"Your assistance is requested.."

Kauto Huopio
Chief Specialist

National Cyber Security Centre Finland

Agenda today

- Incident response and our way of doing it
- Challenges in coordination
- Figures
- Conclusions

The Humble beginning

- 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 (not immediate action)
- We received information that n.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..

- Soon after the first case LE asked for cooperation in contacting victims related to another investigation
- This turned out to be actually a big thing
    - » But, this time the press wasn't that concerned

Incident response

Our normal reporting tools..

- Abuse.py, mass_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 database
- Report templates to most usual cases
  - » DDOS source, botnet client, malware dropsite, defacement, javascript malware, phishing site, botnet c&c
  - » Good when handling a fairly limited number of cases..

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

- [INSERT PICTURE OF THE HD]

LE requested cooperation

- 2 TB hard drive with "lots of logs"
  - Dumps from websites
  - Lists of credentials
  - 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 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

The Figures

What we found	Unique domains	Unique IPs
Adobe Cold Fusion – backdoor (logs dating spring 2013)	49 529	19 008
Adobe Cold Fusion –backdoor (situation when scanned fall 2013)	570	432
Parallels Plesk –vulnerability (ACTIVE cases!)	178 283	13 724
SQL Injection cases	360	-

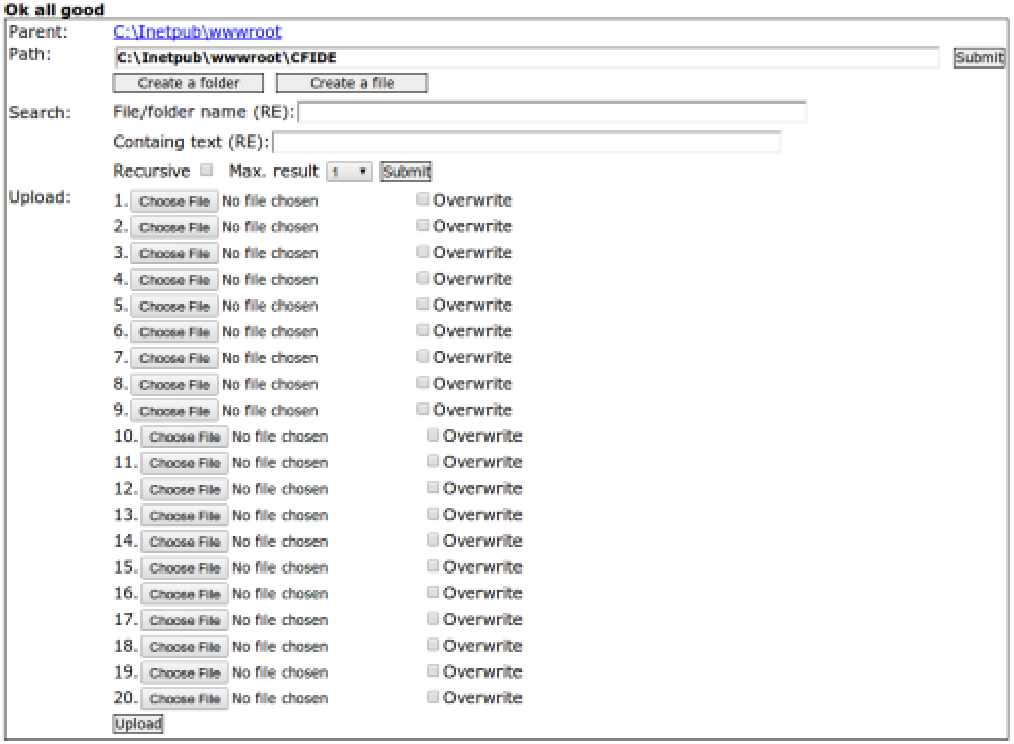
And then some more..

