Challenges in Critical Infrastructure Security

Corrado Leita

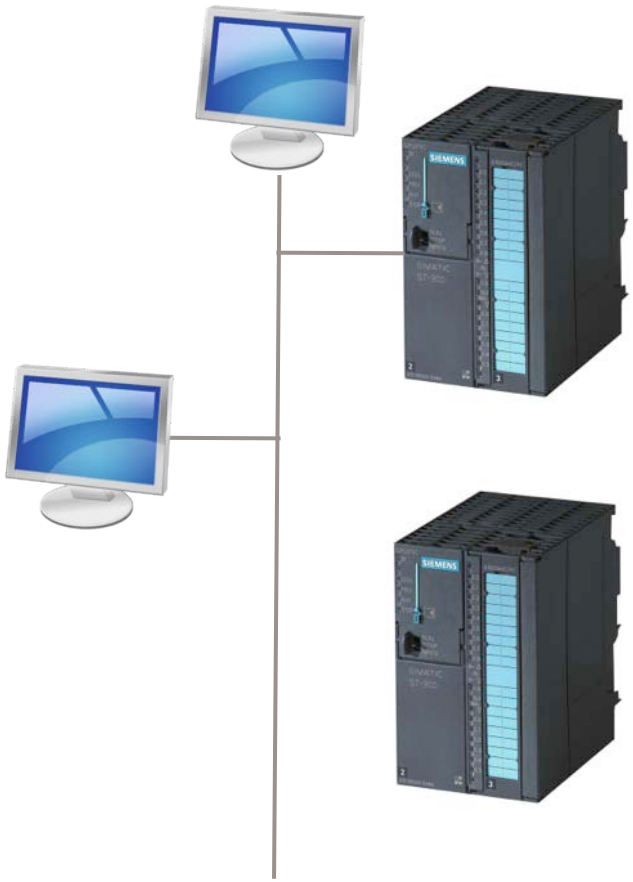
Symantec Research Labs

Symantec Research Labs

- Symantec Research Labs
  - Sophia Antipolis, FR
  - Dublin, IE
  - Culver City, CA
  - Herndon, VA
- European projects:
  - **WOMBAT (2008-2011):** Worldwide Observatory of Malicious Behaviors and Attack Threats
  - **VIS-SENSE (2011-2013):** Visual Analyitics of Large Datasets for Enhancing Network Security
  - **BIGFOOT (2012-2014):** Big Data Analytics of Digital Footprints
  - **CRISALIS (2012-2014):** CRitical Infrastructure Security AnaLysIS

Convergence between IT and ICS technologies

- Interconnection of standard computer systems with industrial control systems
- An **opportunity**?
  - Lower costs and increased system efficiency
  - Opportunity to leverage standard IT techniques (intrusion detection, file scanning, standard hardening techniques, …)
  - Opportunity to enable ICS suppliers to manage and support ICS devices at scale
- A **threat**?
  - Enable attacks and incidents that are typical of standard IT environments
  - Enable attacks on critical infrastructures and environments such as energy, gas, medical
  - Privacy violations from data being more widely available



Culture

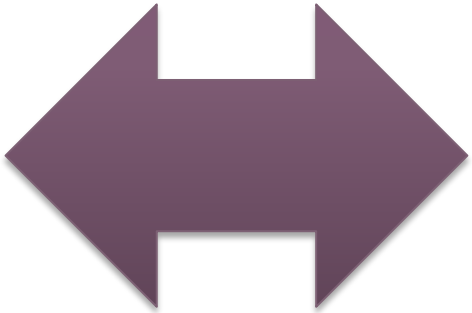
Environments

ICS Security

Threats

Different priorities

How can I prevent unauthorized individuals from accessing my data?



How can avoid a downtime?

The Washington Post

NATIONAL

Corrections | Energy & Environment | Health & Science | Higher Educa

In the News | Super Bowl commercials | Madonna | Josh Pc

Checkpoint Washington

Reporting on diplomacy, intelligence and military affairs

On Twitter | E-Mail Checkpoint | More national security news | RSS Feed

ABOUT THIS BLOG

Checkpoint Washington is produced by the national security staff of The Washington Post.

