

IRTF Update

Leif Nixon

NDGF security officer, EGI CSIRT

April 23, 2012

What's happened since Lyon?

Incidents, incidents, incidents.

I won't bother updating the overview table from the last two F2Fs; the story is the same. . .

Same old, same old

- Incidents happen because credentials get stolen
- Sites haven't installed patches, so they get rooted
- There is no reliable logging, so it's hard to trace the incident

Same old, same old

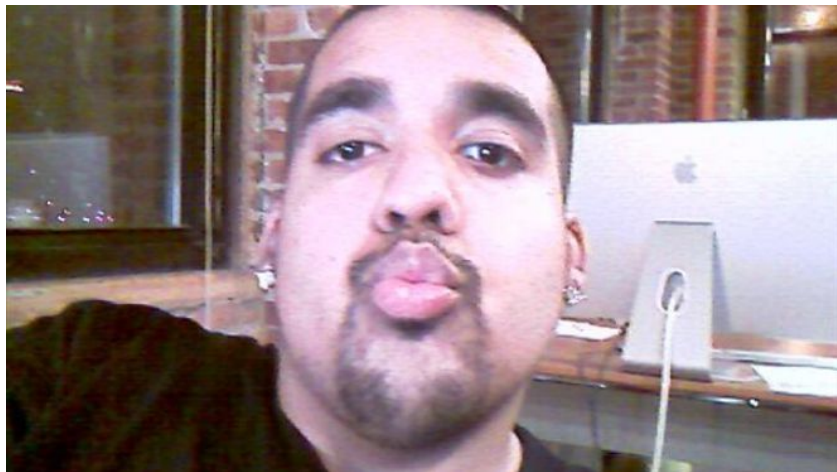
- Incidents happen because credentials get stolen
- Sites haven't installed patches, so they get rooted
- There is no reliable logging, so it's hard to trace the incident

(OK, this is a bit unfair. Observational bias: we mostly only see the sites that get into trouble, not the ones that perform well.)

War on subperforming sites

- We have talked about metrics for a long time; this is now nearing completion. Pretty graphs help build political pressure.
- Perhaps we should have sanctions against underperforming sites (today we only have the penalty of death through suspension).
- Training and security drills. I think Sven has some interesting ideas here.

Good news!



Good news!



Sabu – Hector Xavier Monsegur, arrested 7 June 2011

Good news!



Sabu – Hector Xavier Monsegur, arrested 7 June 2011
FBI informant until March 6, 2012!

Lulzsec in jail

Tflow	<i>arrested July 19, 2011</i>
Topiary	Jake Davis, <i>arrested July 27, 2011</i>
Recursion	Cody Kretsinger, <i>arrested September 22, 2011</i>
Kayla	Ryan Ackroyd, <i>arrested March 6, 2012</i>
Pwnsauce	Darren Martyn, <i>arrested March 6, 2012</i>
Palladium	Donncha O'Cearrbhail, <i>arrested March 6, 2012</i>
Anarchaos	Jeremy Hammond, <i>arrested March 6, 2012</i>

w0rmer in jail

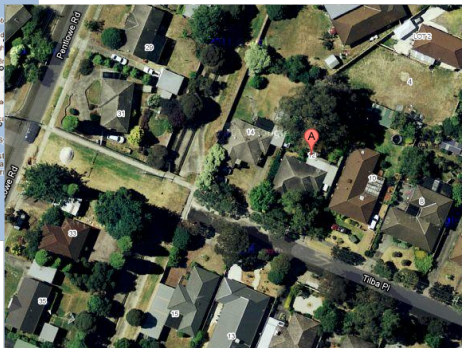
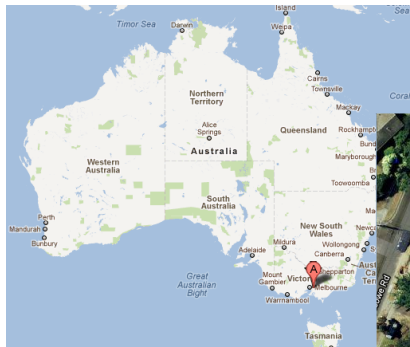