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



Ok all good

Parent: C:\Inetpub\wwwroot

Path: C:\Inetpub\wwwroot\CFIDE [Submit]

[Create a folder] [Create a file]

Search: File/folder name (RE):

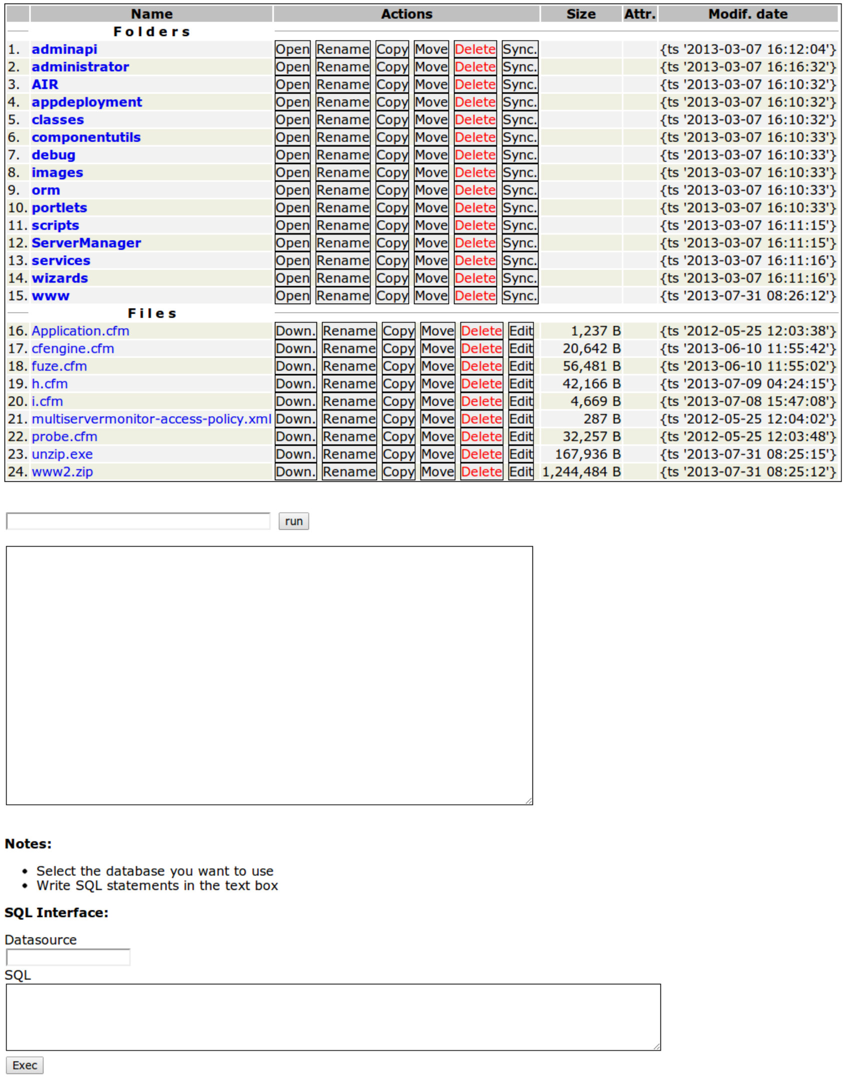
Containg text (RE):

Recursive □ Max. result 1 [Submit]

Upload:

1. [Choose File] No file chosen □ Overwrite
2. [Choose File] No file chosen □ Overwrite
3. [Choose File] No file chosen □ Overwrite
4. [Choose File] No file chosen □ Overwrite
5. [Choose File] No file chosen □ Overwrite
6. [Choose File] No file chosen □ Overwrite
7. [Choose File] No file chosen □ Overwrite
8. [Choose File] No file chosen □ Overwrite
9. [Choose File] No file chosen □ Overwrite
10. [Choose File] No file chosen □ Overwrite
11. [Choose File] No file chosen □ Overwrite
12. [Choose File] No file chosen □ Overwrite
13. [Choose File] No file chosen □ Overwrite
14. [Choose File] No file chosen □ Overwrite
15. [Choose File] No file chosen □ Overwrite
16. [Choose File] No file chosen □ Overwrite
17. [Choose File] No file chosen □ Overwrite
18. [Choose File] No file chosen □ Overwrite
19. [Choose File] No file chosen □ Overwrite
20. [Choose File] No file chosen □ Overwrite

