(C)0ld Case : From Aerospace to China's interests.

Published: 2018-11-16 · Archived: 2026-04-05 14:28:46 UTC

Via the events collected mostly from passive DNS records, I'll highlight that threat actor(s)/ group(s) were using since 2010 a "DNS highjacking" tactic which is here observed as replacing victim's zone authoritative name servers, by their controlled one, for small period of time. This could result in interception, espionage or sabotage by these means. The victims profiles found, strongly align with China's interests. Various areas of activity are concerned, from Fortune 100 to cultual or religious organizations :

- France: Safran, Snecma (now Safran Aircraft Engines)
- Korea: Microsoft, Adobe, Honeywell, Nintendo, Logic Korea (Video game), KFTC (Financial payment service), Minghui (Falun Gong organization), Shinchonji (Evangelists)
- Australia: Australian Postal Corporation, Guangming (Falun Gong organization)
- United States : Makerbot (3D Printing company).

US DOJ & Aerospace

Referring to the indictment by the U.S. Department of Justice (DOJ) of ten Chinese intelligence officers for espionage (2018-10-10), cf:

https://www.justice.gov/opa/pr/chinese-intelligen

THE UNITED STATES DEPARTMENT of JUSTICE

HOME ABOUT AGENCIES RESOURCES NEWS CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, October 10, 2018

Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies

A Chinese Ministry of State Security (MSS) operative, Yanjun Xu, aka Qu Hui, aka Zhang Hui, has been arrested and charged with conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies. Xu was extradited to the United States yesterday.

The charges were announced today by Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the Southern District of Ohio Benjamin C. Glassman, Assistant Director Bill Priestap of the FBI's Counterintelligence Division, and Special Agent in Charge Angela L. Byers of the FBI's Cincinnati Division.

"This indictment alleges that a Chinese intelligence officer sought to steal trade secrets and other sensitive information from an American company that leads the way in aerospace," said Assistant Attorney General Demers. "This case is not an isolated incident. It is part of an overall economic policy of developing China at American expense. We cannot tolerate a nation's stealing our firepower and the fruits of our brainpower. We will not tolerate a nation that reaps what it does not sow."

"Innovation in aviation has been a hallmark of life and industry in the United States since the Wright brothers first designed gliders in Dayton more than a century ago," said U.S. Attorney Glassman. "U.S. aerospace companies invest decades of time and billions of dollars in research. This is the American way. In contrast, according to the indictment, a Chinese intelligence officer tried to acquire that same, hard-earned innovation through theft. This case shows that federal law enforcement authorities can not only detect and disrupt such espionage, but can also catch its perpetrators. The defendant will now face trial in federal court in Cincinnati."

"This unprecedented extradition of a Chinese intelligence officer exposes the Chinese government's direct oversight of economic espionage against the United States," said Assistant Director Priestap.

Yanjun Xu is a Deputy Division Director with the MSS's Jiangsu State Security Department, Sixth Bureau. The MSS is the intelligence and security agency for China and is responsible for counter-intelligence, foreign intelligence and political

> And according to this indictment :"***Beginning in at least December 2013 and continuing*** *until his arrest, Xu targeted certain companies* ***inside and outside the United States*** *that are recognized as leaders in the* ***aviation*** *field. "*

NB: You can read this link too, that summarize also well these recent events.

I decided to look what I can find on a (c)old case "linked" to this indictment. My starting point was this CrowdStrike article from February the 25th, 2014 :


CROWDSTRIKE | BLOG

Featured

Rec

The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity

February 25, 2014 Matt Dahl Research & Threat Intel

Two weeks ago, news broke about strategic web compromise (SWC) activity on the website for the U.S. organization, Veterans of Foreign Wars (VFW). This activity leveraged exploit code for a zero-day vulnerability now identified as CVE-2014-0322 and ultimately infected victims with ZxShell malware. CrowdStrike Intelligence attributed this attack to the AURORA PANDA adversary; however, the discovery of additional indicators revealed that another adversary was leveraging the same vulnerability to carry out

The events (publish and/or occurring were around the same period too..) i.e at the end of the 2013 year and beginning of 2014 :

French Aerospace	VFW	CrowdStrike Article
2014-01-11	2014-02-11	2014-02-25

We know that Safran, Snecma (a Safran subsidiary) and the French aerospace industries association : the “Groupement des industries françaises aéronautiques et spatiales” (GIFAS) were concerned.

I decided to start from what we know, and lookup into Passive DNS data, mostly.

secure[.]safran-group[.]com

First thing was that Safran **let one of his RR pointing for more than two months to a malicious IP. (?!)** The two other domains were *a contrario* malicious domains, crafted for, and not directly related to the victims.

Time Last Seen	Time First Seen ▲	Count	RRname	RRtype	Rdata
2011-06-02 05:35:16	2010-11-30 03:52:10	112	fab7a.com.	A	173.252.252.204
2013-02-09 18:00:49	2012-04-23 03:31:50	231	www.louisvuitton-rabatt.biz.	A	173.252.252.204
2013-07-16 15:20:15	2013-07-16 15:06:00	3	www.qxgxxq.com.	A	173.252.252.204
2013-11-04 04:29:32	2013-11-04 04:29:32	1	icbctjr.com.	A	173.252.252.204
2014-02-09 01:44:02	2013-11-23 20:58:29	25	secure.safran-group.com.	A	173.252.252.204
2014-07-29 21:10:04	2013-12-26 18:07:48	521	icbcqsz.com.	A	173.252.252.204
2014-02-25 09:21:00	2014-02-13 22:09:00	385	gifas.assso.net.	A	173.252.252.204
2014-02-17 03:32:38	2014-02-14 19:07:16	237	ameteksen.com.	A	173.252.252.204
2014-02-18 02:58:29	2014-02-14 20:16:40	180	savmpet.com.	A	173.252.252.204
2014-02-25 10:25:22	2014-02-14 20:24:53	350	exchenage.doomdns.com.	A	173.252.252.204
2018-10-01 02:02:36	2014-02-14 20:24:53	505	173-252-252-204.genericreverse.com.	A	173.252.252.204
2014-02-25 09:27:50	2014-02-14 20:24:53	551	update19.homelinux.org.	A	173.252.252.204
2014-02-25 10:25:23	2014-02-14 20:24:53	297	ns18.is-a-linux-user.org.	A	173.252.252.204
2015-07-13 11:24:03	2014-10-23 23:57:23	457	mifsp.com.	A	173.252.252.204
2014-12-21 02:46:16	2014-10-25 07:20:55	1395	replicasoccershirt.com.	A	173.252.252.204
2014-12-16 00:20:11	2014-10-30 09:22:11	429	replicasocceruniform.com.	A	173.252.252.204
2015-10-22 19:54:36	2014-12-03 14:45:57	1764	www.esocceronline.com.	A	173.252.252.204

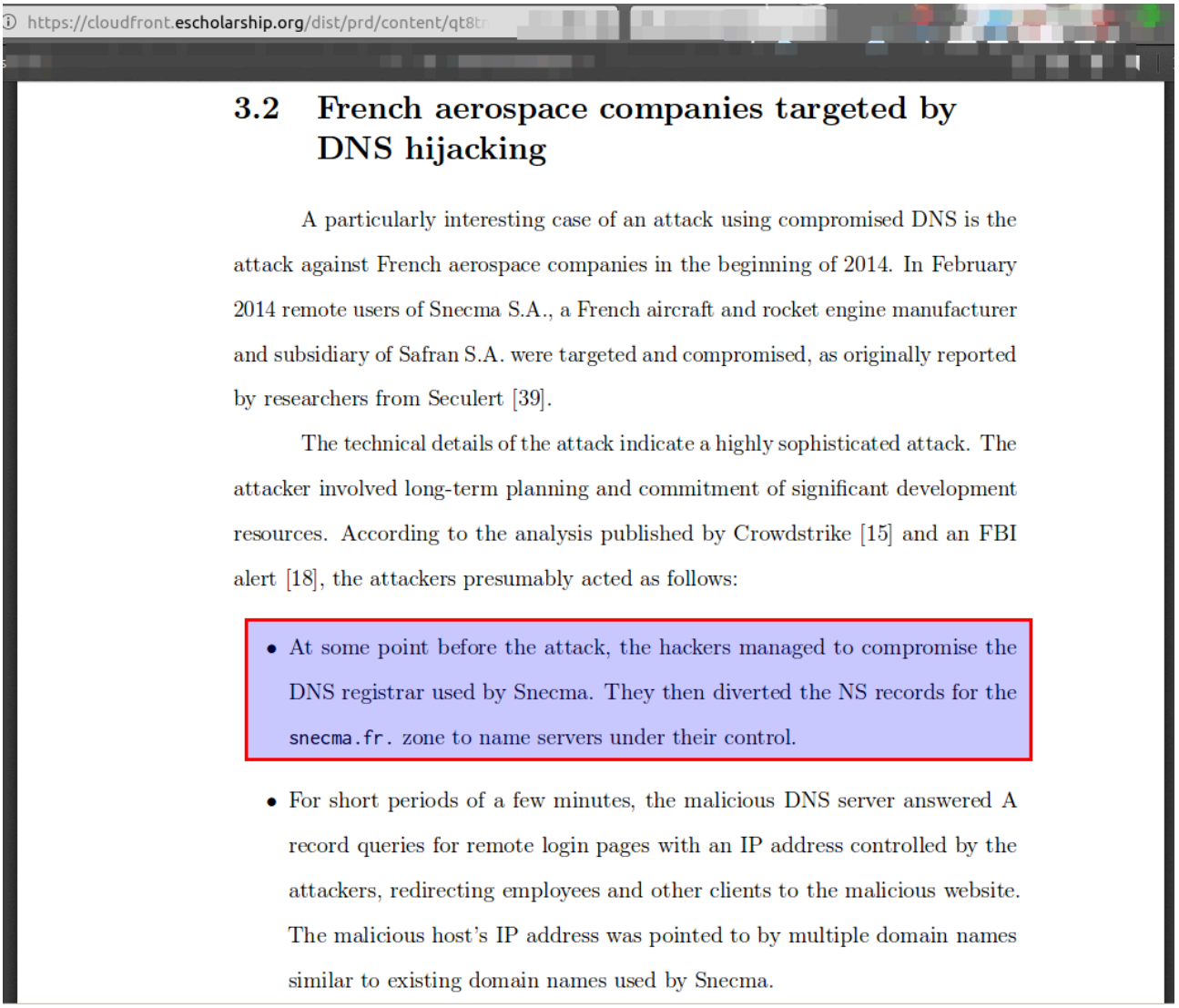
(Source DNSDB)

Safran Name Server

From the CrowdStrike article :

> Of particular interest was **secure[.]safran-group[.]com**. Safran is a France-based aerospace and defense company with a focus on the design and production of aircraft engines and equipment. The company owns the safran-group[.]com domain, and the fact that one of its subdomains was pointed at a malicious IP address suggests **that the adversary compromised Safran's DNS.**

The second point is bold text above : "(…)**the adversary compromised Safran's DNS.**" I didn't find something thus that could help to understand how it was accomplished. By searching the Internet I found a UC San Diego thesis with title : "Investigating DNS Hijacking Through High Frequency Measurements" which seems well informed on the incidents :



https://cloudfront.escholarship.org/dist/prd/content/qt8t

3.2 French aerospace companies targeted by DNS hijacking

A particularly interesting case of an attack using compromised DNS is the attack against French aerospace companies in the beginning of 2014. In February 2014 remote users of Snecma S.A., a French aircraft and rocket engine manufacturer and subsidiary of Safran S.A. were targeted and compromised, as originally reported by researchers from Seculert [39].