E-mail us
Follow us on Twitter:
@checkpointwash

SUBSCRIBE

Posted at 12:44 PM ET, 11/18/2011

Foreign hackers targeted U.S. wa apparent malicious cyber attack,

By Ellen Nakashima

Foreign hackers caused a pump at an Illinois week, according to a preliminary state report attack, if confirmed, would be the first known the systems that supply Americans with wate essentials of modern life.

Lessons

➔ *Those systems can, in most cases, be* ***remotely accessed*** *by employees and contractors via VPN!*

➔ *Is it* ***possible*** *to burn-out a water pump by solely interfacing with the SCADA layer? Fail-safe mechanisms exist to prevent physical damage!*

Culture

Environments

ICS Security

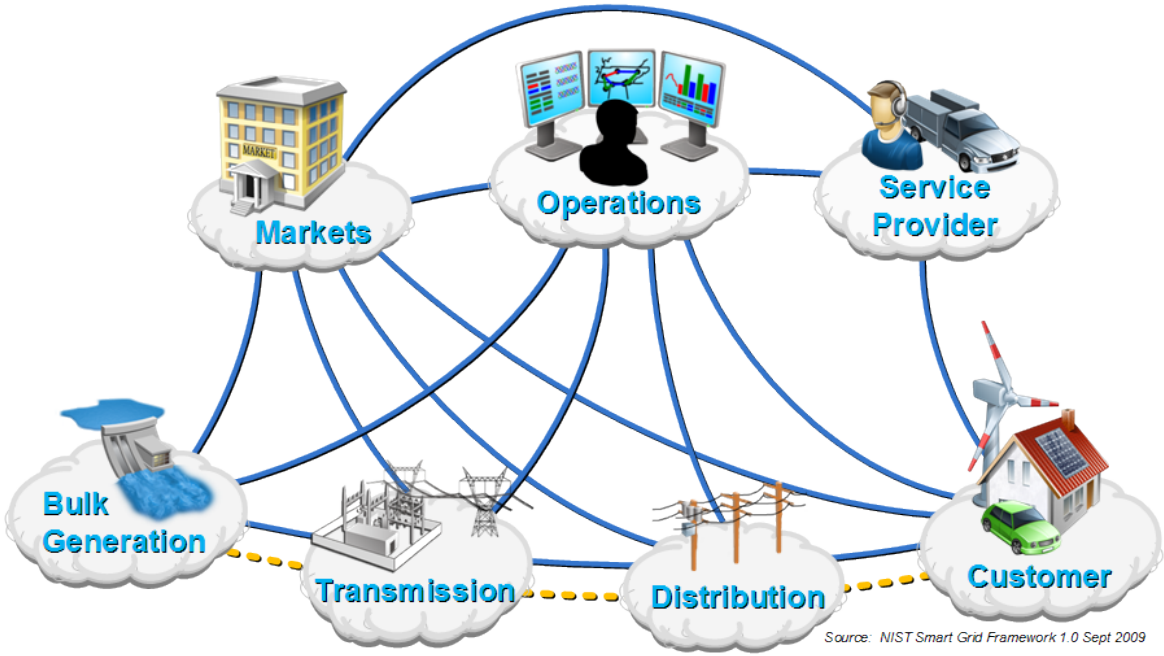
Threats

Are off-the-shelf product suitable for ICS security?

+

= ?