[Upload]



	Name	Actions	Size	Attr.	Modif. date
	Folders				
1.	**adminapi**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:12:04'}
2.	**administrator**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:16:32'}
3.	**AIR**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:32'}
4.	**appdeployment**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:32'}
5.	**classes**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:32'}
6.	**componentutils**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:33'}
7.	**debug**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:33'}
8.	**images**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:33'}
9.	**orm**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:33'}
10.	**portlets**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:10:33'}
11.	**scripts**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:11:15'}
12.	**ServerManager**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:11:15'}
13.	**services**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:11:16'}
14.	**wizards**	Open Rename Copy Move Delete Sync.			{ts '2013-03-07 16:11:16'}
15.	**www**	Open Rename Copy Move Delete Sync.			{ts '2013-07-31 08:26:12'}
	Files				
16.	Application.cfm	Down. Rename Copy Move Delete Edit	1,237 B		{ts '2012-05-25 12:03:38'}
17.	cfengine.cfm	Down. Rename Copy Move Delete Edit	20,642 B		{ts '2013-06-10 11:55:42'}
18.	fuze.cfm	Down. Rename Copy Move Delete Edit	56,481 B		{ts '2013-06-10 11:55:02'}
19.	h.cfm	Down. Rename Copy Move Delete Edit	42,166 B		{ts '2013-07-09 04:24:15'}
20.	i.cfm	Down. Rename Copy Move Delete Edit	4,669 B		{ts '2013-07-08 15:47:08'}
21.	multiservermonitor-access-policy.xml	Down. Rename Copy Move Delete Edit	287 B		{ts '2012-05-25 12:04:02'}
22.	probe.cfm	Down. Rename Copy Move Delete Edit	32,257 B		{ts '2012-05-25 12:03:48'}
23.	unzip.exe	Down. Rename Copy Move Delete Edit	167,936 B		{ts '2013-07-31 08:25:15'}
24.	www2.zip	Down. Rename Copy Move Delete Edit	1,244,484 B		{ts '2013-07-31 08:25:12'}

[run]

Notes:

- Select the database you want to use
- Write SQL statements in the text box

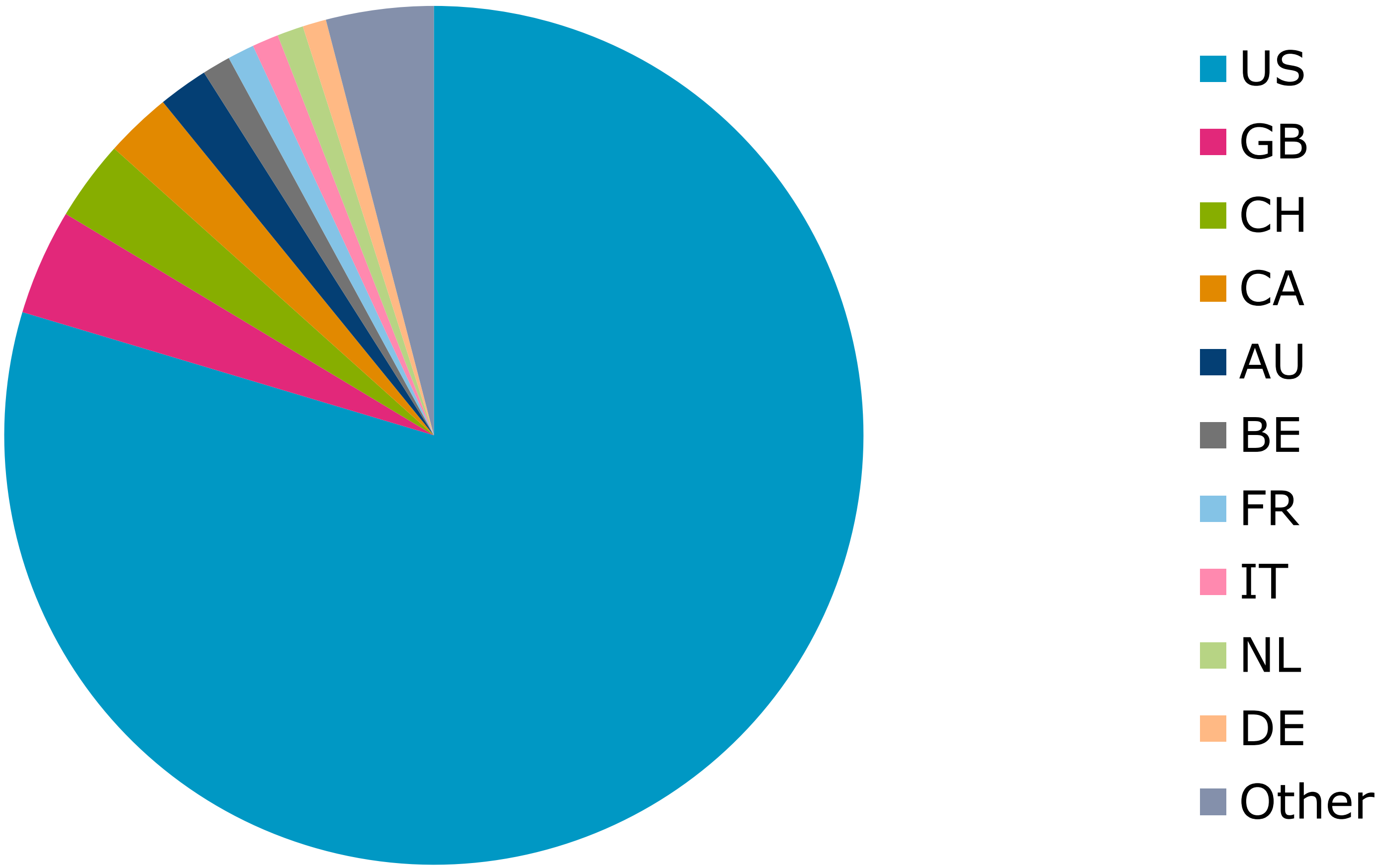
SQL Interface:

Datasource

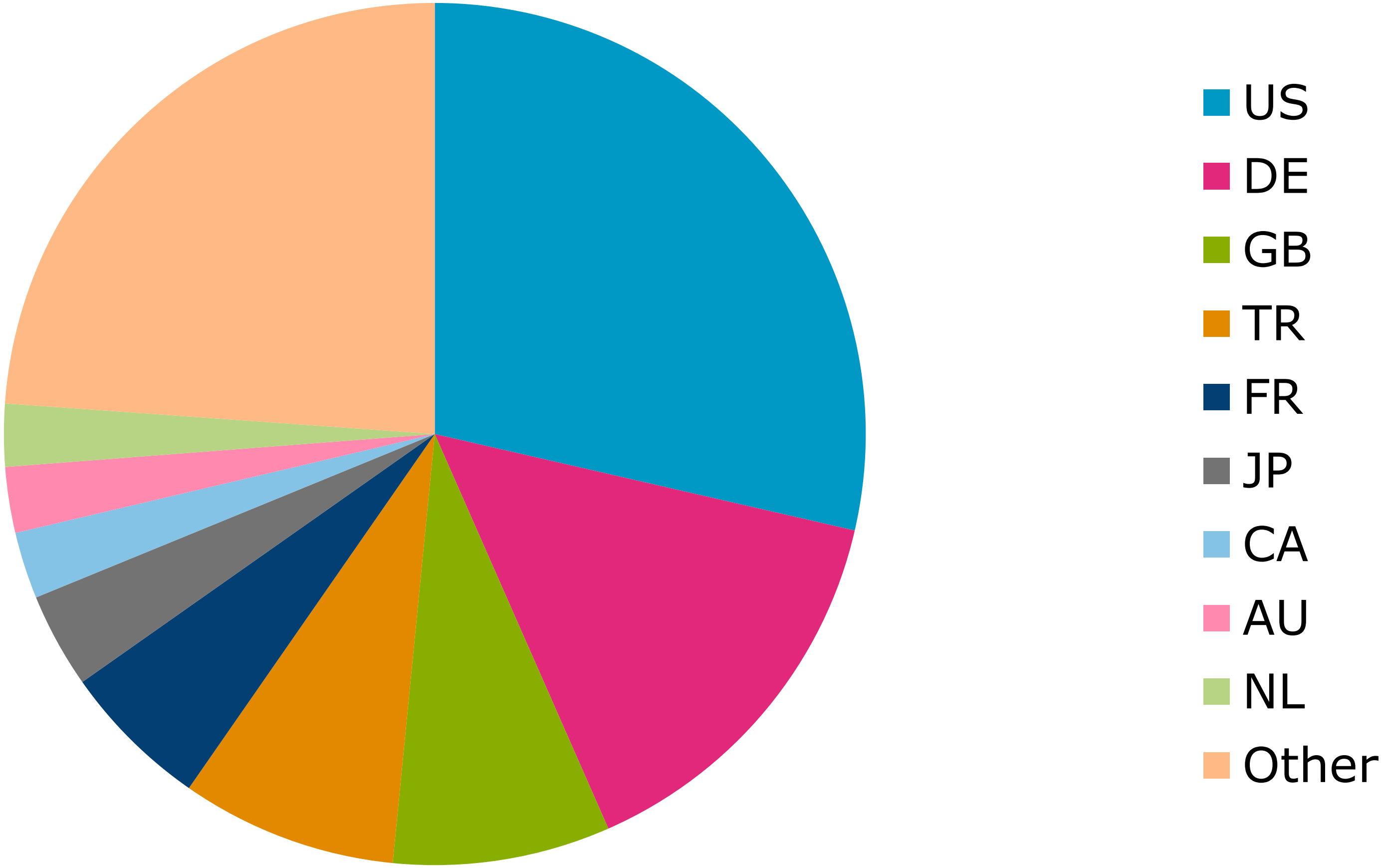
SQL

[Exec]

ColdFusion breaches by country



Parallells Plesk Panel breaches by country



Challenges in coordination

Challenges in coordination

- When you have this many victims to contact..mostly outside your own constituency, what would be the best approach?

  A. Not our problem. Let's leave it like this.

  B. Via our regular abuse channels

     -using our 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
- This in mind, we took option B: National CERTs
  - » There are still some countries without a clear national PoC

The most widespread case for us

- Victims in 100+ countries
- A lot of contact-finding needed
  - Did you see our messages on FIRST mailing lists?
- A CSIRT team website doesn't mean that the team is active and responsive

What is a expiry date of a vulnerable site?

- 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

Feedback..

- ... appears to be difficult
- So you've contacted the CERTs around the world
  - » Perhaps a handful gives feedback
  - » Some request more information
  - » The rest stay silent
- Did the information really go through?
  - » No assurance on how many countries acted on the info.
- Was our infopackage sufficient?
  - » Something more?

Conclusions

Got a abuse/problem report? Best practices..

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

Got something to report out?
Best practices..

- Provide your case ID as a tag on Subject: -line
- Describe problem in a clear and concise manner
- Provide incident data in a processable format
  - » "CYMRU"-format preferred as the least common denominator
  - » Prepare yourself for STIX/TAXII –world!
- On a case involving IP addresses – TIMESTAMPS are a nescessity!
  - » NAT devices at customer locations / operator NAT
  - » Provide timezone, UTC strongly recommended
  - » Accuracy!

Good CERT / LE cooperation essential!

- While we are not a law enforcement agency,, we can and will contact the LE when possible and required
- CERT <-> LE cooperation can be very productive to both parties
  - » LE – catching criminals - slow
  - » CSIRTS – notifying victims – fast and agile
- LE contact on permission by the reporting source
  - » In some cases mandated reporting
- Arrange and maintain relations in due time

Conclusions and final observations

- Prepare with appropriate resources
  - » Consider teaming up with other CSIRTs
- 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!

Finally..