"Your assistance is requested.."

Kauto Huopio
Chief Specialist

National Cyber Security Centre Finland
(NCSC-FI)

Finnish Communications Regulatory Authority
National Cyber Security Centre

Agenda today

- ”The case”
- NCSC-FI practices on incident ”victim notification”
- Challenges in coordination
- Figures
- Conclusions

NCSC-FI in short

- National Cyber Security Centre Finland
- Part of Finnish Communications Regulatory Authority (FICORA)

Key functions that merged into NCSC-FI

- » National CERT, GovCERT-functions (formerly CERT-FI)
- » National Communications Security Authority (formerly NCSA-FI)
  - Information Assurance functions and services
- » Telecommunications service provider security regulation

- ~50 persons, 19 in direct CSIRT activities

The case – humble beginnings

- Message from a U.S. based website operator in September 2013
  - » A site's admin sent a report to (then) CERT-FI about a site that was supposedly hacked from a Finnish source
  - » We forwarded the report to LE (no immediate action)
- House call and arrest: appr.160 Finnish and 300 foreign sites had been breached by means of SQL injection
  - » We thought that this was big
  - » So did the press. END OF THE WORLD.

The plot thickens..

- October 2013: LE asked for cooperation in contacting victims related to another (linked) investigation
- This turned out to be actually a big thing
  - » But, this time the press wasn't that concerned

Incident response coordination

NCSC-FI tools and techniques

Our normal reporting tools..

- Abuse.py, batch_mail.py, inspect-js.py
  - » Inhouse-built (Thanks Jussi & co!) set of scripts
  - » Finding of most propable reporting targets
  - » WHOIS scraping
  - » DNS scraping
  - » (Nationally) AS-based incident reporting contact database
- Report templates to most usual cases
  - » DDOS source, botnet client, malware dropsite, defacement, malicious javascript, phishing site, botnet c&c
  - » Good when handling a fairly limited number of cases..

..were not enough! We got a "present"..

LE requested cooperation

- 2 TB hard drive with "lots of logs"
  - » Dumps from websites
  - » Lists of credentials
  - » Malware samples
  - » Attack tools
  - » Random files that needed to be looked at
  - » It's like walking around in 2nd hand electronics shoppe; "oh.. this is interesting.. oh.. so is this.."
- Our role would be incident handling – victim notification. It turned out to be a LOT of victim notification.

Normal incident response procedures were not enough

- Two incident responders were assigned to the case
  - » Work was done when regular duty officer weeks and other tasks allowed
  - » Scraping the files took longer than expected – the first case of this size, so we had no tools for forensics or analysing ready at hand
  - » Counted together, months of hands-on work for both going through data and preparing the notifications
- Additional tool development went hand in hand with forensics and other preparations
  - » Our abuse arsenal can handle hundreds and even thousands of events but in the end it doesn't scale well

Figures

Finnish Communications Regulatory Authority
National Cyber Security Centre

The Figures

What we found	Unique domains	Unique IPs
Adobe ColdFusion – backdoor (earliest logs dating spring 2013)	49 529	19 008
Active CF backdoors (situation when scanned fall 2013)	570	432
Compromised Parallels Plesk Panels (ACTIVE cases!)	178 283	13 724
SQL Injection cases	360	-

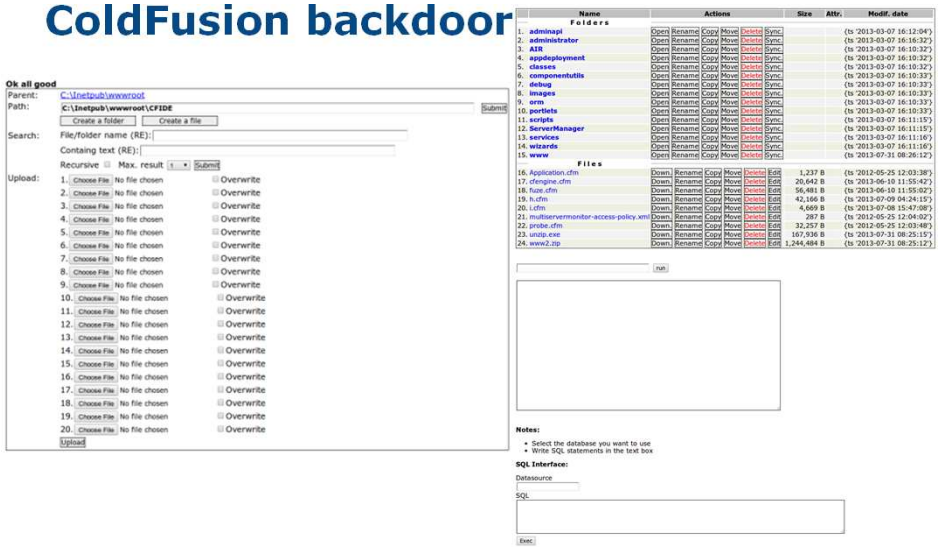
And then some more..