Smart Grid as a complex ecosystem

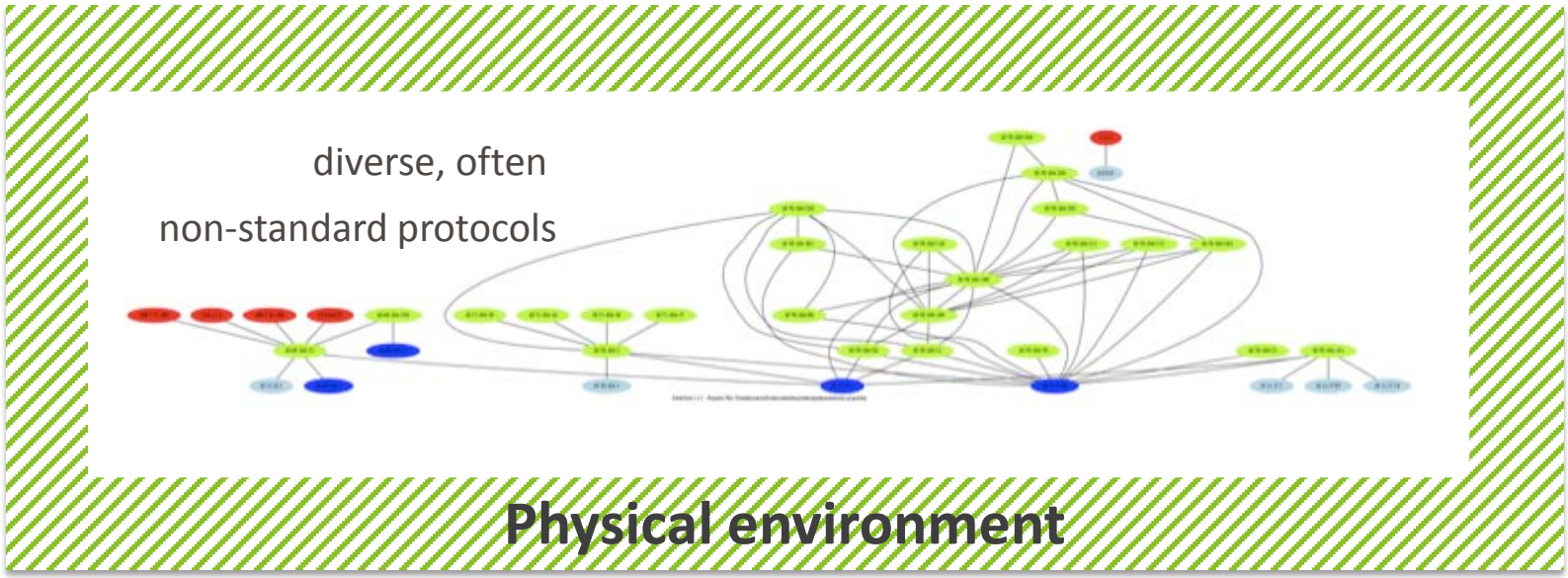


Our focus

SCADA → AMI

A composition of complex environments

flow datagram generated from the analysis of one hour of operation of a water pump control system