This image was published by w0rmer after the CabinCr3w group hacked law enforcement websites in Arizona.

wOrmer in jail

```
$ jhead wOrmer.jpg
Camera make : Apple
Camera model : iPhone 4
Date/Time : 2012:02:06 14:08:23
Resolution : 540 x 651
Flash used : No (auto)
Focal length : 3.8mm
Exposure time: 0.067 s (1/15)
Aperture : f/2.8
ISO equiv. : 200
Whitebalance : Auto
Metering Mode: spot
Exposure : program (auto)
GPS Latitude : S 37d 51.42m 0s
GPS Longitude: E 145d 15.02m 0s
GPS Altitude : 60.23m
```

w0rmer in jail



This handily pinpoints the location of w0rmer's girlfriend, which leads LE to w0rmer himself, one Higinio O. Ochoa III.

On the morning of New Year's Eve, I get a message from Adam – bad incident in Poland. Sigh.

- The intrusion is traced to KAIST in Korea. . .

On the morning of New Year's Eve, I get a message from Adam – bad incident in Poland. Sigh.

- The intrusion is traced to KAIST in Korea. . .
- from KAIST to University of Twente in the Netherlands (who reports it to the police) . . .

On the morning of New Year's Eve, I get a message from Adam – bad incident in Poland. Sigh.

- The intrusion is traced to KAIST in Korea. . .
- from KAIST to University of Twente in the Netherlands (who reports it to the police) . . .
- from UTwente to German academic systems

On the morning of New Year's Eve, I get a message from Adam – bad incident in Poland. Sigh.

- The intrusion is traced to KAIST in Korea. . .
- from KAIST to University of Twente in the Netherlands (who reports it to the police) . . .
- from UTwente to German academic systems

On the morning of New Year's Eve, I get a message from Adam – bad incident in Poland. Sigh.

- The intrusion is traced to KAIST in Korea. . .
- from KAIST to University of Twente in the Netherlands (who reports it to the police) . . .
- from UTwente to German academic systems

Here I used my eminent detective skills to construct a theory of the individuals behind the intrusions. Which seems to have been all wrong. :)

Then, on February 14, a modified sshd is discovered on the Stallo supercomputer at the university of Tromsø, in Norway. *My turf!*

Then, on February 14, a modified sshd is discovered on the Stallo supercomputer at the university of Tromsø, in Norway. *My turf!*

And on a new supercomputer system in Iceland, yet to be inaugurated.

Then, on February 14, a modified sshd is discovered on the Stallo supercomputer at the university of Tromsø, in Norway. *My turf!*

And on a new supercomputer system in Iceland, yet to be inaugurated.

And on a bunch of systems at multiple departments at the University of Trondheim.

Then, on February 14, a modified sshd is discovered on the Stallo supercomputer at the university of Tromsø, in Norway. *My turf!*

And on a new supercomputer system in Iceland, yet to be inaugurated.

And on a bunch of systems at multiple departments at the University of Trondheim.

And on several academic systems in the Czech Republic. (Daniel's turf.)

All these incidents were obviously part of EGI-20121231-01; the malware and hosts involved made that very clear.

This time we also discovered that the compromised hosts were connected to an IRC server in Korea.

There was no access control on the server. Connecting to it, one could find the nicks dwaan and xS as admins on the bot channels.

This time we also discovered that the compromised hosts were connected to an IRC server in Korea.

There was no access control on the server. Connecting to it, one could find the nicks dwaan and xS as admins on the bot channels.

Conveniently, the High Tech Crime Unit of the national Dutch police also monitored the channels.

So, a couple of weeks ago, xS was arrested in the Netherlands, and dwaan was brought in for questioning in Australia.

I believe this is the first time somebody has been arrested in connection with an EGI incident.

Interestingly, both had recently been in contact with Sabu. I think we will see arrests for a long time, thanks to Sabu. . .

Focus group time!

Now, time for *you* to work.

Form three groups of approx. 4 people. Please come up with:

- a list of three things that we do well
- a list of three things that we do not so well
- *preferably*: suggestions what to about the bad things