9d3c4b364c3*) one IP address and two domain names in order to contact the C&C server *123.108.110.3* (AS24544), located in Hong-Kong.

www.yahcoo.net domain name associated to the C&C server was also connected with CVE-2012-4969 with payload Help.exe (*ea4c2b0f71e3551fa82b7dc13eb1cee3*) obfuscated with XOR 70 operation on the bytes which value differs from 00 or 70. This payload was found on www.yeoushin.com.tw, the 19 September 2012 [22]. De-obfuscated payload (*105e2b7eb2afb5f87c72a1e8f2c92a2c*) tries to connect to the mentioned domain name [23].

Another actual interesting behavior of this C&C domain name is the associated page in Google cache. A Google Gmail login page is present on *http://blogs.sacbee.com/sac_history_happenings/0%5B1%5D.1%26disp%3Dsafe%26zw*

3.2 Metasploit Integration

Two days after the public disclosure of the incident Metasploit released "*ie_cbutton_uaf*" exploit module [24]. Initial version of this module could be considered as the first known fork of CVE-2012-4792.

3.3 Exodus Intelligence Fork

Exodus Intelligence published [25] the 2 January a detailed analysis of CVE-2012-4792 vulnerability. Initial code version, used in the "*Very Early Phase*", was using Microsoft Office vulnerability and the traditional Java 6 non-ASLR *msvcr71.dll* library in order to bypass ASLR. Exodus Intel published a new Internet Explorer 8 vulnerability exploitation proof of concept bypassing ASLR with **HTML+TIME**.

This new proof of concept replaced rapidly original Metasploit "*ie_cbutton_uaf*" and was also rapidly forked by "*attackers*" in additional "*drive-by*" attacks that occurred during the "*Structure Formation Phase*".

Also, this proof of concept was a source of confusion for the detection of a new zero-day, also known as CVE-2013-1347, during the April 2013 "watering hole" attack against United States Department of Labor.

3.4 DWORD variant

DWORD variant is a well-known JavaScript exploit kit, using JSE6 ASLR bypass, firstly discovered used with CVE-2011-1996 [26]. This code could be considered as the first "in the wild" variant of CVE-2012-4792.

3.5 Early Phase Conclusion

"*Early Phase*" could be considered as the eye of the storm, a transitioning phase. The initial "*watering hole*" campaign surely ended after his discovery and public disclosure.

4. STRUCTURE FORMATION PHASE

This third phase will describe, and provide additional information's, on the structure formation phase of the attack just after Exodus Intelligence fork.

We can consider that the "*Structure Formation Phase*" started the 2 January, date of the Exodus Intelligence proof of concept publication, and finished when the first Exploit Packs integrated this vulnerability. Some of the mentioned variants are still in use today.

4.1 Reverse Chronology

During this phase the initial campaign still continued and we detected only one additional website with the original code sample. But five other code variants were used in parallel "*watering hole*" campaigns, or by organized crime, and involved in dozens of new compromised websites.