The technical details of the attack indicate a highly sophisticated attack. The attacker involved long-term planning and commitment of significant development resources. According to the analysis published by Crowdstrike [15] and an FBI alert [18], the attackers presumably acted as follows:

- At some point before the attack, the hackers managed to compromise the DNS registrar used by Snecma. They then diverted the NS records for the `snecma.fr.` zone to name servers under their control.
- For short periods of a few minutes, the malicious DNS server answered A record queries for remote login pages with an IP address controlled by the attackers, redirecting employees and other clients to the malicious website. The malicious host's IP address was pointed to by multiple domain names similar to existing domain names used by Snecma.

Snecma Name Server

What we can read in CrowdStrike article, is that a number of domains were added to the "host's" file of victim machines, but :

> "the purpose of this component is unclear. It does not map these domains to malicious IP addresses because the 217.108.170.0/24 range belongs to the company"

By looking at the **snecma.fr** Name Servers I found some weird ones at the moment : **ns1.acfine.net** and **ns2.acfine.net**

Time Last Seen	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2018-11-10 18:29:58	2010-06-24 07:27:08	1743358	fr.	snecma.fr.	NS	snecma.snecma.fr. snecma2.snecma.fr.
2018-10-29 07:56:22	2010-06-24 05:11:23	1126853	snecma.fr.	snecma.fr.	NS	snecma.snecma.fr. snecma2.snecma.fr.
2014-09-30 16:47:17	2013-11-20 19:25:08	10149	fr.	snecma.fr.	NS	ns1.acfine.net. ns2.acfine.net.
2013-03-20 10:44:36	2013-03-20 10:44:35	3	snecma.fr.	snecma.fr.	NS	server.dns.local. snecma.snecma.fr. snecma2.snecma.fr. snecma9.snecma.fr. snecma10.snecma.fr.
2012-06-05 10:53:43	2012-05-14 09:44:38	11198	snecma.fr.	snecma.fr.	NS	snecma.snecma.fr. snecma2.snecma.fr. smartarchidns.snecma.fr.

Time first seen was the 20th of November 2013 : Did the attack occur first ? Idem from 2 days in August 2013.no id

Time Last Seen	Time First Seen ▲	Count	Bailiwick	RRname	RRtype	Rdata
2013-08-15 08:42:35	2013-08-13 18:10:36	3298	acfine.net.	ns1.acfine.net.	A	216.244.81.150
2013-11-21 20:08:00	2013-11-20 19:22:17	128	acfine.net.	ns1.acfine.net.	A	198.52.125.42
2014-05-05 11:25:54	2014-04-15 02:24:44	59	net.	ns1.acfine.net.	A	74.121.190.105
2014-08-11 14:25:05	2014-04-15 02:24:45	1850	acfine.net.	ns1.acfine.net.	A	74.121.190.105
2014-09-01 15:26:37	2014-08-11 14:30:04	3660	acfine.net.	ns1.acfine.net.	A	23.89.232.225
2014-10-02 10:20:00	2014-09-26 18:25:08	4317	acfine.net.	ns1.acfine.net.	A	23.88.10.35

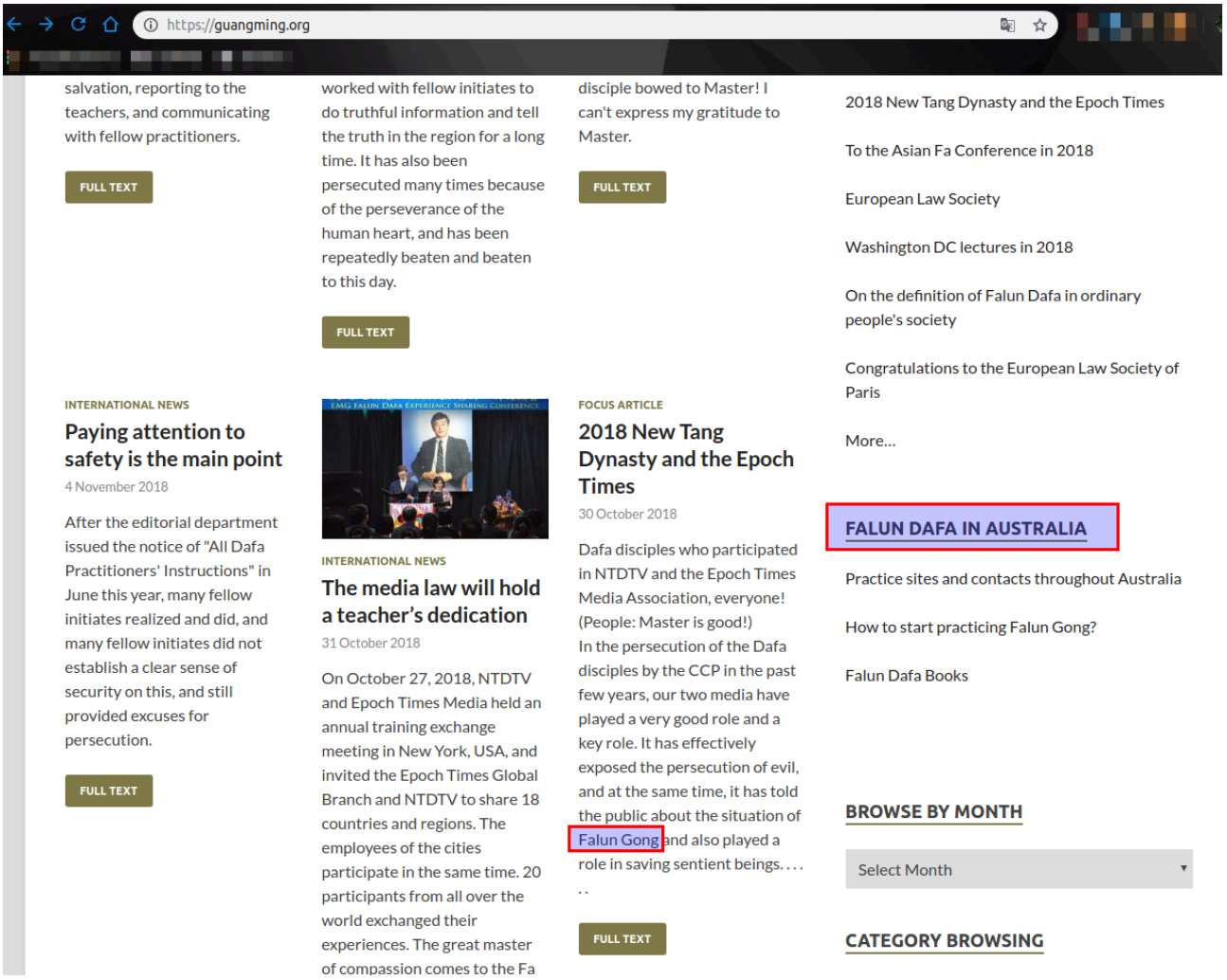
If we look at the **domains now that were using these Name Servers**, we see interesting points :

Time Last Seen	Time First Seen	Count	RRname	RRtype	Rdata
2014-09-30 16:47:17	2013-11-20 19:25:08	10149	snecma.fr.	NS	ns1.acfine.net.
2014-09-01 06:38:48	2014-08-10 15:50:06	662	guangming.org.	NS	ns1.acfine.net.
2014-08-31 18:00:16*	2014-08-10 18:01:07*	22	guangming.org.	NS	ns1.acfine.net.
2014-05-05 11:25:54	2014-04-15 02:24:44	59	makerbot.com.	NS	ns1.acfine.net.
2013-08-15 07:44:32	2013-08-13 18:10:36	1535	auspost.com.au.	NS	ns1.acfine.net.

