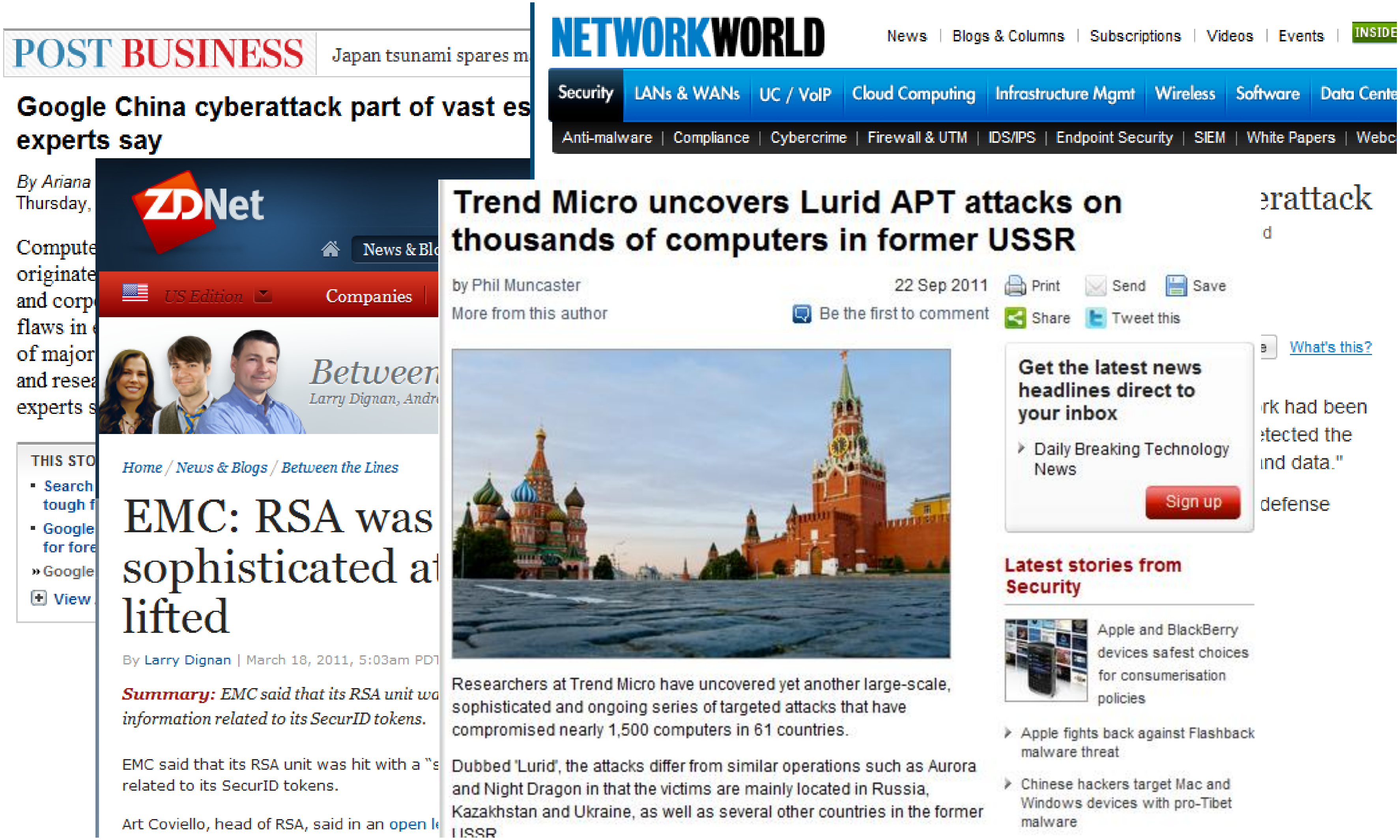
Sherlock Holmes and the Case of the Advanced Persistent Threat

Ari Juels Ting-Fang Yen

RSA Laboratories

April 24, 2012

In the news



POST BUSINESS | Japan tsunami spares m

Google China cyberattack part of vast es experts say

By Ariana
Thursday,

Compute
originate
and corp
flaws in
of major
and resea
experts s

THIS STO
- Search tough f
- Google for fore

» Google
View

erattack
d

What's this?

rk had been
tected the
nd data."

defense

Between
Larry Dignan, Andr

Home / News & Blogs / Between the Lines

EMC: RSA was sophisticated at lifted

By Larry Dignan | March 18, 2011, 5:03am PDT

***Summary:** EMC said that its RSA unit wa information related to its SecurID tokens.*

EMC said that its RSA unit was hit with a "s related to its SecurID tokens.