Private RSA keys	**66749**
Database admin credentials	**39145**
Credit card numbers	**~500000**
FTP accounts	**143749**

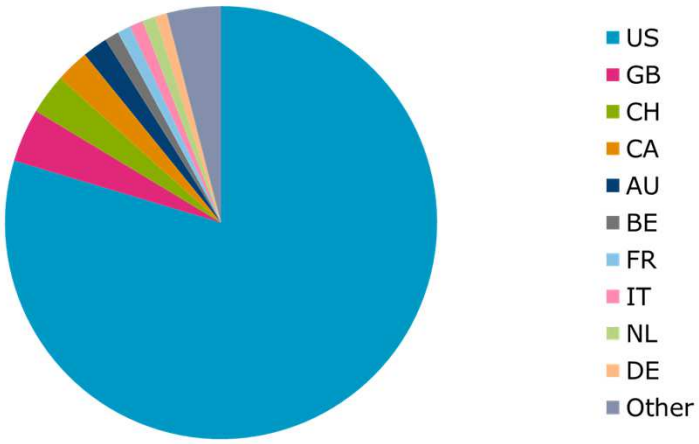
ColdFusion scan

- We performed a scan for all CF backdoor URLs we found.
- We started by doing HTTP HEAD requests to all affected sites. We then retrieved the full page for all those with relevant responses.
- We identified two versions of the backdoor, one password protected and one world-readable.
- Both versions contained unique identifiers we could use for identifying the backdoor.
- A few greps later we had a list of still vulnerable servers 6 months after the initial compromise took place.

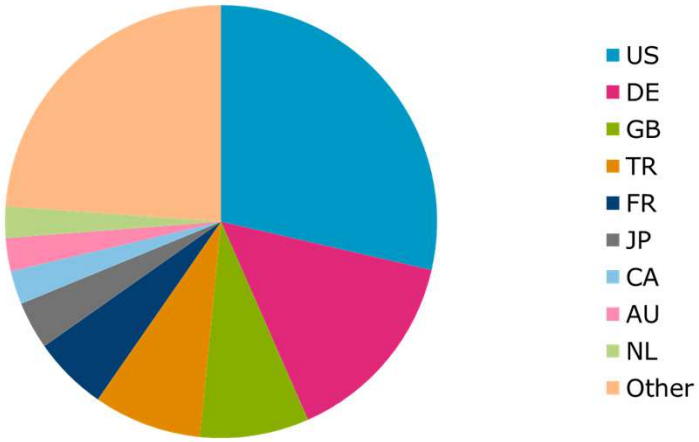
ColdFusion backdoor



ColdFusion breaches by country



Parallells Plesk Panel breaches by country



Challenges in coordination

Challenges in coordination

- The data was and still is part of active LE investigation – sharing the original data (the HD image) to other teams not possible
- When you have this many victims to contact..mostly outside your own constituency, what would be the approach?
  A. Not our problem. Let's leave it like this.
  B. Via regular abuse channels
     -using tools to find contacts from domain whois/dns server/network owner automatically
  C. Via teams of national responsibility

Challenges in coordination

- Going through automation would lead to sending numerous emails to upstream providers, DNS providers and other 3rd parties
  - » Some of them might feel it'd not be their job to contact the potential victims
  - » The service provider might not be the actual SP of the victim
  - » We did not have resources to individually advise all affected service providers
- This in mind, we took option C: National CERTs
  - » There are still some countries without a clear national PoC

Reporting example: ColdFusion

********** CERT-FI Incident ID: 769806

****

CERT-FI is currently busy analysing information related to a series of security breaches. This work will take some time due to the high volume of data involved.

Our intention is to provide relevant results of the analysis to appropriate national CERT teams in order to reach the victims found within their constituencies. We will also inform the teams when all of the data has been analysed. This is the third batch of this kind and the last regarding ColdFusion.

This set of data is related to vulnerable Adobe ColdFusion servers having a backdoor installed. This may have lead to several kinds of malicious activity, such as:

- **Installing rootkit**
- **Spreading malware**
- **DoS attacks**
- **Manipulation of data on the server**
- **SQL database dumping**

These incidents have taken place sometime before spring of 2013. This set contains all the ColdFusion backdoor URLs we found on the confiscated server but were unable to verify. A majority of these have probably already been fixed, however some may still be compromised with a backdoor at some other URL or the backdoor may have been cleaned by the attackers after compromising the system.