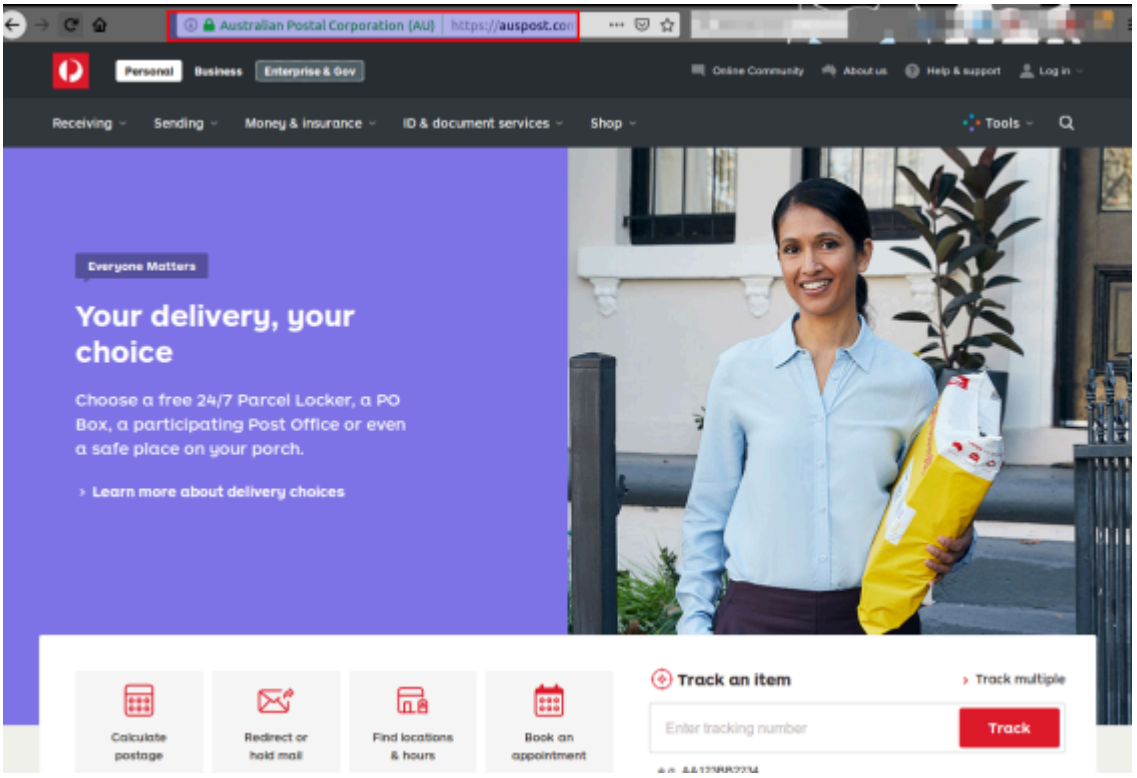
What is interesting here with these domains/sites is the **mix of targets profiles and China's Interests :**

- **snecma.fr** was previously indicated and was China's interest without any doubt at that time. We have covered briefly this above.
- **guangming.org** seems to be a "Falun Gong" information website, this is of the **utter interest in China's policy**. We can see multiple references to this "organization", and China see it as a cult (see this official

Chinese governmental link e.g). NB: The website may be related to their practice in Australia.



- **auspost.com.au**



This is the website of **Australian Postal Corporation**. Maybe linked to the previous Falun Gong possible supposed targets ?

- **makerbot.com** is a 3D Printing company, based in New York.

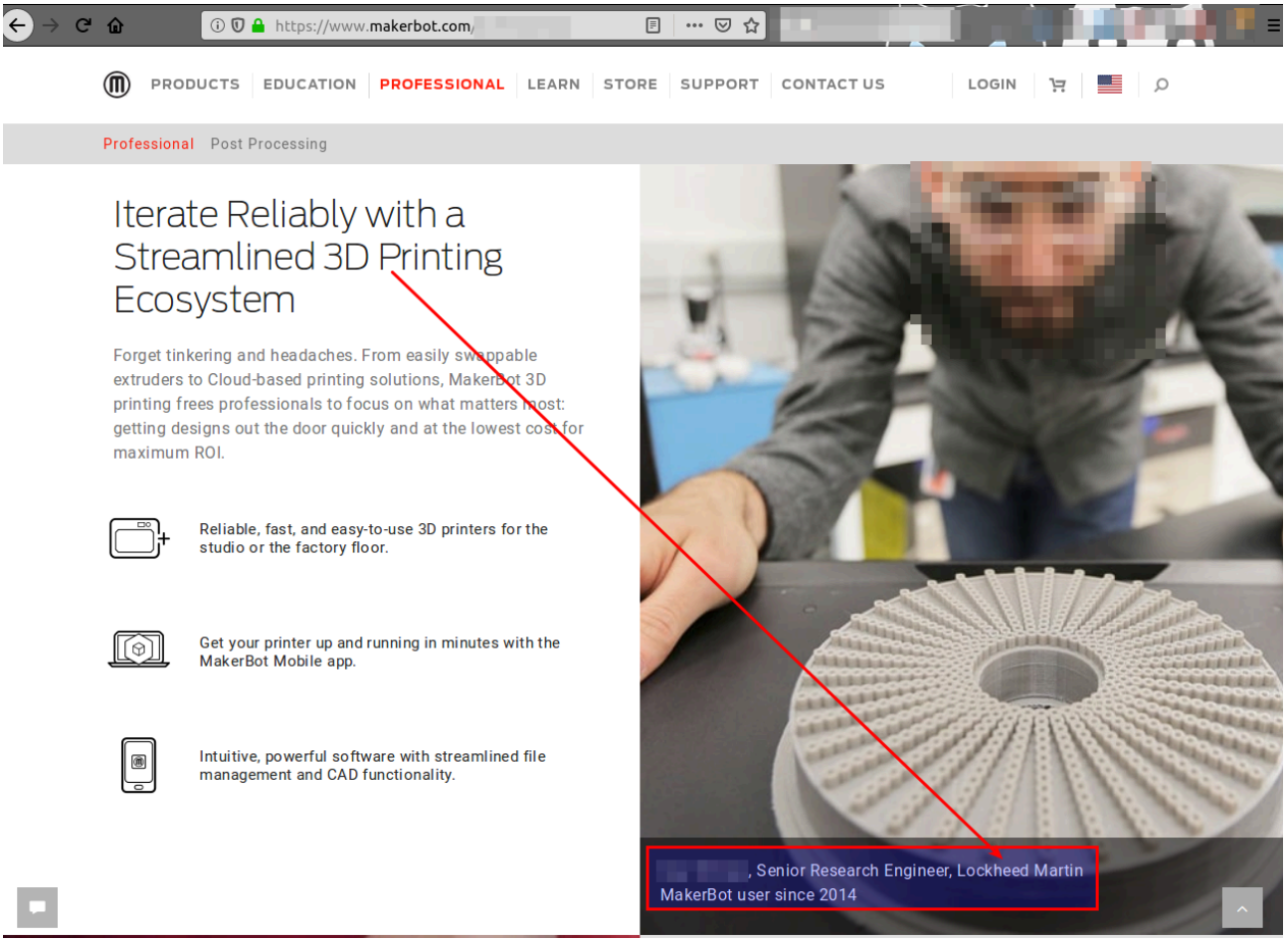
Could this be another objective from attackers, or another group inside a team ? APT could be composed of several groups/teams, with different goals, and sometime using the same architecture or sharing the same TTPs.

Some **open line of investigation** on this… but I found on the website that a Lockheed Martin's Senior Research Engineer was using their product **since 2014 : It could be interesting for attackers to target this company to correlate different data.**

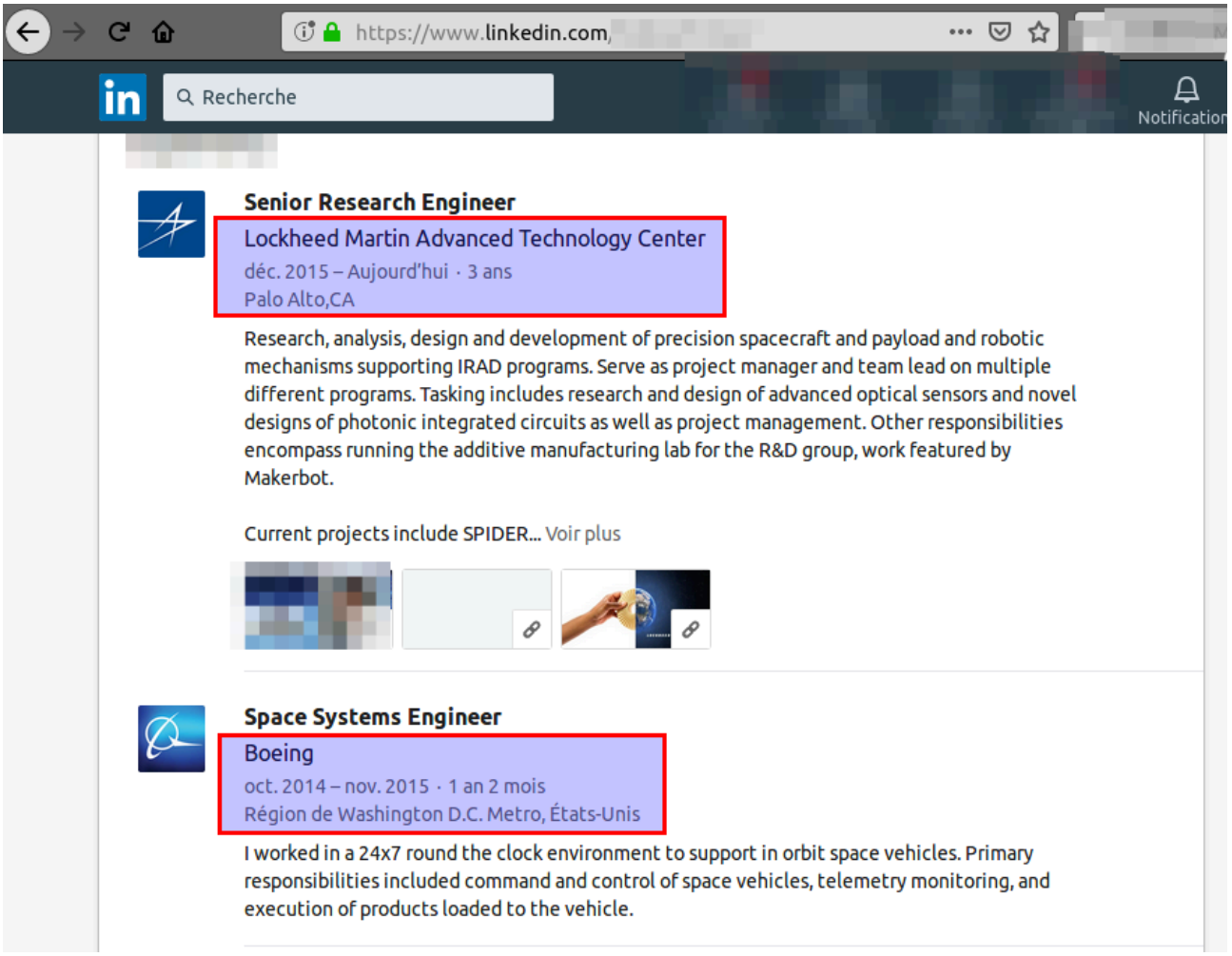
ex: Lockhed Martin Blueprints + robotic mechanisms & Engineering

As **correlating** two different databases could reveal useful information,

ex: Office of Personnel Management (OPM) wich handle SF-86 form to obtain a security clearance + Anthem (Health Insurance) permitted to find the CIA agents by doing a diff between the data…



Linkedin profile :



Airbus & Microsoft Korea

blog.airbuscybersecurity.com/post/2015/09/APT-Black

v1.0 (21/11/2012)

At this step, Sakula was just born but already implements commands 0 to 5. Its configuration is encrypted with the key **0x88** and communications with the key **0x59**.