Art Coviello, head of RSA, said in an open le

NETWORKWORLD
News | Blogs & Columns | Subscriptions | Videos | Events | INSIDE
Security | LANs & WANs | UC / VoIP | Cloud Computing | Infrastructure Mgmt | Wireless | Software | Data Cente
Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SIEM | White Papers | Webc

Trend Micro uncovers Lurid APT attacks on thousands of computers in former USSR

by Phil Muncaster
More from this author

22 Sep 2011
Be the first to comment

Researchers at Trend Micro have uncovered yet another large-scale, sophisticated and ongoing series of targeted attacks that have compromised nearly 1,500 computers in 61 countries.

Dubbed 'Lurid', the attacks differ from similar operations such as Aurora and Night Dragon in that the victims are mainly located in Russia, Kazakhstan and Ukraine, as well as several other countries in the former USSR

Get the latest news headlines direct to your inbox

- Daily Breaking Technology News

Sign up

Latest stories from Security

- Apple and BlackBerry devices safest choices for consumerisation policies
- Apple fights back against Flashback malware threat
- Chinese hackers target Mac and Windows devices with pro-Tibet malware

What is APT?

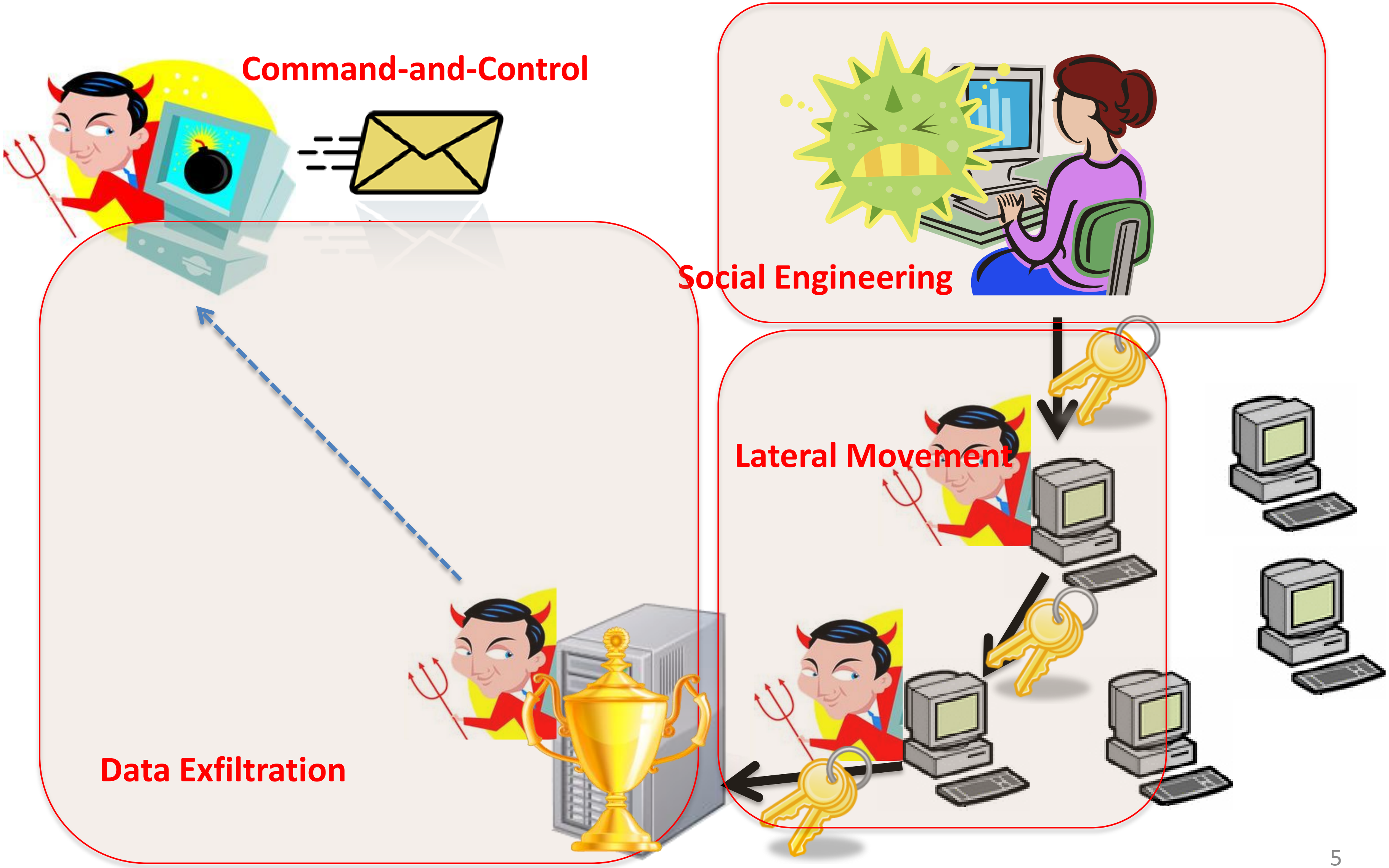
- Advanced
  - "Operate[s] in the full spectrum of computer intrusion." [Bejtlich'10]
- Persistent
  - Maintains presence
  - Targeted
- Threat
  - Well-resourced, organized, motivated

