Eg-CERT lessons learned

By Ahmed Mashaly

Cyber security awareness Department manager

The real start

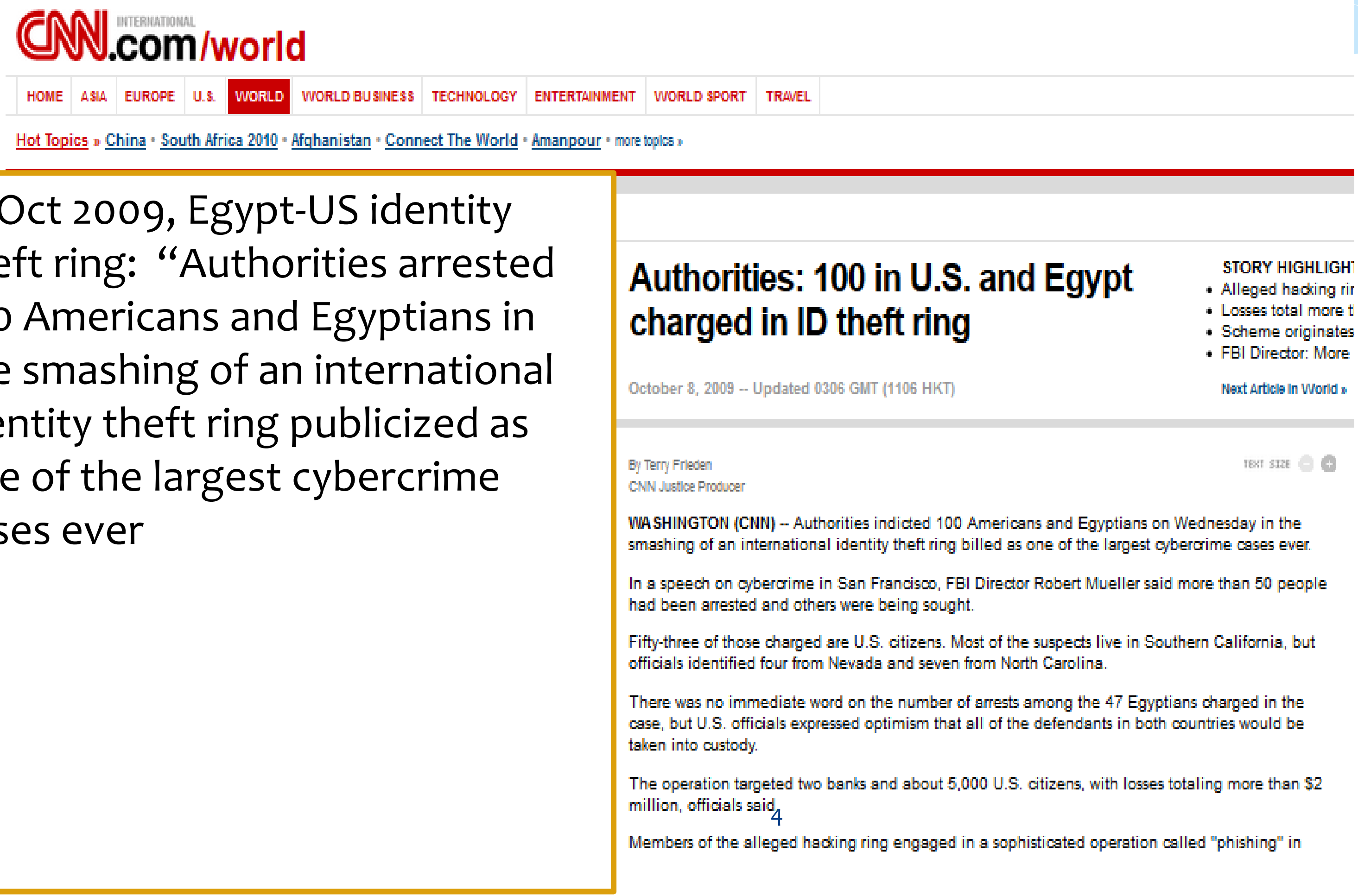
- 1-2 years before the official start in 4/2009.

The start

- As usual with CERTs, we started with an incident response team.
- 6 team members, now we are around 35 team members.
- Now we have (incident handling, Digital forensics, malware analysis and penetration testing)
- We were hit by a major national case that required digital forensic analysis.

Phish Phry…

In Oct 2009, Egypt-US identity theft ring: "Authorities arrested 100 Americans and Egyptians in the smashing of an international identity theft ring publicized as one of the largest cybercrime cases ever


CNN INTERNATIONAL .com/world
HOME
ASIA
EUROPE
U.S.
WORLD
WORLD BUSINESS
TECHNOLOGY
ENTERTAINMENT
WORLD SPORT
TRAVEL
Hot Topics » China • South Africa 2010 • Afghanistan • Connect The World • Amanpour • more topics »
TEXT SIZE

Authorities: 100 in U.S. and Egypt charged in ID theft ring

October 8, 2009 -- Updated 0306 GMT (1106 HKT)

STORY HIGHLIGHT

- Alleged hacking rir
- Losses total more t
- Scheme originates
- FBI Director: More

Next Article in World »

By Terry Frieden
CNN Justice Producer

WASHINGTON (CNN) -- Authorities indicted 100 Americans and Egyptians on Wednesday in the smashing of an international identity theft ring billed as one of the largest cybercrime cases ever.

In a speech on cybercrime in San Francisco, FBI Director Robert Mueller said more than 50 people had been arrested and others were being sought.

Fifty-three of those charged are U.S. citizens. Most of the suspects live in Southern California, but officials identified four from Nevada and seven from North Carolina.

There was no immediate word on the number of arrests among the 47 Egyptians charged in the case, but U.S. officials expressed optimism that all of the defendants in both countries would be taken into custody.

The operation targeted two banks and about 5,000 U.S. citizens, with losses totaling more than $2 million, officials said.

Members of the alleged hacking ring engaged in a sophisticated operation called "phishing" in

Vision

- Having a vision.
- Knowing exactly where you are and where you want to be.

Major difficulties

- Getting the political leadership on board.
- Which organization will incubate the CERT.

NTRA
EGYPT
الجهـــاز القومـــى لتنظيـــم الإتصـــالات
NATIONAL TELECOM REGULATORY AUTHORITY

Major difficulties

Major difficulties

- Recruiting the appropriate calibers and building the needed knowledge.
- communication with entities that are vital to our goals.

Major difficulties

- Communicating and Enforcing the needed actions with different telecom leaders (ISPs, Mobile operators, ..etc)
- Awareness and Education for critical infrastructure IT staff (governmental entities, banks,…)
- The process of building a CERT team and an incident handling process (from our experienced partners)

Models

- Choosing a model (incident response only, incident response + awareness, malware analysis,… .)
- A new model that focuses on industrial control systems and infrastructure protection.
- Also mobile security.

Commnication

- Try to find a way to communicate and stay in touch with your stake holders and your community (conferences, periodical meetings, newsletters, even social media)

Questions