A PDB path **E:\编程\C++程序\打头\打头\Release\打头.pdb** is present in the sample.

At its start, Sakula does some action to set up persistence:

- It copies itself to **%WINDIR%\system32\Sweep.exe** (if 32 bits)
- It copies itself to **%WINDIR%\SysWOW64\Sweep.exe** (if 64 bits)
- It creates a service pointing to its copy
  - Option **SERVICE_AUTO_START** (the service starts automatically during system startup)
  - Its name is **Office Auto Update**
  - Its description is **Microsoft Office Auto Update**
- It starts the service using the command **net start "Office Auto Update"**
- It removes itself using the command **ping 127.0.0.1 & del /q "<malware_path>"**

The configuration structure is:

```
struct ConfigV1_0
{
    CHAR    cc_domain[100];             //  update.microsoft.co.kr
    CHAR    uri_get1_folder[100];       //  /photo/
    CHAR    uri_get3_file[100];         //  check.asp
    CHAR    uri_get2_file[100];         //  /viewphoto.asp
    CHAR    uri_get3_arg[100];          //  imageid
    CHAR    copy_name[100];             //  Sweep.exe
    CHAR    service_name[100];          //  Office Auto Update
    CHAR    service_description[100];   //  Microsoft Office Auto Update.
    DWORD   waiting_time;               //  0x956A0 (612000 milliseconds, ~
}
```

On this version, the command n°5 (which updates the waiting time between requests for orders) allows a maximum waiting time of 0x83D216 ms (+0x3E9), which is approximatively 2 hours and 23 minutes. The machine name is in plain text in URI (without serial number).

The **User Agent** used is **iexplorer**.

An example of used URIs:

- POST /check.asp?imageid=[MACHINE_NAME]&type=[CMD_ID]
- GET (1) /photo/[MACHINE_NAME].jpg
- GET (2) /viewphoto.asp?photoid=[MACHINE_NAME]

Sample (0237f92714f28d755025fa6ba0f4759c7797edd73c4ccbd544495941ae0e0bcd) contacting the Microsoft domain :

Basic Properties

MD5	a3ca10e35e6b7dc2e7af2814ce05d412
SHA-1	a5b9409a95fcf625d279aebcc0cf534e1ff5d7f3
Authentihash	216c6759cb4d6eb23b80bd9c680e1aa6f33611d742caa998fd7181199fd9
Imphash	7302505a107422288e7df076d9742a78
SSDEEP	768:lZf3BDqz0GxbLehmRhMuOBdl+/irabcFw3qrH0h4iUo2PwfED/nN6cSl /3WH:z3BOgmHMnfYqFFoQHUbU5PrdA3W
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	54.5 KB

Tags

peexe

History

Creation Time	2012-11-21 07:17:31
First Seen In The Wild	2012-08-29 17:26:19
First Submission	2012-11-26 05:16:05
Last Submission	2018-05-07 10:20:55
Last Analysis	2018-05-07 10:20:55
Debug Artifacts	2012-11-21 06:17:31

Names

/home/virustotal/sample/A3CA10E35E6B7DC2E7AF2814CE05D412
a3ca10e35e6b7dc2e7af2814ce05d412
a3ca10e35e6b7dc2e7af2814ce05d412.exe
pat.exe.vir_BACKDOOR
Sweep.exe
C:\g8FWT76\9Us0UuJxxJ\JITgFY\SVLgPZtV1\XCVIG.tar.bz2

Portable Executable Info

Debug Artifacts

Path	E:\编程\C++程序\打头\打头\Release\打头.pdb
GUID	462b339b-23a3-4a25-ac5c-6721d8c8612f

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2012-11-21 07:17:31
Entry Point	12187
Contained Sections	5

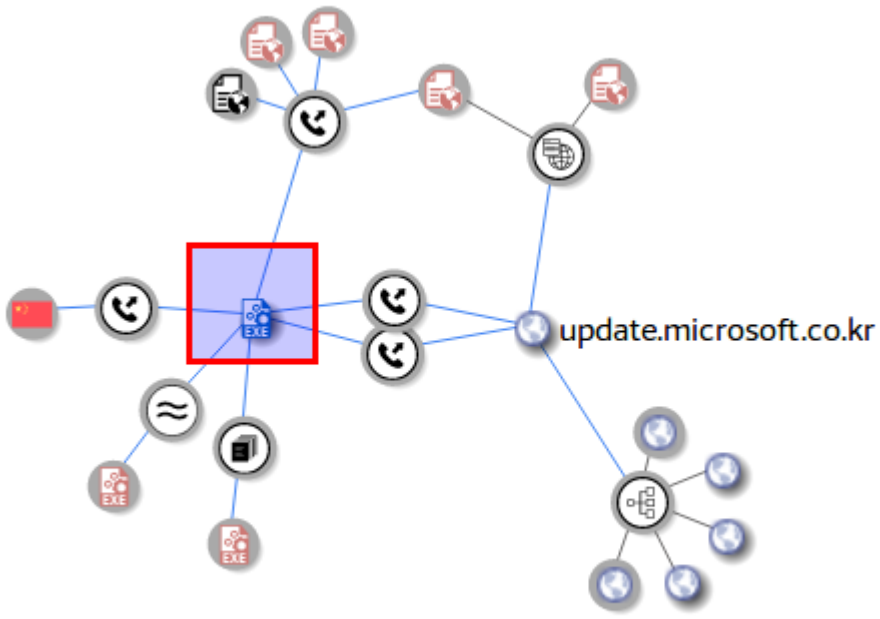
Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5

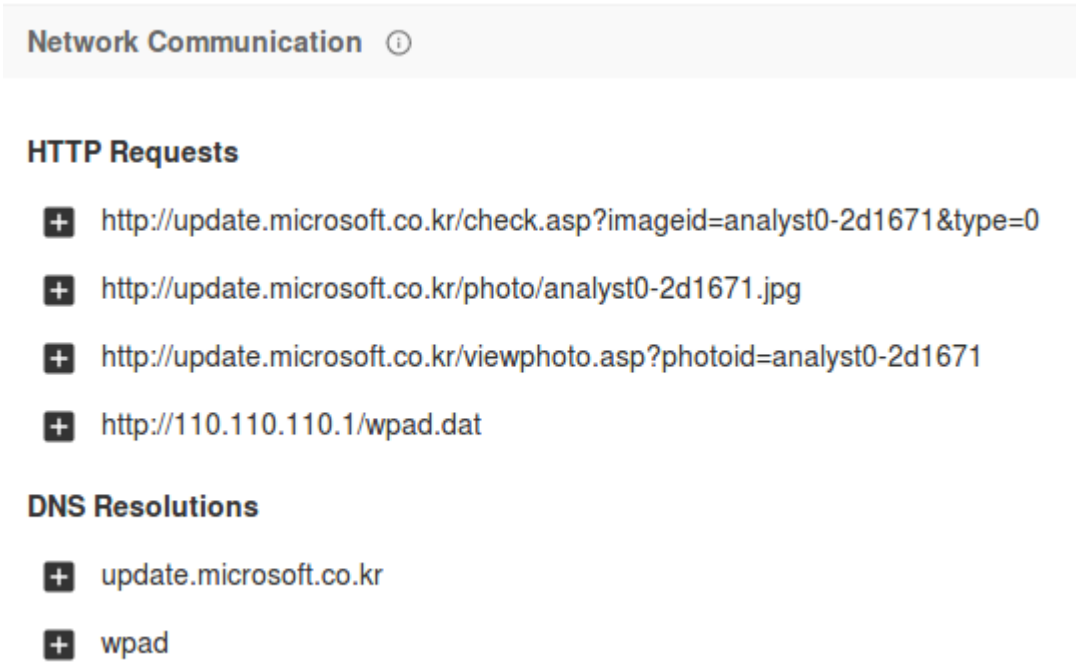
ExifTool File Metadata

CodeSize	34304
EntryPoint	0x2f9b
FileType	Win32 EXE
FileTypeExtension	exe

NB: The compilation timestamp **2012-11-21 07:17:31** from the above sample is consistent with the DNSDB timestamps too, see below : **2012-11-11 to 2012-11-22**



Here are the contacted URLs : (Source VT)



A victim contacted a Microsoft domain ? A legit one ? I did a little research and **yes microsoft.co.kr** redirect now to microsoft.com/korea for its corporate's website.

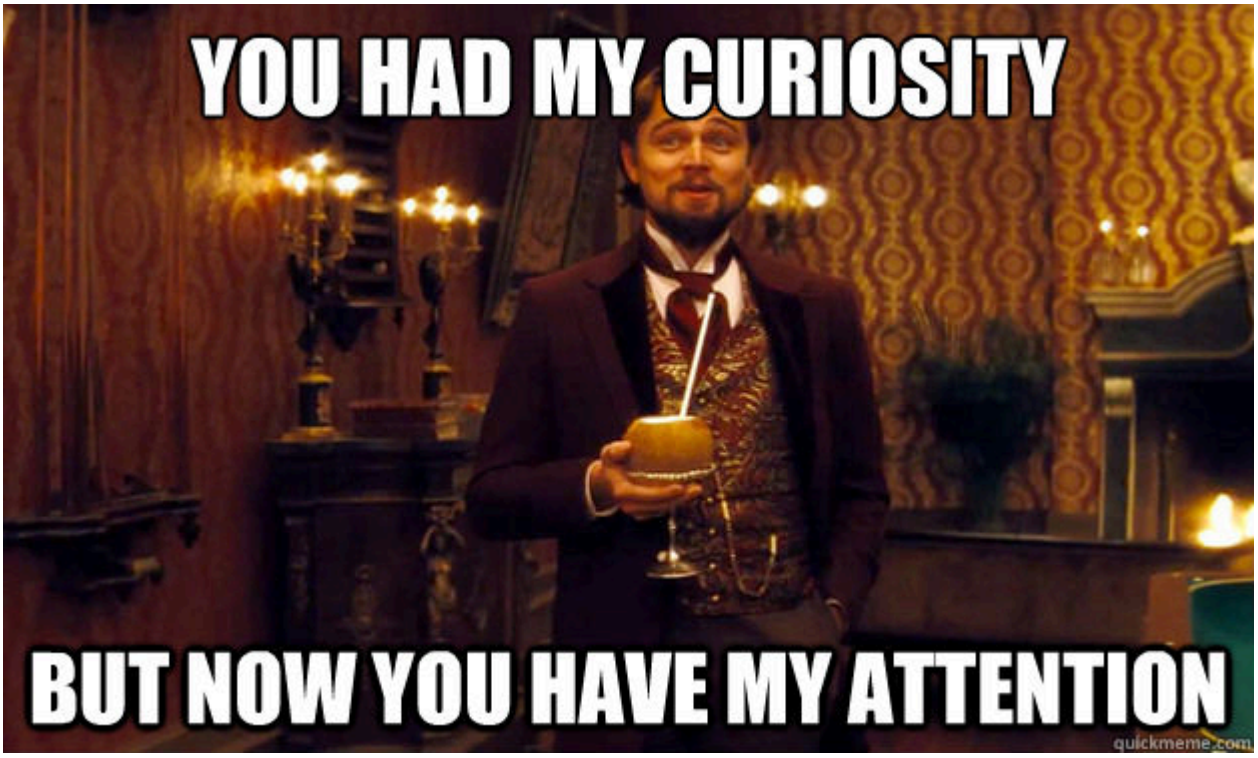
I did a search on Farsight DNSDB passive DNS records and looked at all records for this domain : **microsoft.co.kr .**