Is this new?

	Traditional attackers	APT
Means of exploitation	Software vulnerabilities, Social engineering	
Objective	Spam, DoS attack, Identity theft	Espionage, Intellectual property theft
Motive	Fame, Financial gain	Military, Political, Technical
Target	Machines with certain configurations	Users
Scope	Promiscuous	Specific
Timing	Fast	Slow
Control	Automated malware	Manual intervention

- Who cares?

How does it work?



An APT isn’t a playbook.
It’s a *campaign*.

Let’s explore the possibilities…

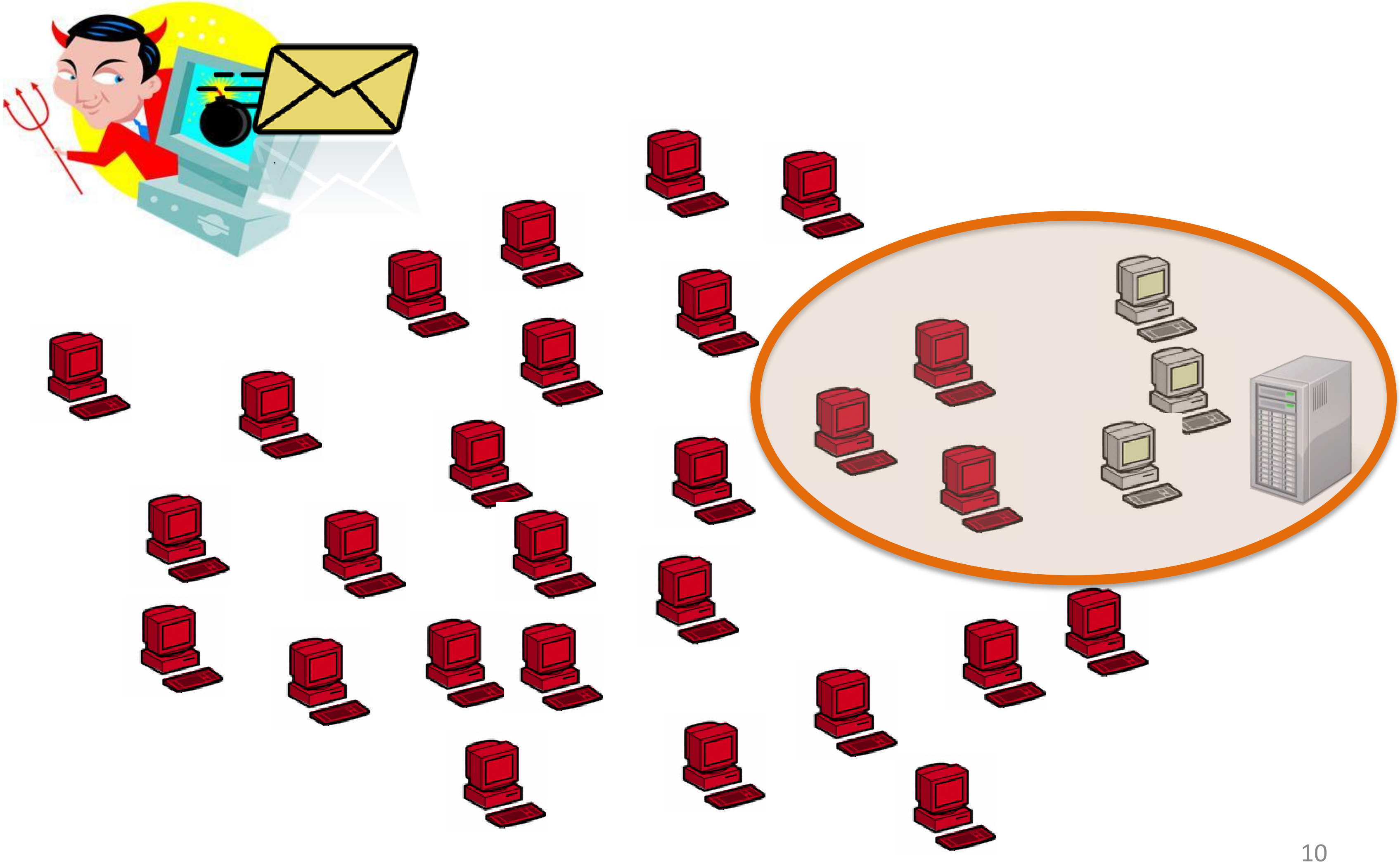
The Adventure of the Red-Headed League