servers

gateways

clients in main network

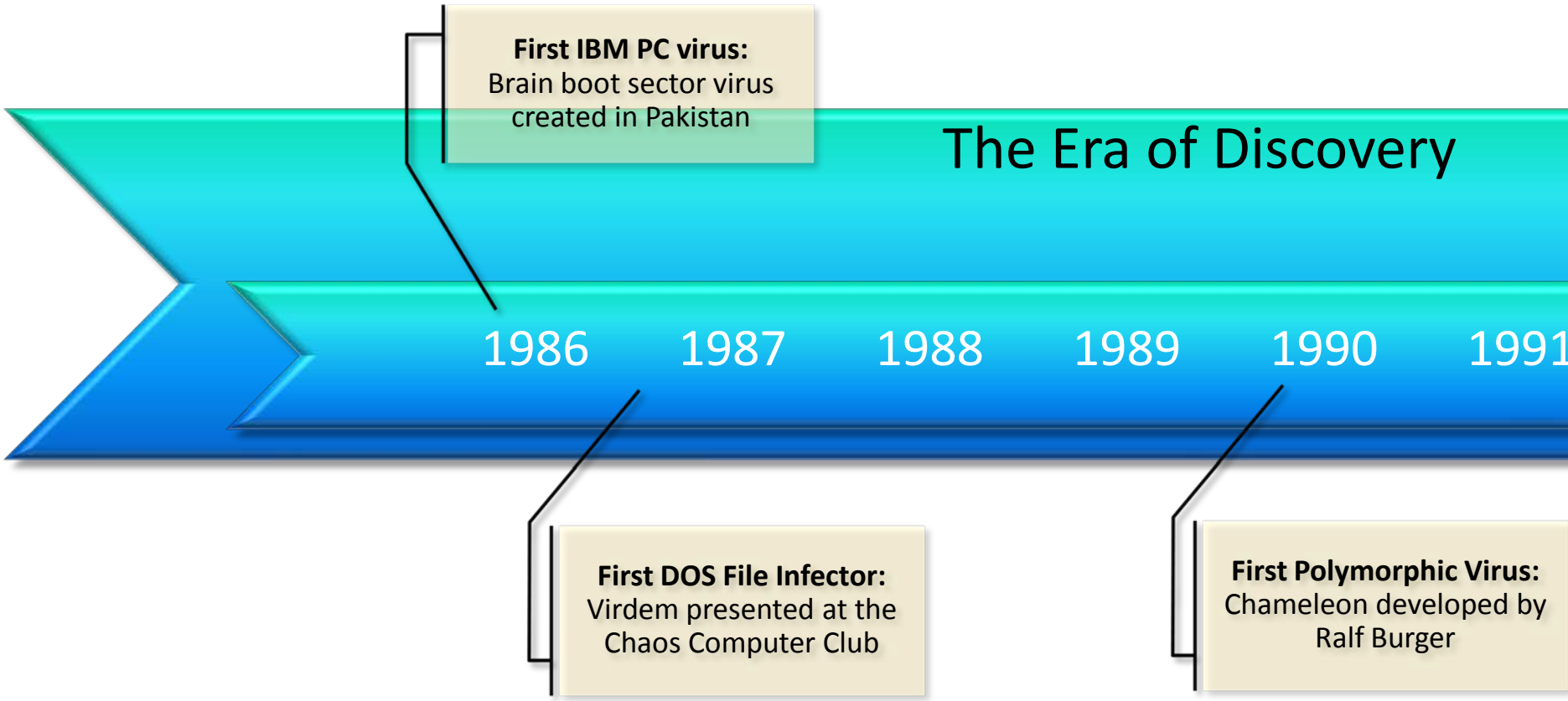
clients in separate network

Culture

Environments

ICS Security

Threats


First IBM PC virus:
Brain boot sector virus created in Pakistan
The Era of Discovery
1986
1987
1988
1989
1990
1991
First DOS File Infector:
Virdem presented at the Chaos Computer Club
First Polymorphic Virus:
Chameleon developed by Ralf Burger