Time Last Seen	Time First Seen ▲	Count	Bailiwick	RRname	RRtype	Rdata
2012-05-01 17:17:53	2010-07-28 16:33:24	1672	microsoft.co.kr.	microsoft.co.kr.	A	207.46.197.32 207.46.232.182 210.220.209.174
2010-08-26 12:07:38	2010-07-28 16:33:24	47	co.kr.	microsoft.co.kr.	NS	ns2.msft.net. ns3.msft.net.
2010-08-27 02:13:04	2010-08-26 01:37:05	4	co.kr.	microsoft.co.kr.	NS	ns21.dollar2host.com. ns22.dollar2host.com.
2010-08-27 02:13:04	2010-08-27 02:13:04	2	kr.	microsoft.co.kr.	NS	ns21.dollar2host.com. ns22.dollar2host.com.
2015-01-08 18:39:07	2010-08-28 11:48:02	2127	co.kr.	microsoft.co.kr.	NS	ns2.msft.net. ns3.msft.net. ns4.msft.net.
2010-08-30 06:19:35	2010-08-30 03:00:51	6	kr.	microsoft.co.kr.	NS	ns2.msft.net. ns3.msft.net. ns4.msft.net.
2012-05-02 20:54:08	2012-05-02 03:36:37	5	microsoft.co.kr.	microsoft.co.kr.	A	65.55.58.201 207.46.197.32 210.220.209.174
2014-04-30 02:59:50	2012-05-04 03:50:58	836	microsoft.co.kr.	microsoft.co.kr.	A	64.4.11.37 65.55.58.201 210.220.209.174
2018-07-16 03:28:54	2012-05-27 14:40:56	5	microsoft.co.kr.	microsoft.co.kr.	NS	ns2.msft.net. ns3.msft.net. ns4.msft.net.
2012-11-22 06:43:04	2012-11-11 06:12:59	30	co.kr.	microsoft.co.kr.	NS	ns0.nscomdomain.com. ns1.nscomdomain.com.
2014-06-12 12:58:26	2014-05-01 18:48:44	25	microsoft.co.kr.	microsoft.co.kr.	A	65.55.58.201 134.170.188.221

Same as previously, for a few time period in 2010 : 1 day, and more than 11 days in 2012, Microsoft Korean Name Servers were directed to what I immediately found suspect, resp. **ns21.dollar2host.com** / **ns22.dollar2host.com** and **ns0.nscomdomain.com** / **ns1.nscomdomain.com**.

NB: **ns2.msft.net** (an ns3, and 4..) were not suspect because legit Microsoft domain, but **NOT** the others…

Microsoft in Korea was pwned 2 times, in 2010 and 2012 and as far as I know I didn't see these information well documented.



What could possibly go wrong ?

Same tactic ? DNS highjacking, Let's see…

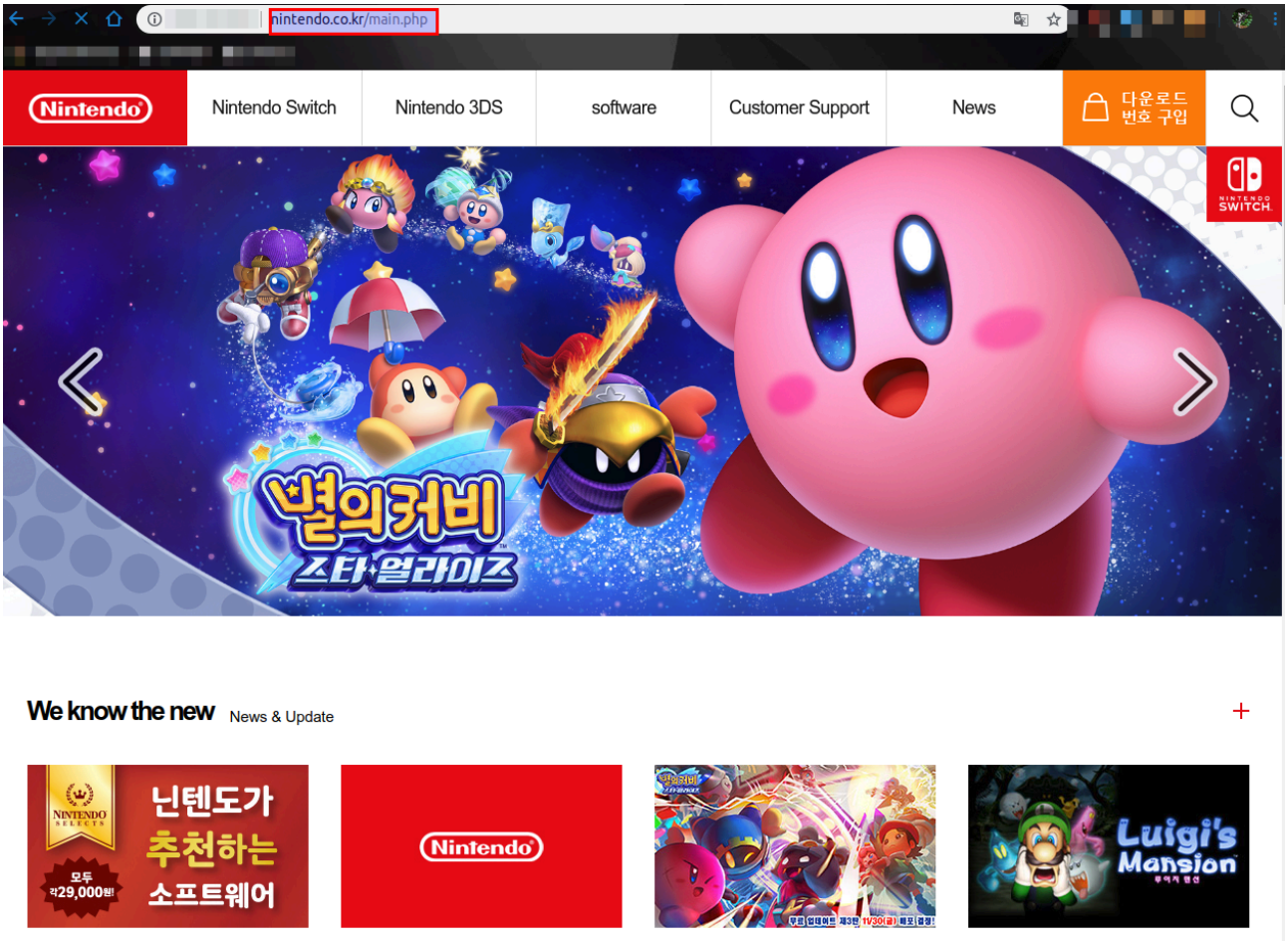
ns21.dollar2host.com / ns22.dollar2host.com (NS)

What domains were using these Name Servers ? First of all there are a LOT of domains.. crappy or legitimate ones. While trying to look around the time of usage for my **microsoft.co.kr** domain, I found several others corporate domains :

- **microsoftstore.co.kr**
- **adobe.co.kr**
- **nintendo.co.kr**

Time Last Seen	Time First Seen ▲	Count	RRname	RRtype	Rdata
2015-08-13 11:18:57	2010-08-26 21:39:44	2360	conexiaperu.com.	NS	ns21.dollar2host.com.
2010-08-26 23:52:03	2010-08-26 23:01:59	30	nintendo.co.kr.	NS	ns21.dollar2host.com.
2010-08-27 02:19:16	2010-08-27 02:19:16	3	thelifestylepartners.com.	NS	ns21.dollar2host.com.
2011-08-26 03:09:50*	2010-08-27 02:54:08*	365	homero.biz.	NS	ns21.dollar2host.com.
2011-08-07 15:24:19	2010-08-27 03:08:00	674	get-rid-of-heartburn.com.	NS	ns21.dollar2host.com.
2011-01-27 09:18:59	2010-08-27 03:14:52	32	sallygallarelli.com.	NS	ns21.dollar2host.com.
2013-06-16 17:29:32	2010-08-27 03:20:35	60	new2know.com.	NS	ns21.dollar2host.com.
2011-05-06 17:43:25	2010-08-27 03:45:17	35	buypspphone.com.	NS	ns21.dollar2host.com.
2010-08-27 15:54:05	2010-08-27 03:48:44	21	microsoftstore.co.kr.	NS	ns21.dollar2host.com.
2010-08-27 19:36:34	2010-08-27 04:56:18	2	adobe.co.kr.	NS	ns21.dollar2host.com.

Ex for Nintendo **today's** website for nintendo.co.kr domain :



I discovered while sweeping through the pages and pages (…) of domains other financial & banking domains but I suppose they answer to another objective because the time they were using the NS is longer : Few months and not hours/minutes and didn't check if domains were legit at the time of if they were mimicking their target's name.