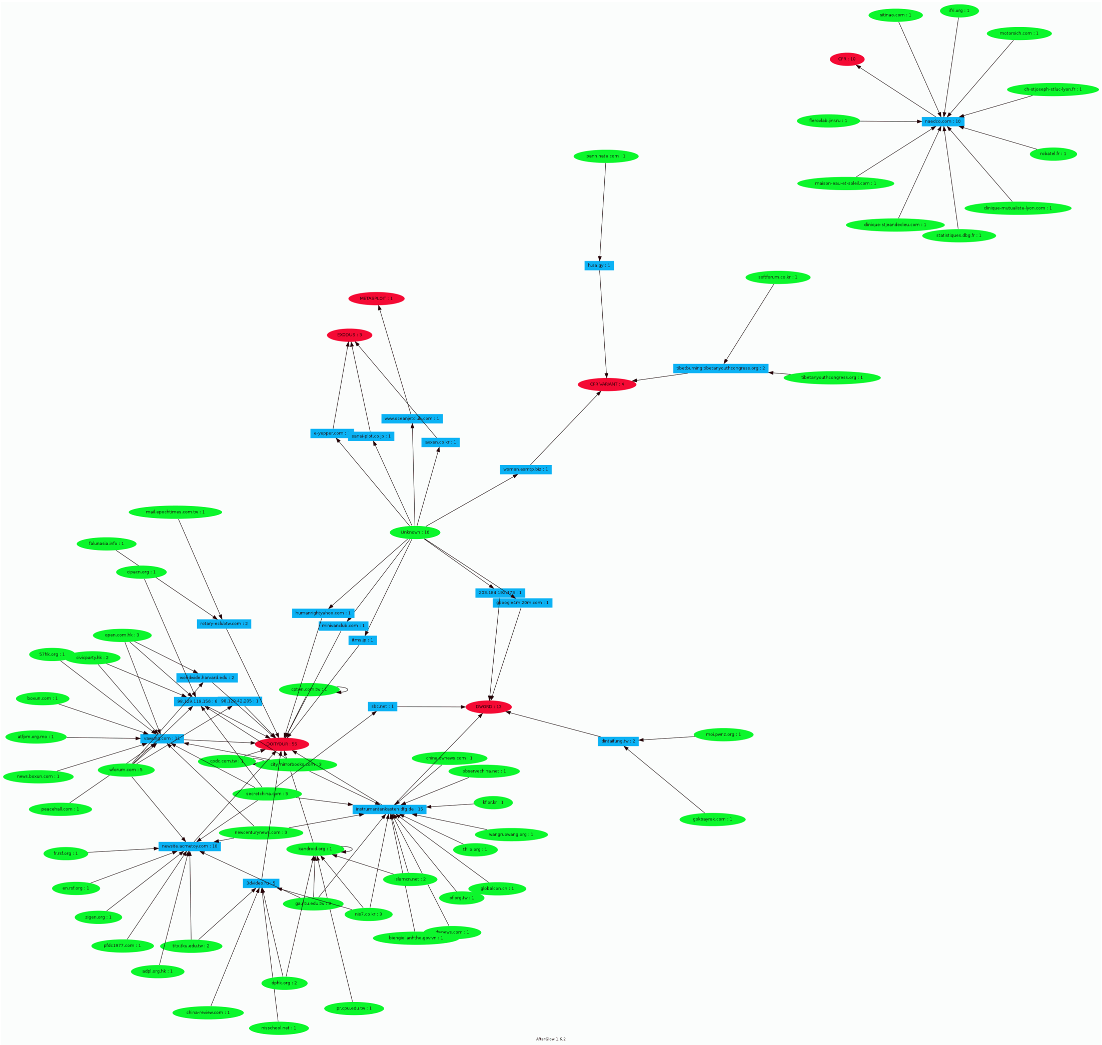
In order to better distinguish the different codes we will name the original code "CFR", some variants of CFR original code to "CFR VARIANT", Metasploit original fork "METASPLOIT", Exodus Intelligence fork "EXODUS", and the two last variants "DOITYOUR" and "DWORD".

Website	Website Type	Country	Code Type	Sample Date
gooogle4m.20m.com	Hosting Website	US	DWORD	2013/01/03
h.sa.gy	Hosting Website	KR	CFR VARIANT	2013/01/04
tibetburning.tibetanyouthcongress.org	Tibetan	US	CFR VARIANT	2013/01/05
woman.esmtp.biz	Hosting Website	N.A.	CFR VARIANT	2013/01/06
naedco.com	Oil & Gas Company	US	CFR	2013/01/06
cpdc.com.tw	Oil & Gas Company	TW	DOITYOUR	2013/01/07
cptwn.com.tw	Company	TW	DOITYOUR	2013/01/07
instrumentenkasten.dfg.de	Foundation	DE	DOITYOUR	2013/01/07
itms.jp	Travel Agency	US	DOITYOUR	2013/01/07
humanrightyahoo.com	Hosting Website	HK	DOITYOUR	2013/01/07
minivanclub.com	Cars Club	US	DOITYOUR	2013/01/07
dintaifung.tw	Political Dissident	TW	DWORD	2013/01/07
oceanjetclub.com	Travel Agency	JP	METASPLOIT	2013/01/10
rotary-eclubtw.com	Hosting Website	US	DOITYOUR	2013/01/11
axxen.co.kr	Unknown	KR	EXODUS	2013/01/11
e-yepper.com	Medicine	KR	EXODUS	2013/01/13
98.129.119.156	Hosting Website	US	DOITYOUR	2013/01/14
98.129.42.205	Hosting Website	US	DOITYOUR	2013/01/14
kandroid.org	Development Community	KR	DOITYOUR	2013/01/14
newsite.acmetoy.com	Hosting Website	SG	DOITYOUR	2013/01/17
203.184.192.173	Hosting Website	HK	DWORD	2013/01/18
humanrightyahoo.com	Hosting Website	HK	EXODUS	2013/02/03
worldwide.harvard.edu	University	US	DOITYOUR	2013/03/08
vawung.com	Political Dissident	MO	DOITYOUR	2013/03/11
3dvideo.ru	Hosting Website	RU	DOITYOUR	2013/03/11