[From north, south, east, and west every man who had a shade of red in his hair had tramped into the city to answer the advertisement. Fleet Street was choked with red-headed folk...]

The Red-Headed-League Attack:

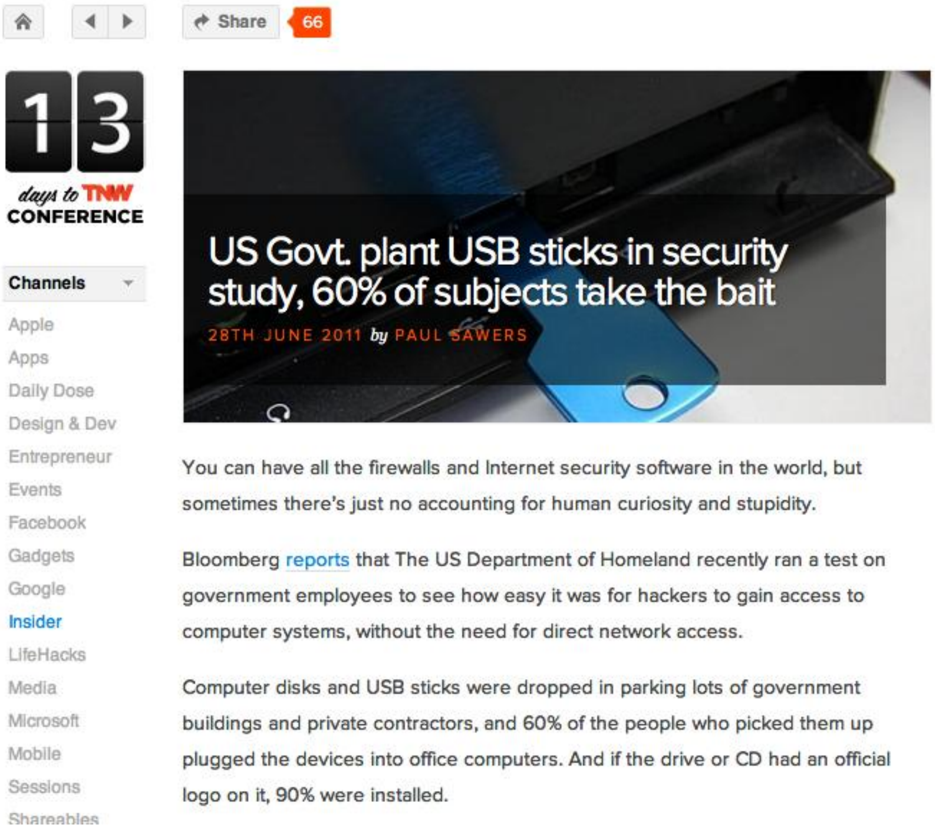
Encompass a victim in a general event that conceals a targeted attack.

Example: A Red-Headed Botnet



Other Red-Headed Attacks

- Open source software
- Social networks
  - “Friend-finding” f
- Free USB sticks



US Govt. plant USB sticks in security study, 60% of subjects take the bait

28TH JUNE 2011 by PAUL SAWERS

You can have all the firewalls and Internet security software in the world, but sometimes there's just no accounting for human curiosity and stupidity.