Time Last Seen	Time First Seen ▲	Count	RRname	RRtype	Rdata
2010-12-03 18:09:29*	2010-08-24 18:10:04*	102	comparelendersservice.com.	NS	ns21.dollar2host.com.
2010-12-03 18:09:29*	2010-08-24 18:10:04*	102	usbankmyaccountonline.com.	NS	ns21.dollar2host.com.
2010-12-03 18:09:29*	2010-08-24 18:10:04*	102	hometrustbankingservice.com.	NS	ns21.dollar2host.com.
2010-12-03 18:09:29*	2010-08-24 18:10:04*	102	walmartcreditcardsonline.com.	NS	ns21.dollar2host.com.
2010-12-03 18:09:29*	2010-08-24 18:10:04*	102	ameriquestmdlsettlementservice.com.	NS	ns21.dollar2host.com.
2010-12-04 18:09:16*	2010-08-24 18:10:04*	103	wellsfargofinancialcardsonline.com.	NS	ns21.dollar2host.com.
2012-01-11 18:14:28*	2010-08-24 18:10:04*	500	sexoticas.net.	NS	ns21.dollar2host.com.
2011-06-24 17:49:59	2010-08-24 22:12:27	76	www.joomlamake.com.	CNAME	ns21.dollar2host.com.
2010-11-05 21:52:40*	2010-08-24 22:52:28*	73	ctoc.info.	NS	ns21.dollar2host.com.
2012-01-08 21:53:50*	2010-08-24 22:52:28*	500	schoolgrade.info.	NS	ns21.dollar2host.com.

NB: **chryslerfinancialinfoservice.com** from 2010-08-23 to 2010-11-28 not represented above.

This could be what I call a **batch process** used by threat actor, look at the exact same timing. In these groups, they need to “stick to the rules” to protect (Compartmentalization) the information for security, and their registration process may reveal batch operations.

2018-11-24 Update : Continuing on ns21. I saw that **microsoft.kr was usign briefly this NS in 2010 too :**

2010-08-26 01:05:59	2010-08-26 01:05:59	1	microsoft.kr.	NS	ns21.dollar2host.com.

I found also **ns1.dqtec.com** (and **ns2.dqtec.com**) who where using too **this NS in 2010, e.g with ns1.dqtec.com below**:

2010-08-27 02:13:04	2010-08-26 01:37:05	6	microsoft.co.kr.	NS	ns21.dollar2host.com.
2010-08-27 02:19:16	2010-08-27 02:19:16	3	thelifestylepartners.com.	NS	ns21.dollar2host.com.
2010-08-27 03:31:13	2010-08-15 05:41:25	22	indiantvserials.org.	NS	ns21.dollar2host.com.
2010-08-27 03:34:45	2010-08-25 03:20:33	5	chryslerfinancialinfoservice.com.	NS	ns21.dollar2host.com.
2010-08-27 07:31:49	2010-08-27 07:31:49	9	ns1.dqtec.com.	NS	ns21.dollar2host.com.
2010-08-27 12:22:50	2010-08-20 15:56:30	140	desitvforum.me.	NS	ns21.dollar2host.com.
2010-08-27 14:33:21	2010-08-13 15:42:22	265	e-ordi.com.	NS	ns21.dollar2host.com.
2010-08-27 15:54:05	2010-08-27 03:48:44	21	microsoftstore.co.kr.	NS	ns21.dollar2host.com.

What was the IP resolution of these records ?

ns1.dqtec.com ==> **67.212.186.170**

ns2.dqtec.com ==> **67.212.186.171**

cf:

Time Last Seen ▲	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2010-08-27 07:31:49	2010-08-27 07:31:49	1	dqtec.com.	ns1.dqtec.com.	A	67.212.186.170
2010-08-27 07:31:49	2010-08-27 07:31:49	1	dqtec.com.	ns1.dqtec.com.	NS	ns21.dollar2host.com. ns22.dollar2host.com.
2010-09-09 07:30:57	2010-09-03 07:30:52	8	ns1.dqtec.com.	ns1.dqtec.com.	A	67.212.186.170
2010-09-09 07:30:57	2010-09-03 07:30:52	8	ns1.dqtec.com.	ns1.dqtec.com.	NS	ns21.dollar2host.com. ns22.dollar2host.com.
2010-10-09 08:34:23	2010-08-27 07:31:49	26	com.	ns1.dqtec.com.	A	67.212.186.170
2010-10-26 18:10:06*	2010-08-21 18:10:14*	67	com.	ns1.dqtec.com.	A	67.212.186.170

and :

Time Last Seen ▲	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2010-09-01 07:45:56	2010-09-01 07:45:56	1	dqtec.com.	ns2.dqtec.com.	A	67.212.186.171
2010-09-01 07:45:56	2010-09-01 07:45:56	1	dqtec.com.	ns2.dqtec.com.	NS	ns21.dollar2host.com. ns22.dollar2host.com.
2010-09-15 08:04:58	2010-09-01 07:45:56	19	ns2.dqtec.com.	ns2.dqtec.com.	A	67.212.186.171
2010-09-15 08:04:58	2010-09-01 07:45:56	19	ns2.dqtec.com.	ns2.dqtec.com.	NS	ns21.dollar2host.com. ns22.dollar2host.com.
2010-10-09 08:34:23	2010-08-27 07:31:49	26	com.	ns2.dqtec.com.	A	67.212.186.171
2010-10-26 18:10:06*	2010-08-21 18:10:14*	67	com.	ns2.dqtec.com.	A	67.212.186.171

Now What?

Ecuador

If these IPs used for bad things at the moment (no idea..), some other records may have been pointed to.. Again pivoting :

time_last	time_first	count	rrname	rrtype	rdata
GMT: Tuesday, March 13, 2012 8:08:53 PM	GMT: Tuesday, March 13, 2012 8:08:53 PM	1	hanm.gob.ec.	A	67.212.186.170
GMT: Tuesday, July 30, 2013 1:42:43 AM	GMT: Thursday, June 30, 2011 10:17:21 PM	644	cnecarchi.gob.ec.	A	67.212.186.170
GMT: Friday, June 1, 2012 1:35:36 PM	GMT: Friday, January 21, 2011 6:14:44 AM	111	seyfae.mil.ec.	A	67.212.186.170
GMT: Sunday, October 30, 2011 4:24:29 PM	GMT: Sunday, October 30, 2011 4:24:29 PM	1	academiadeguerraaerea.mil.ec.	A	67.212.186.170

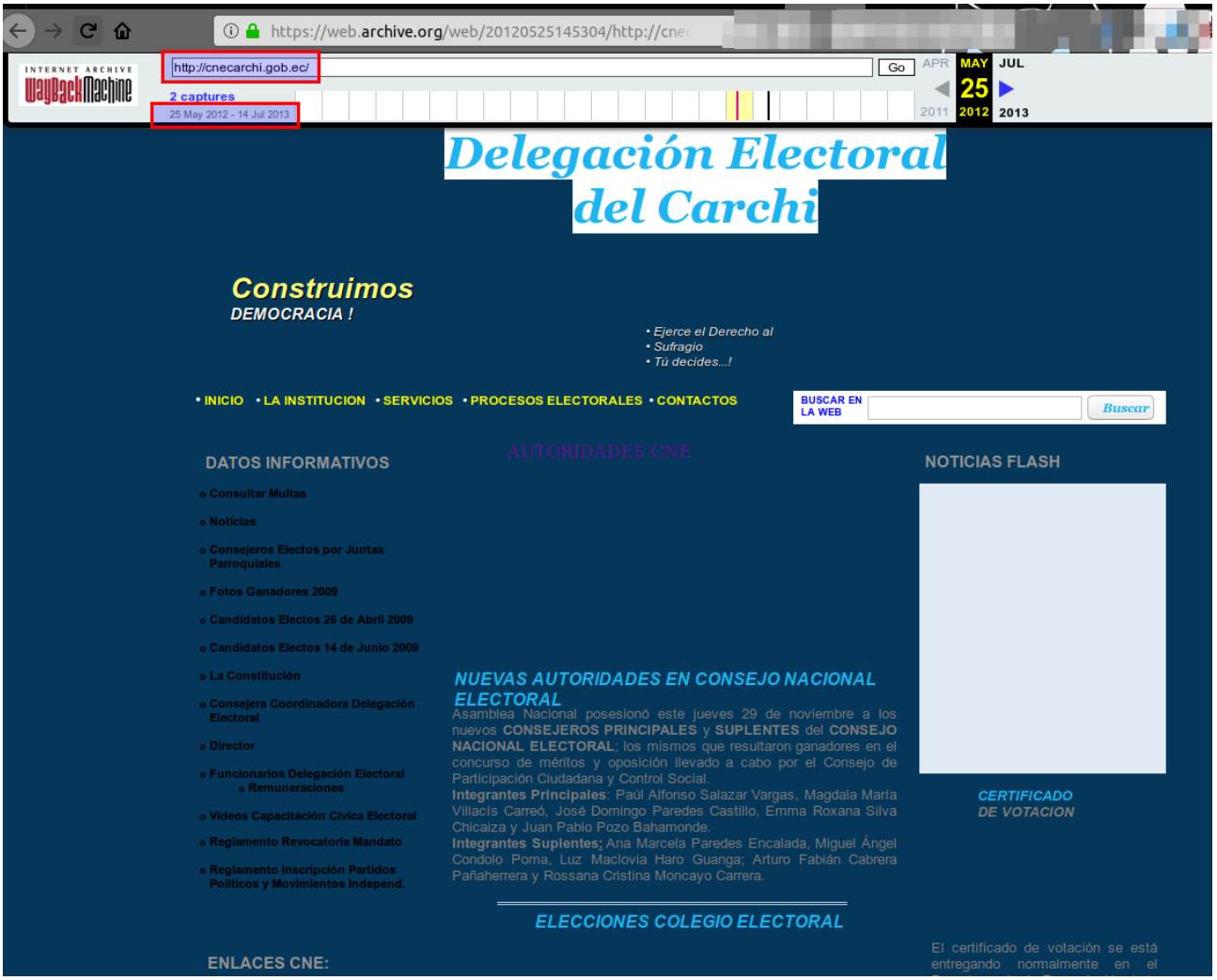
Source: DNSDB

I have no idea if these records were legit at this time. First thing first, referring to Wikipedia, .gob.ec was replaced by .gov.ec :

- **.EDU.EC** Educational entities.
- **.GOB.EC** Government of Ecuador, since July 2010
- **.GOV.EC** Government of Ecuador, being replaced by GOB.EC
- **.MIL.EC** Ecuadorian military

For the domains :