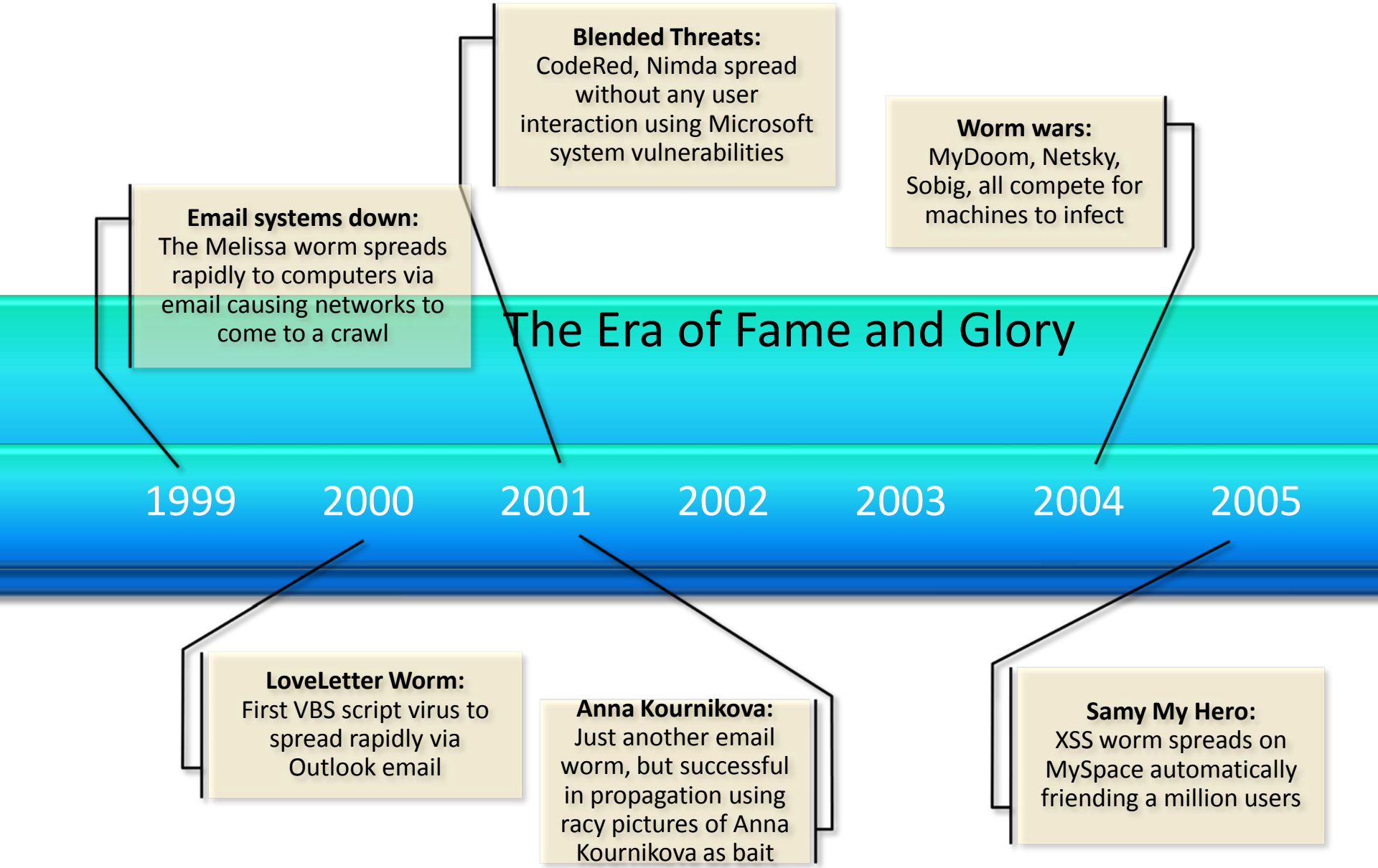
The Era of Transition

Michaelangelo trigger date:
Causes widespread media panic that computers would be unbootable

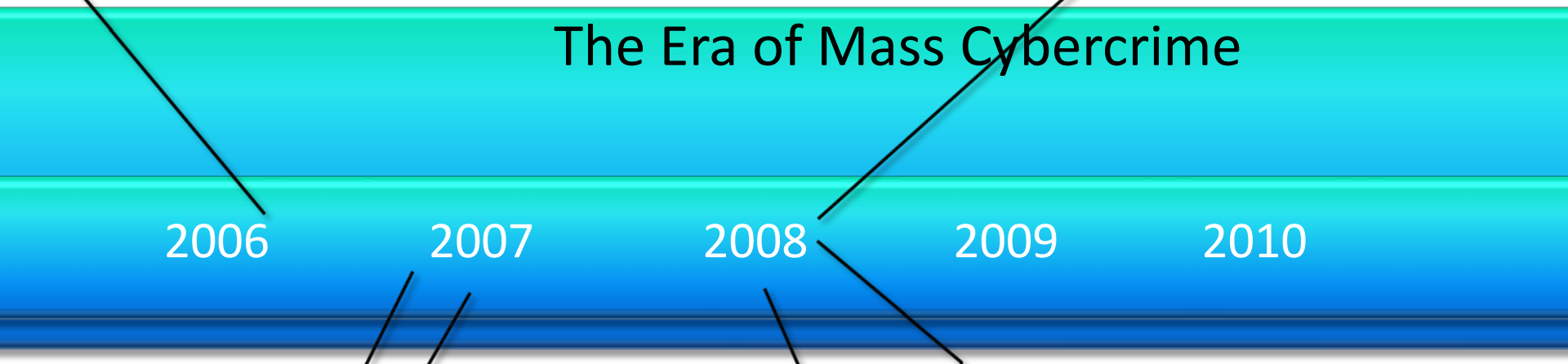
CIH:
A Windows file infector that would flash the BIOS

1992 1993 1994 1995 1996 1997 1998

First Word Macro virus:
Concept is the first macro virus infected Microsoft Word documents


Blended Threats:
CodeRed, Nimda spread without any user interaction using Microsoft system vulnerabilities
Worm wars:
MyDoom, Netsky, Sobig, all compete for machines to infect
Email systems down:
The Melissa worm spreads rapidly to computers via email causing networks to come to a crawl
The Era of Fame and Glory
1999
2000
2001
2002
2003
2004
2005
LoveLetter Worm:
First VBS script virus to spread rapidly via Outlook email
Anna Kournikova:
Just another email worm, but successful in propagation using racy pictures of Anna Kournikova as bait
Samy My Hero:
XSS worm spreads on MySpace automatically friending a million users