Bloomberg reports that The US Department of Homeland recently ran a test on government employees to see how easy it was for hackers to gain access to computer systems, without the need for direct network access.

Computer disks and USB sticks were dropped in parking lots of government buildings and private contractors, and 60% of the people who picked them up plugged the devices into office computers. And if the drive or CD had an official logo on it, 90% were installed.

The Adventure of the Blue Carbuncle

[I was leaning against the wall at the time and looking at the geese which were waddling about round my feet, and suddenly an idea came into my head...]

The Blue-Carbuncle Attack:

Conceal unauthorized communications within commonplace objects or activities.

Blue Carbuncles in APTs

HTTP, FTP

*4.2.04.TIFF-1.0 (INDEXED, 1 LAYER) 512X512
File Edit Select View Image Layer Colors Tools Dialogs Filters
px
100%
Background (2.27 MB)

A Scandal in Bohemia

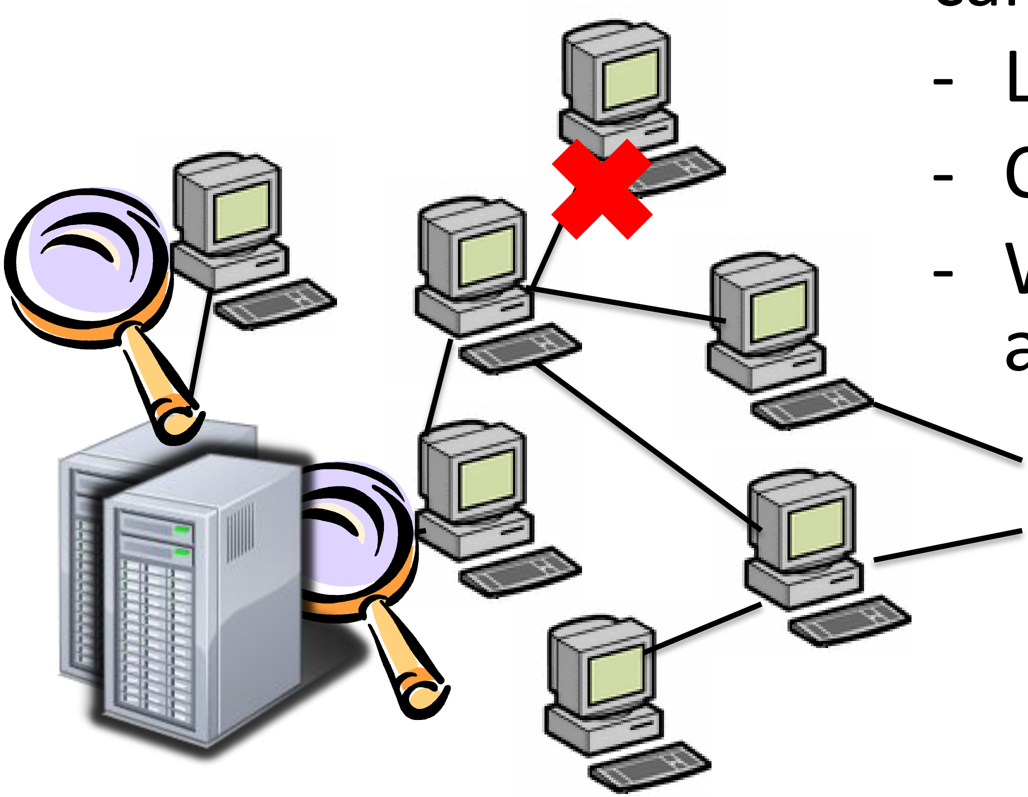
[The alarm of fire was admirably done. The smoke and shouting were enough to shake nerves of steel. She responded beautifully.]

The Bohemian-Scandal Attack:

Create disturbances to the victim to obtain intelligence about a target resource.