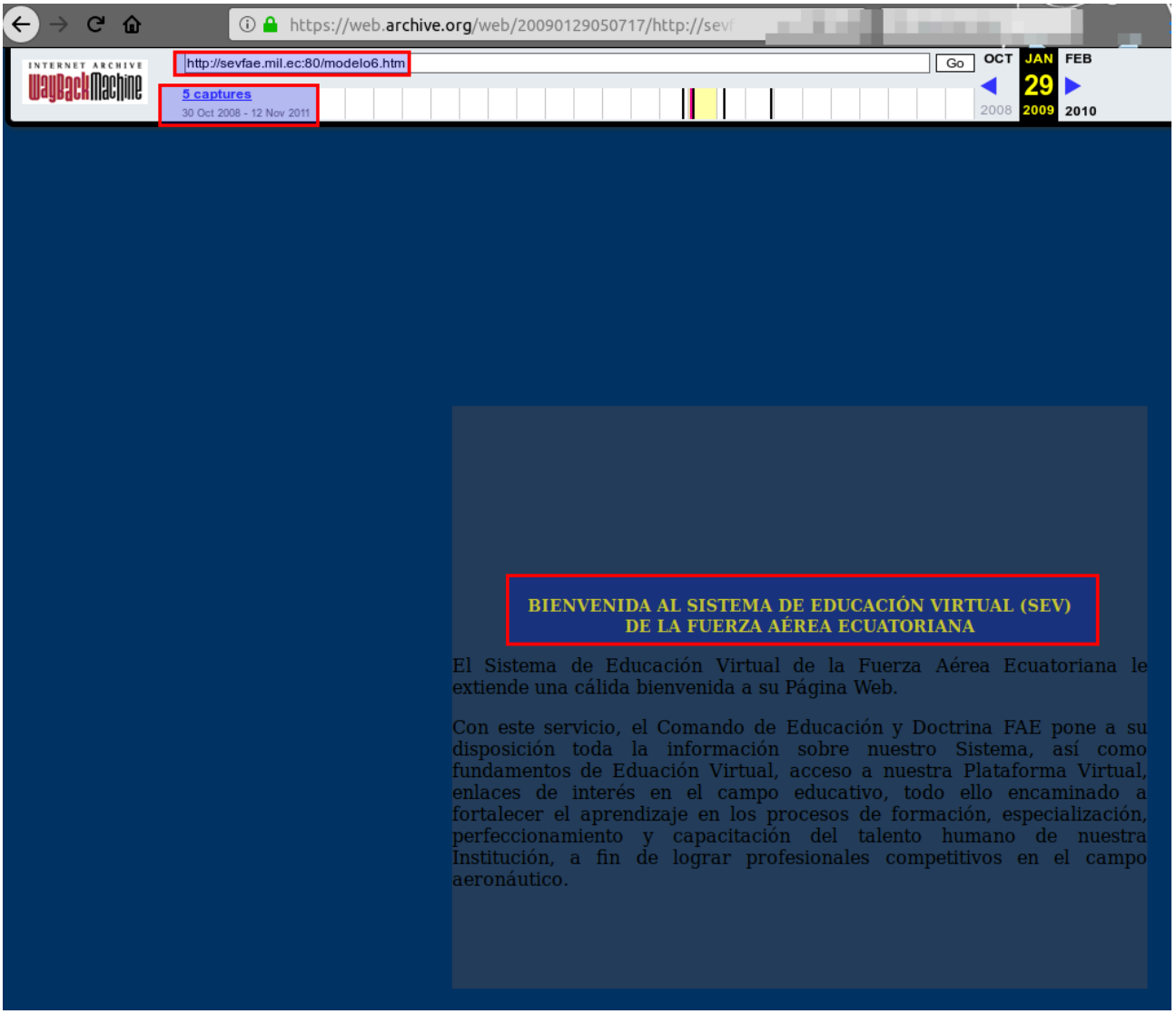
- **hanm.gob.ec** was “el Hospital Provincial Alfredo Noboa Montenegro”.
- **cnecarchi.gob.ec** was la “Delegación Electoral del Carchi”, depending from Ecuador National Electoral Council for “la delgacion de” (translate to approx. “district of”…) Carchi, website at the moment (2012-05-25) :



Nowadays the website :

- **sevfae.mil.ec** : We can interpret the function as globally : Ecuador's Air Force virtual education system. It's a Military website and domain.

At the moment website was :


https://web.archive.org/web/20090129050717/http://sevf
INTERNET ARCHIVE
WayBack Machine
http://sevfae.mil.ec:80/modelo6.htm
Go
OCT
JAN
FEB
5 captures
30 Oct 2008 - 12 Nov 2011
2008
29
2009
2010
BIENVENIDA AL SISTEMA DE EDUCACIÓN VIRTUAL (SEV)
DE LA FUERZA AÉREA ECUATORIANA
El Sistema de Educación Virtual de la Fuerza Aérea Ecuatoriana le extiende una cálida bienvenida a su Página Web.
Con este servicio, el Comando de Educación y Doctrina FAE pone a su disposición toda la información sobre nuestro Sistema, así como fundamentos de Eduación Virtual, acceso a nuestra Plataforma Virtual, enlaces de interés en el campo educativo, todo ello encaminado a fortalecer el aprendizaje en los procesos de formación, especialización, perfeccionamiento y capacitación del talento humano de nuestra Institución, a fin de lograr profesionales competitivos en el campo aeronáutico.

Nowadays :

AGA is “Academia de Guerra Aérea FAE” which translate to Ecuador’s Air Force war academy. This is also “similar” with the last domain below :

- **academiadeguerraaerea.mil.ec**

Illustration nowadays (not same domain..) :

ns0.nscomdomain.com / ns1.nscomdomain.com (NS)

Same process. What domains were using these Name Servers ?

Here when I search for ns0, there's less domains, in fact, only 6, including our **microsoft.co.kr**. All information was from 2012 :

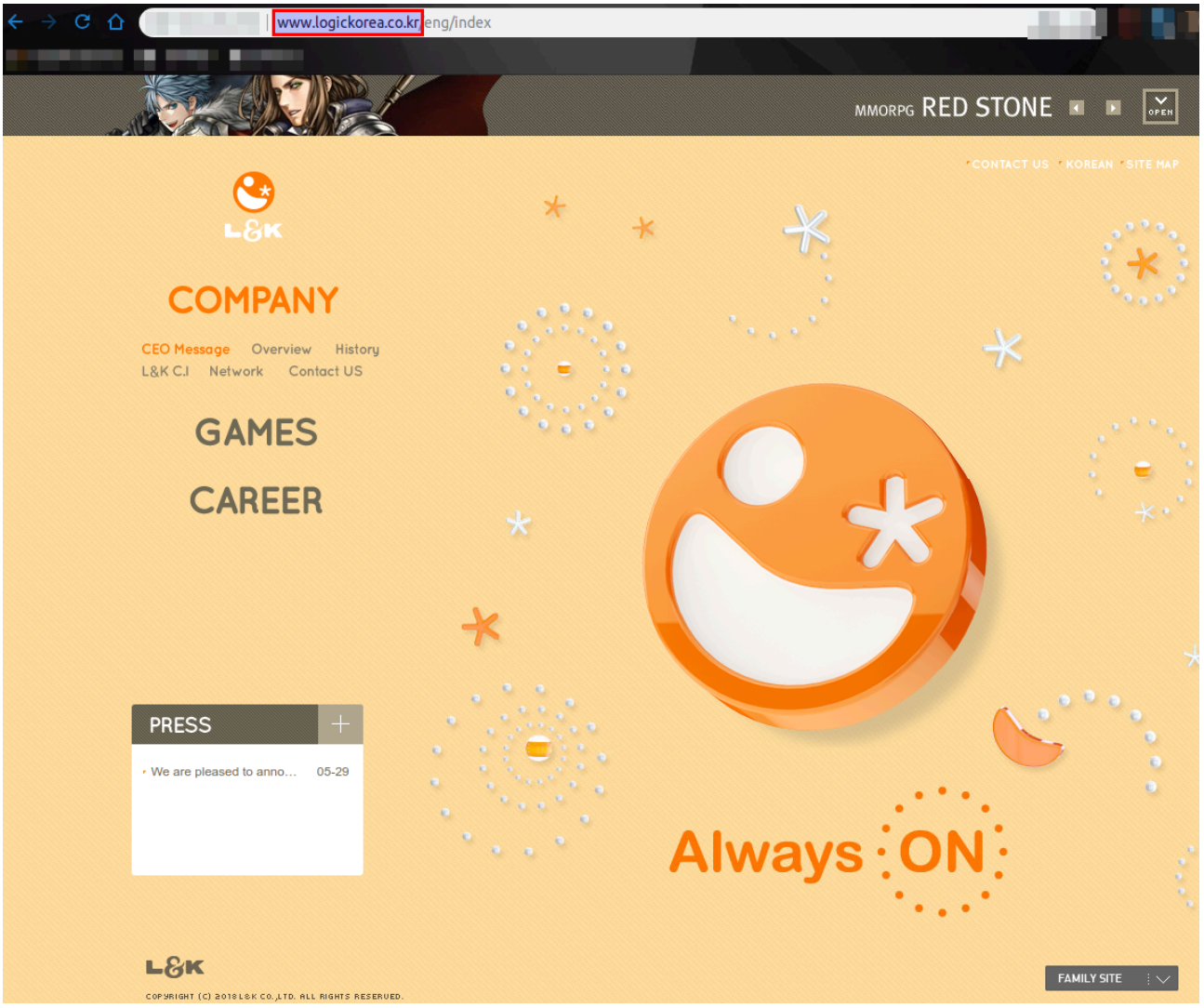
Time Last Seen	Time First Seen ▲	Count	RRname	RRtype	Rdata
2012-10-08 13:04:56	2012-10-08 13:04:56	1	minghui.or.kr.	NS	ns0.nscomdomain.com.
2012-10-10 02:18:37	2012-10-09 16:28:16	62	shinchonji.kr.	NS	ns0.nscomdomain.com.
2012-10-25 00:35:25	2012-10-24 15:36:03	7	logickorea.co.kr.	NS	ns0.nscomdomain.com.
2012-11-22 06:43:04	2012-11-11 06:12:59	30	microsoft.co.kr.	NS	ns0.nscomdomain.com.
2013-02-27 14:37:54	2013-02-27 10:44:08	13	kftc.or.kr.	NS	ns0.nscomdomain.com.
2013-02-27 15:43:18	2013-02-27 15:43:18	4	honeywell.co.kr.	NS	ns0.nscomdomain.com.