The backdoors we have seen consist of two different types, password protected and unprotected.

Password protected backdoors contain the following code:

```
<form method="post">
        <label for="code">Code:</label>
        <input type="text" name="code" />
        <br/>
        <input type="submit" value="Login" />
        </form>
```

Unprotected backdoors contain the word 'FileManager:' and the directory of the ColdFusion installation in the HTML title-tag.

We kindly ask the local CERT teams to contact the owners of the targeted servers. The systems should be analysed for possible breaches and updated to current software versions.

We recommend the victims to check their servers for signs of compromise even if no backdoor is currently present at the reported location, unless such an investigation has been previously conducted. It is also important to inform the users of the compromised services about the breach and advise or force them to e.g. change their credentials.

Finnish LE has arrested a suspect related to this case.

The LE contact in this case is <...>

Reporting: Plesk Panel -cases

The Plesk server configuration file (Server Backup file) was downloaded by the attackers from the hacked Plesk Panel servers. The backups contained usernames and passwords for e-mail accounts, FTP-accounts, SSH-accounts and databases as well as private RSA keys and certificates stored on the Plesk Panel.

This information may have been used for malicious activity, such as:

-Installing a backdoor on the compromised website
-Spreading malware
-DoS attacks
-Manipulation of data on the server
-SQL database dumping

These incidents have taken place in April 2013

Plesk panel vector

The attackers utilized a SQL-injection vulnerability in enterprise/control/agent.php (CVE-2012-1557) to gain access to the Plesk Panel API RPC and download server configuration backups. The backup was then deleted from the server.

The most widespread case for us – challenges to reach even national PoCs!

- Victims in 100+ countries
  - » FIRST: 301 teams across 65 countries
- A lot of contact-finding needed
  - » FIRST directory
  - » TERENA TI directory
  - » Kauto's rolodex ☺
  - » Assistance requests on various forums
    - Did you see our requests on FIRST mailing lists?
- **A CSIRT team website doesn't mean that the team is active and responsive**

Is there an "expiry date" of a website intrusion?

- How old cases should you even report?
  - » If the original vulnerability has been patched, has the backdoor also been removed?
- How much information should you include to be taken seriously?
  - » In some cases additional information was indeed required, several times
- Real-life response from a ISP in this case: ***"Should we really deal with 10 months old incidents? A waste of our time?"***

Feedback..

- ... appears to be difficult
  - » A handful of teams contacted responded with feedback
  - » Some request more information
  - » The rest stayed silent
- Did the information really go through?
  - » Was our message delivered to victims?
- Was our information package sufficient?
  - » Something more?

Have you received a abuse/problem report? Best practices..

- **Analyse**
  - » Is the reported problem in my constituency?
  - » Valid issue?
  - » Can I act? (Can I forward the message)
- **Reply**
  - » KEEP the tags on Subject: line
  - » State your intentions
  - » Indicate your own case ID (with your tag on Subject: -line)
- **Act!**
- **Acknowledge/Report actions**
  - » What was done, observations, further recommendations

Have something to report out? Best practices..

- Provide your case ID as a tag on Subject: -line
- Describe problem in a clear and concise manner
  - » Your counterpart is not likely using English as a primary language
- Provide incident data in a processable format
  - » "CYMRU"-format preferred is the de-facto least common denominator
  - » Prepare yourself for STIX/TAXII –world!
- Provide ACTIONABLE reports
- On a case involving IP addresses – TIMESTAMPS are a nescessity!
  - » NAT devices at customer locations / operator NAT
  - » Provide timezone, UTC strongly recommended
  - » Accuracy essential!

Good CERT / LE cooperation essential!

- CERT <-> LE cooperation can be very productive to both parties
  - » LE – catching criminals – slow cooperation
  - » CSIRTS – notifying victims – fast and agile practices
- CSIRT can facilitate LE contacts on permission by the reporting source
  - » In some cases CSIRT is required to report a case to LE
- Arrange and maintain relations in due time

Conclusions

Finnish Communications Regulatory Authority
National Cyber Security Centre

Final observations

- Prepare for a ”big one” with planning
  - » Consider teaming up with other CSIRTs – distributing the analysis workload
- Figure out a schedule and stick on it
- If your data is >1 year old (but still valid!) – prepare for resistance
- Good information packs are essential
- Prepare to be overwhelmed by press
  - » Have your advisories or statements ready
- We could not do this without YOUR assistance!

Finnish Communications Regulatory Authority
National Cyber Security Centre


Thank You