The Era of Mass Cybercrime



Rogue AV:
Becomes ubiquitous charging $50-$100 for fake proteciton

Mebroot:
MBR rootkit that steals user credentials and enables spamming

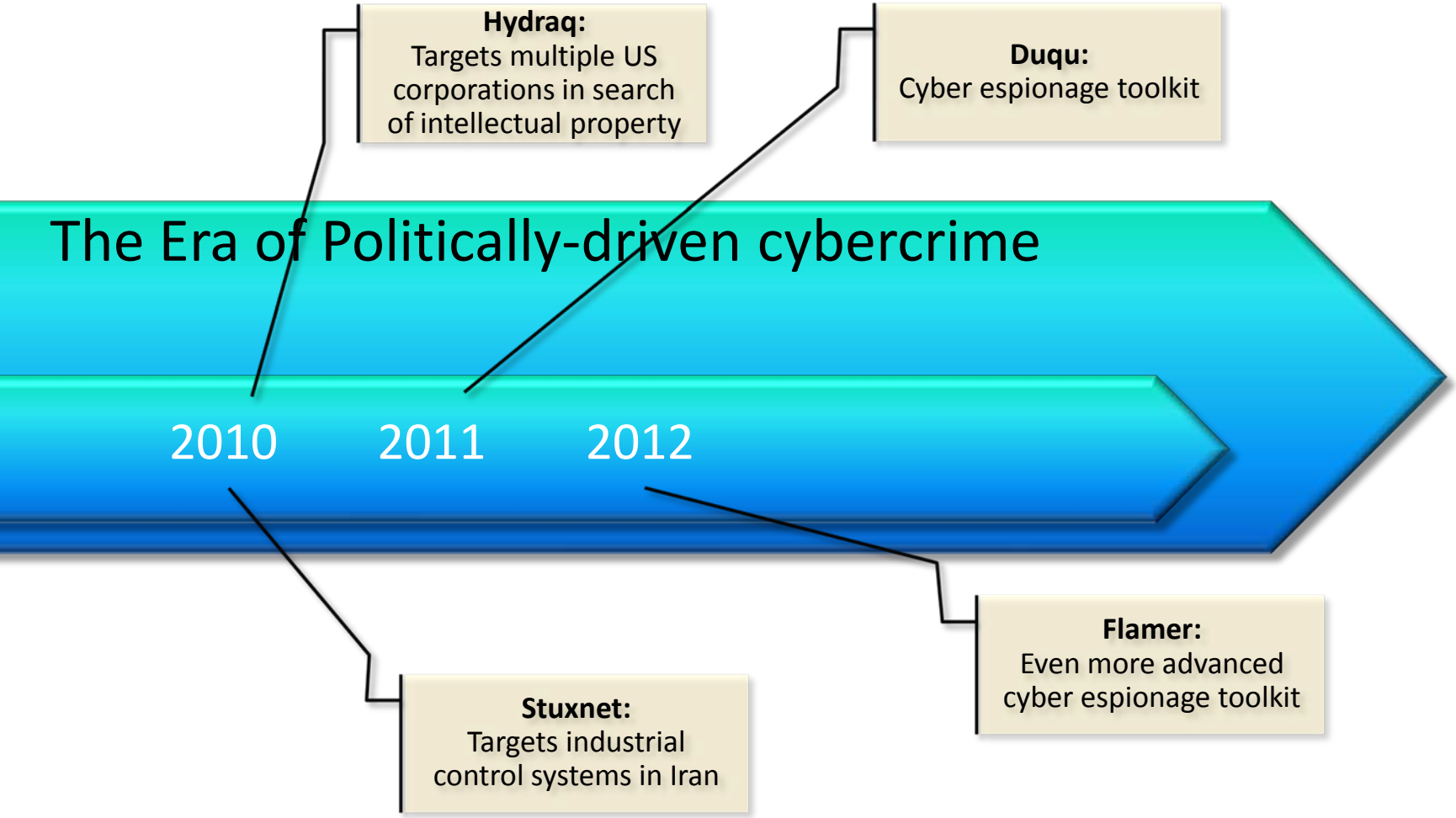
Zeus Bot:
Hackers botnet executable of choice -- steals online banking credentials