A Bohemian APT

- Recommended responses to a breach…



can reveal…

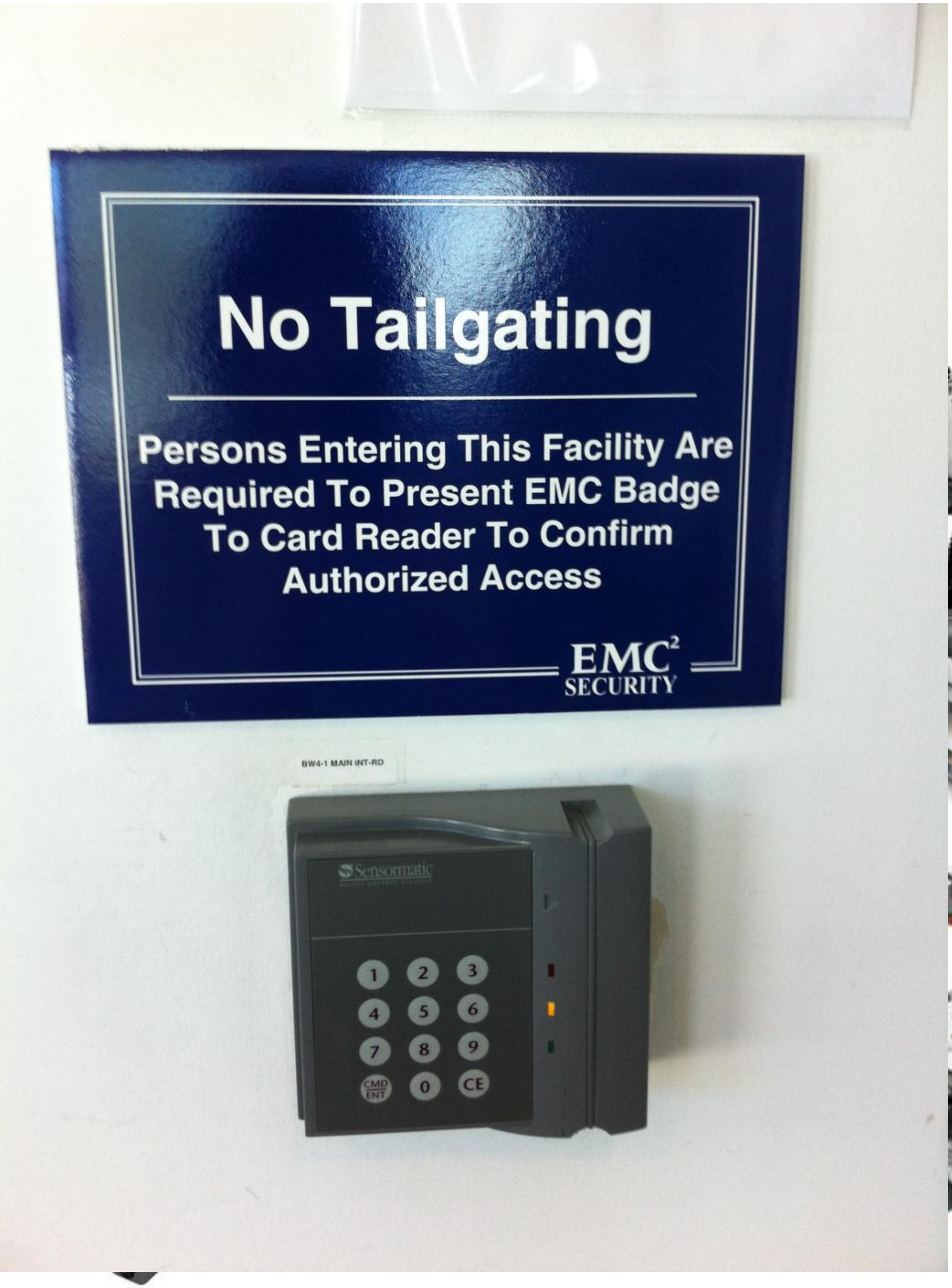
- Location of valuables
- Critical services
- What you know about the attack

The Adventure of the Speckled-Band

[… it became clear to me that whatever danger threatened an occupant of the room could not come either from the window or the door. My attention was speedily drawn, as I have already remarked to you, to this ventilator…]

The Speckled-Band Attack:

Breach a security perimeter through unconventional means.



No Tailgating

Persons Entering This Facility Are Required To Present EMC Badge To Card Reader To Confirm Authorized Access

EMC²
SECURITY

Other Ropes and Ventilators

- Infected digital photo frames
- Infected mobile phones
- Bluetooth vulnerabilities
- Compromised device drivers
- The locked-room illusion…

APT is a campaign

- Broaden conceptualization of APTs
  - No formula or playbook of tactics
- How about detection?
  - Behavior profiling
  - Defensive deception
  - Information sharing

Thank you!