We can observe that landing pages of "DOITYOUR" variant wasn't targeting specific languages, but was still using the original ASLR bypass methods from the "*Very Early Phase*". We can also observe that the "DWORD" variant was targeting specific languages.

Website	Targeted languages						Java ASLR bypass	Office ASLR bypass	HTML+TIME ASLR bypass
	zh-cn	zh-tw	en-us	ja	ru	ko			
gooogle4m.20m.com	X	X	X	X		X	X		
h.sa.gy	X	X	X	X	X	X	X		
tibetburning.tibetanyouthcongress.org							X	X	
woman.esmtp.biz							X	X	
www.naedco.com	X	X	X	X	X	X	X		
cpdc.com.tw							X	X	
cptwn.com.tw							X	X	
instrumentenkasten.dfg.de							X	X	
itms.jp							X	X	
humanrightyahoo.com							X	X	
minivanclub.com							X	X	
dintaifung.tw	X	X	X	X		X	X		
oceanjetclub.com							X		
rotary-eclubtw.com							X	X	
axxen.co.kr	X		X	X		X			X
e-yepper.com	X		X	X		X			X
98.129.119.156							X	X	
98.129.42.205							X	X	
www.kandroid.org							X	X	
newsite.acmetoy.com							X	X	
203.184.192.173							X		
humanrightyahoo.com									X
worldwide.harvard.edu							X		
vawung.com							X	X	
3dvideo.ru							X	X	

Here under all the mapping between the "*infected*" sites to "*distribution*" servers involved in the "*watering hole*" campaign. This AfterGlow visualization file is provided as annex to this document.



5. ULTIMATE FATE PHASE

CVE-2012-4792 vulnerability was discovered integrated into Cool Exploit Kit the 26 January 2013, followed by an integration into CritXPack the 9 February 2013 and then into Gong Da exploit kit the 15 April.

6. CONCLUSIONS

It's a bit complicated to draw many hard, evidence-based conclusions from this campaign. What is really surprising to us is how lame the attackers may be and be still potentially successful. Many of the exploits were patched really fast, but were still in use weeks or months after patch release, because both we and attackers know that people simply refuse to update, either because they're lazy, or unaware of patching or afraid of breaking things. The very same problem is with the server admins – many of the servers we've seen to be infected were re-infected multiple times – it means that people are unaware of the problems they have and again, they do not patch and close the holes, making the internet worse place for everyone.

The watering hole approach is a good device for the semi-lame attackers. It lets them narrow their 'demographic' but without all the preliminary reconnaissance usually needed for targeted attacks – no spear phishing, just simple hack of the server where can the attackers wait for their victims to come.

Regarding the purpose and attribution – it seems clear that the purpose in this phase is to gather information about human rights activists that may pose danger to China. All the installed tools were key loggers or advanced remote access tools that would let the attackers to eavesdrop the victims and get more evidence on other potential targets of this espionage campaign.

7. REFERENCES

[1] Chinese Hackers Suspected in Cyber Attack on Council on Foreign Relations – The Washington Free Beacon. *http://freebeacon.com/chinese-hackers-suspected-in-cyber-attack-on-council-on-foreign-relations/*

[2] urlQuery.net CFR website submissions. *http://www.urlquery.net/search.php?q=cfr.org&type=string&start=2012-11-01&end=2012-12-28&max=200*

[3] CLEAN MX CFR website submission. *http://support.clean-mx.de/clean-mx/viruses.php?id=8724375*

[4] xsainfo.jpg VirScan submission. *http://r.virscan.org/7985b346f75a60148ace03b31f1a37fe*