Examining these domains I was really surprised to find that **minghui.or.kr was linked to "Faloun Gong" too !** Do you remember at the beginning of this blog post "**guangming.org**" ? That could reveal the same kind of interest by this/these actor(s).

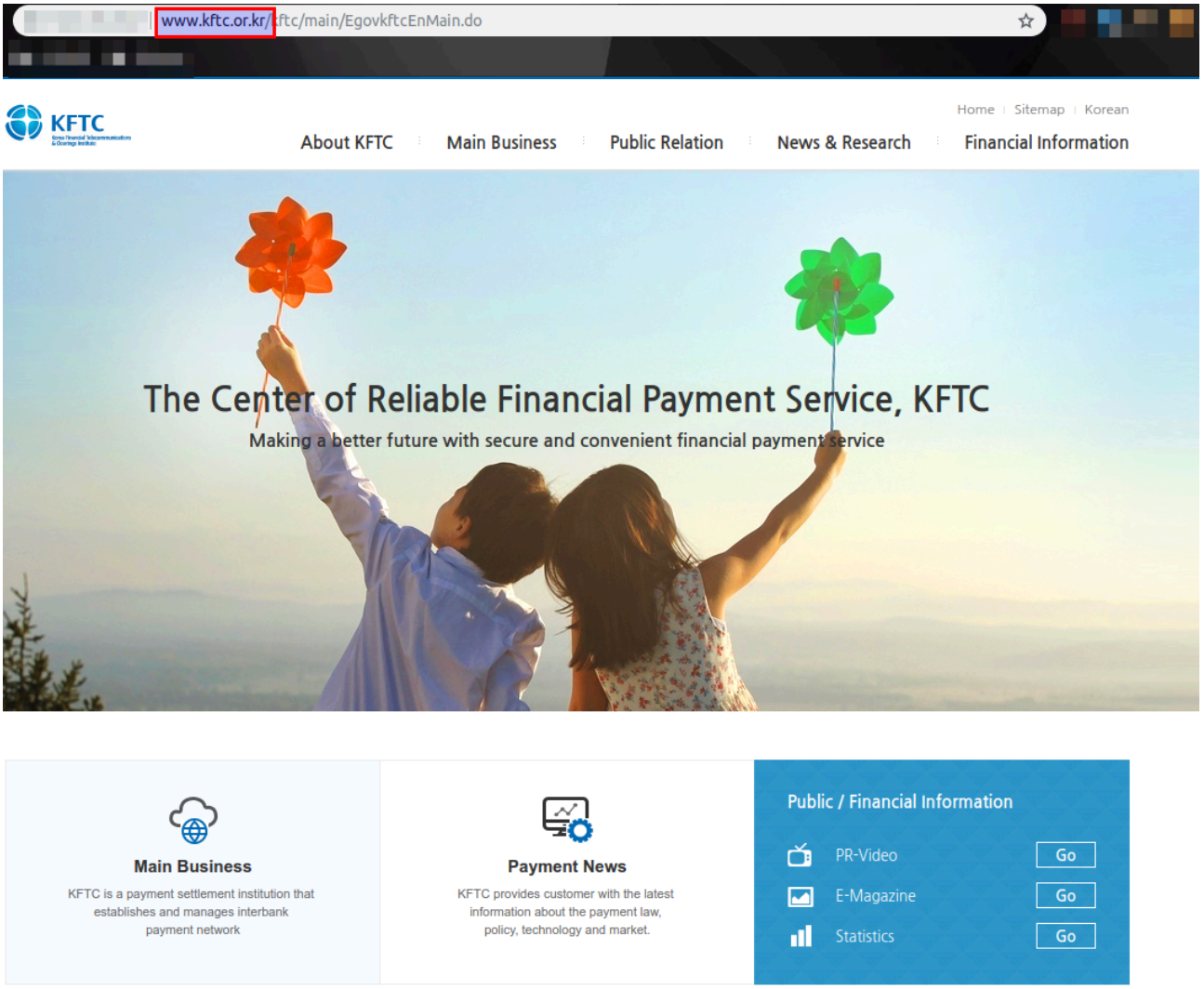
- **shinchonji.kr** is another religious/cult (Evangelists as far as I understand) organization that may represent an interest too for China's monitoring policy.

- **logickorea.co.kr** A Korean Company, in the Video Games business. I immediately think about the APT that targeted Video games industry (Winnti) . As Kaspersky noted noted in its report “Winnti. More than just a game”, South Korean video games vendors were targeted :

> Interestingly, the digital signature belonged to another video game vendor – a private company known as KOG, based in South Korea.

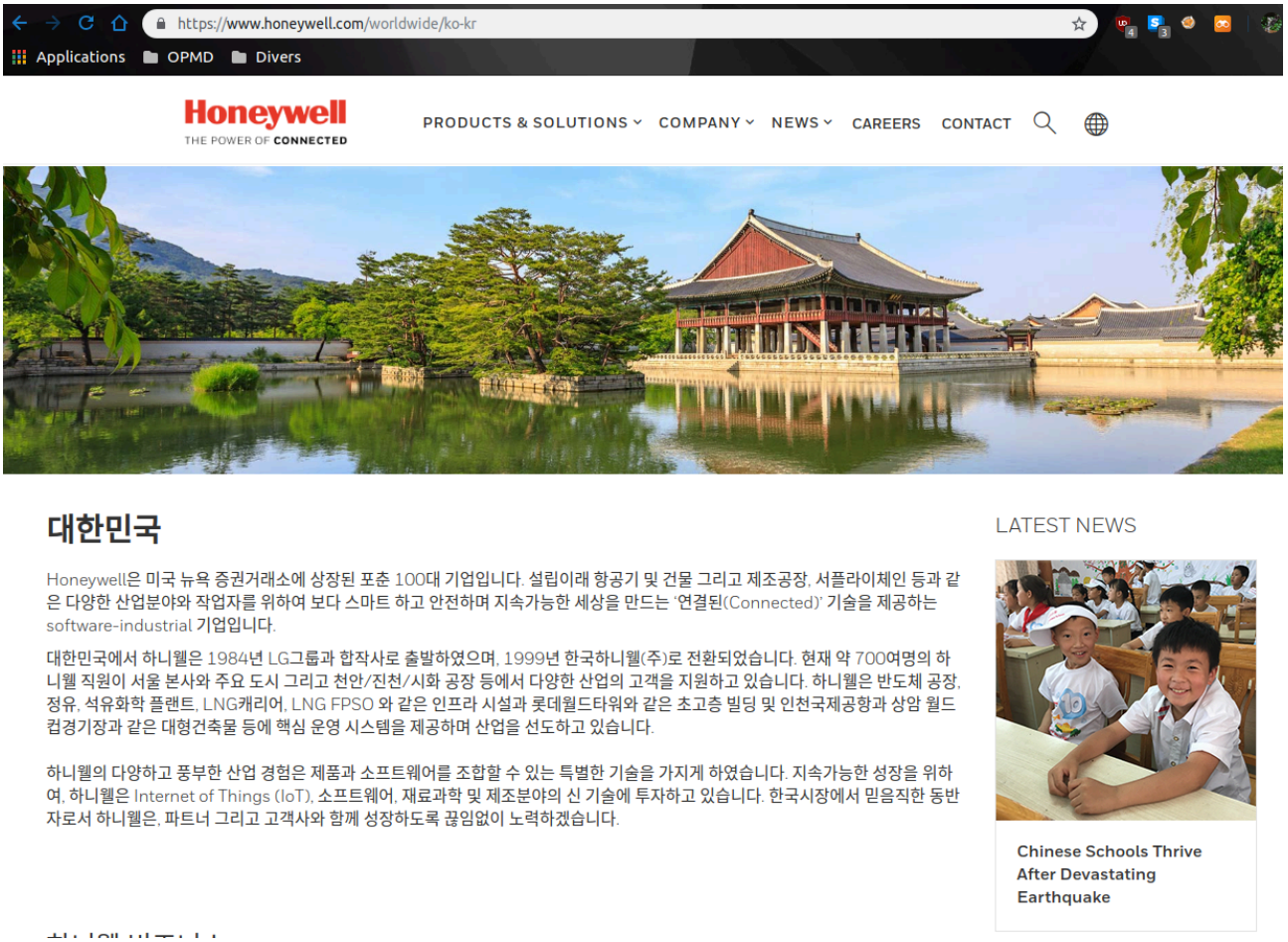


- **kftc.or.kr** is a Korean financial payment service company with a lot of service today : Cash Dispenser (CD) Network, Interbank Fund Transfer(IFT), HOFINET, and The Korea Cash (K-CASH) Network connects KFTC, all banks in Korea and a system service provider (SP) for payment settlements using an electronic currency. The K-CASH would be a target for any Intelligence service on earth, including the Ministry of State Security (MSS / Guoanbu). Do you remember the NSA compromised the SWIFT Network revealed in 2017 ?



- **honeywell.co.kr**

I know that one 🙂 Honeywell, not because I'm a ICS/SCADA guy but because Shodan ! 😉 Anyway, this Honeywell Korean website was in the list too… NB: **honeywell.co.kr** website redirect to **http://www.honeywell.com/worldwide/ko-kr**



Conclusion

Starting from public indicators and passive DNS data, and by looking at the domains, their zone **authoritative name servers**, and the other domains using the latters (**pivoting**) we discovered victims.

The **volume** and **diversity** of domains names suggest that it is likely that **multiple threat actors** were involved. This is also likely that **China's interests** are in line with these operations, especially because of the cultual/religious aspect, which was of utter interest from China at the time of these events. NB: The same kind of interest is e.g from NetTraveler which specifically targets Tibetan/Uyghur activists.

Actors could **use** a service like a **"DNS highjacking" tactic broker** (as Elderwood project was in comparison an APT 0-day-broker), or they are likely to used a **shared process** for this tactic.

By understanding actor's tradecraft, we also shine some light on China's policy, supposed Intelligence services (MSS/Guoanbu), and business needs since 2010 from APT actors (sometime named Turbine Panda / BlackVine & Winnti) where one of the central and common capacity is the **Sakula** malware.

Source: https://cyberthreatintelligenceblog.wordpress.com/2018/11/16/c0ld-case-from-aerospace-to-chinas-interests/