Storm Worm:
P2P Botnet for spamming and stealing user credentials

Koobface:
Spreads via social networks and installs pay-per-install software

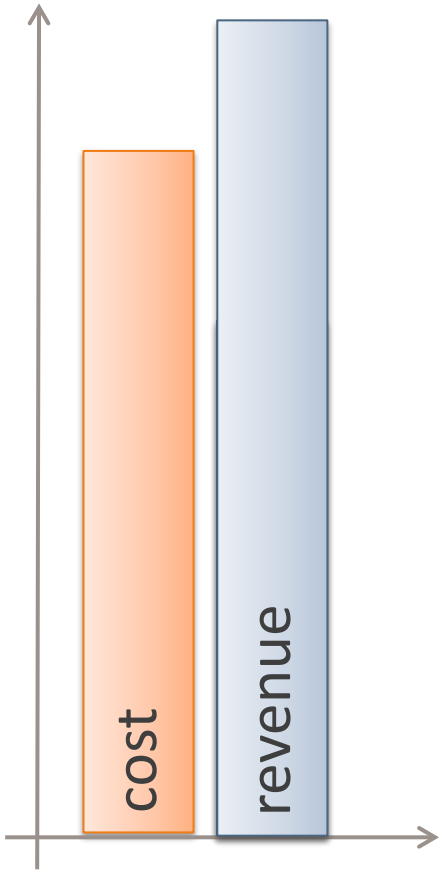
Conficker:
Spreads via MS08-067, builds millions-sized botnet to install pay-per-install software

Symantec


Hydraq:
Targets multiple US corporations in search of intellectual property
Duqu:
Cyber espionage toolkit
The Era of Politically-driven cybercrime
2010
2011
2012
Stuxnet:
Targets industrial control systems in Iran
Flamer:
Even more advanced cyber espionage toolkit

Threat economy

- Security mechanisms often aim at rendering an intrusion “difficult enough”
- Their effectiveness depends on the value of the target!
  - Requiring a signed certificate to inject a kernel driver
  - Keeping valuable resources in a private network
  - Storing a certificate in a secure room
  - …