[5] xsainfo.jpg VirusTotal submission. *https://www.virustotal.com/file/e4b7b8dd6a4f9dc93b14205ef7d41647ce5c6b18a1194bd88d3205deb7bf26fa/analysis/*

[6] Bypassing Microsoft Windows ASLR with a little help by MS-Help - GreyHatHacker.NET. *http://www.greyhathacker.net/?p=585*

[7] CFR Watering Hole Attack Details – FireEye. *http://www.fireeye.com/blog/technical/malware-research/2012/12/council-foreign-relations-water-hole-attack-details.html*

[8] Trojan:Win32/Diofopi.A – Microsoft Malware Protection Center. *http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan%3AWin32%2FDiofopi.A*

[9] AhnLab blog post. *http://asec.ahnlab.com/897*

[10] support.ayuisyahooapis.com on ThreatExpert. *http://www.threatexpert.com/report.aspx?md5=99baa58ce02872016b4ad25d2deef36e*

[11] support.ayuisyahooapis.com on Symantec. *http://www.symantec.com/security_response/writeup.jsp?docid=2012-122110-0259-99*

[12] Analysis of a PlugX variant (PlugX version 7.0) - Computer Incident Response Center Luxembourg. *http://www.circl.lu/files/tr-12/tr-12-circl-plugx-analysis-v1.pdf*

[13] nProtect blog post. *http://erteam.nprotect.com/321*

[14] A Deeper Look In CVE-2012-4792 Watering Hole Campaigns – Alljap Chapter – Eric Romang. *http://eromang.zataz.com/2013/02/18/a-deeper-look-in-cve-2012-4792-watering-hole-campaigns-alljap-chapter/*

[15] Alljap.net chapter Google Fusion Tables – *All Hits.* *https://www.google.com/fusiontables/DataSource?docid=11vFe_t2KiKDTCBJ8A-XiU1BisE8h2k5rYrCwuCE*

[16] Alljap.net chapter Google Fusion Tables – All MSIE 8 Hits. *https://www.google.com/fusiontables/DataSource?docid=1NaBaZVKKA0weB7LpNANsJfzQGR5sI6hwrla0fMM*

[17] goddess.nexon.com.au chapter Google Fusion Tables – All Hits. *https://www.google.com/fusiontables/DataSource?docid=14qPcT1hf4a3HG3IrDZM3qvUZ9hXH1ncb8fFL4XQ*

[18] CVE-2012-4969 CLEAN MX submission. *http://support.clean-mx.de/clean-mx/viruses.php?id=2251432*

[19] *ras-ru.oicp.net* ThreatExpert submission. *http://www.threatexpert.com/report.aspx?md5=08ec21075df33b9275233be239e851a3*

[20] Elderwood Project Behind Latest Internet Explorer Zero-Day Vulnerability – Symantec. *http://www.symantec.com/connect/blogs/elderwood-project-behind-latest-internet-explorer-zero-day-vulnerability*

[21] Chinese Uygur Minority Also Targeted in the CFR Watering Hole Attack And More – Eric Romang. *http://eromang.zataz.com/2013/01/03/chinese-uygur-minority-also-targeted-in-the-cfr-watering-hole-attack-and-more/*

[22] Help.exe (*ea4c2b0f71e3551fa82b7dc13eb1cee3*) on Minotaur Analysis. *http://minotauranalysis.com/search.aspx?q=ea4c2b0f71e3551fa82b7dc13eb1cee3*

[23] De-obfuscated Help.exe (105e2b7eb2afb5f87c72a1e8f2c92a2c) on ThreatExpert. *http://www.threatexpert.com/report.aspx?md5=105e2b7eb2afb5f87c72a1e8f2c92a2c*

[24] ie_cbutton_uaf Metasploit exploit module. *http://www.metasploit.com/modules/exploit/windows/browser/ie_cbutton_uaf*

[25] Happy New Year Analysis of CVE-2012-4792 – Exodus Intelligence. *http://blog.exodusintel.com/2013/01/02/happy-new-year-analysis-of-cve-2012-4792/*

[26] Short Story regarding Microsoft MS11-081 CVE-2011-1996 - Eric Romang. *http://eromang.zataz.com/2013/01/13/short-story-regarding-microsoft-ms11-081-cve-2011-1996/*