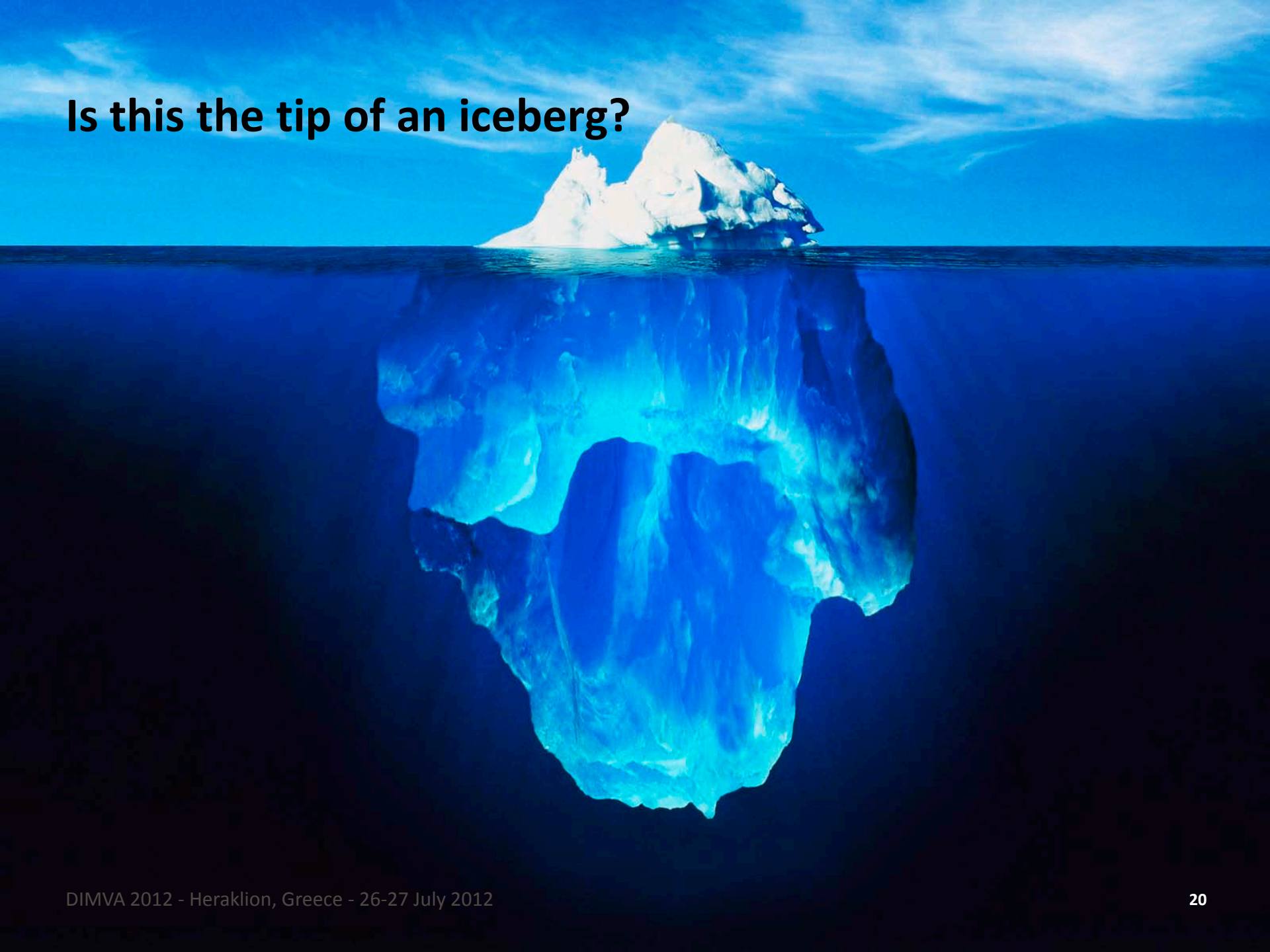


Cyber warfare

- **Stuxnet:** first publicly known malware to cause public damage
- **Duqu:** shares many similarities, used for cyber espionage
- **Flamer:** even more advanced platform for data exfiltration

➔ **Cyber warfare is not a myth!**

Is this the tip of an iceberg?



What is your experience with each of this type of attacks? (1580 industries contacted, 2010)

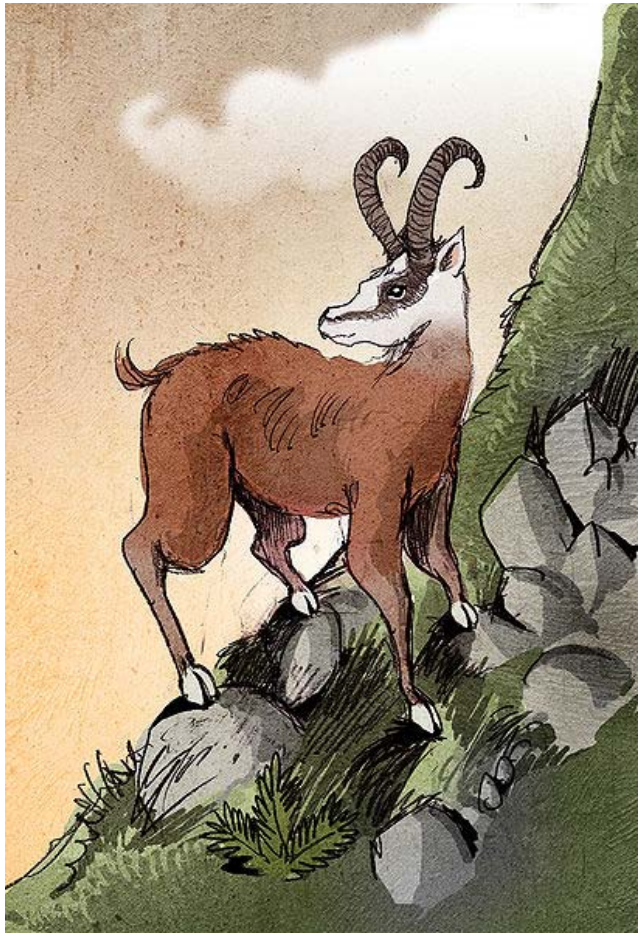
Symantec 2010 Critical Infrastructure Protection Study - **http://bit.ly/bka8UF**

How many times have you suspected or been sure each of the following has occurred in the last 5 years?

Symantec 2010 Critical Infrastructure Protection Study - **http://bit.ly/bka8UF**

The risk of dahusian research

- How can we protect from threats we do not know?



Culture

Environments

ICS Security

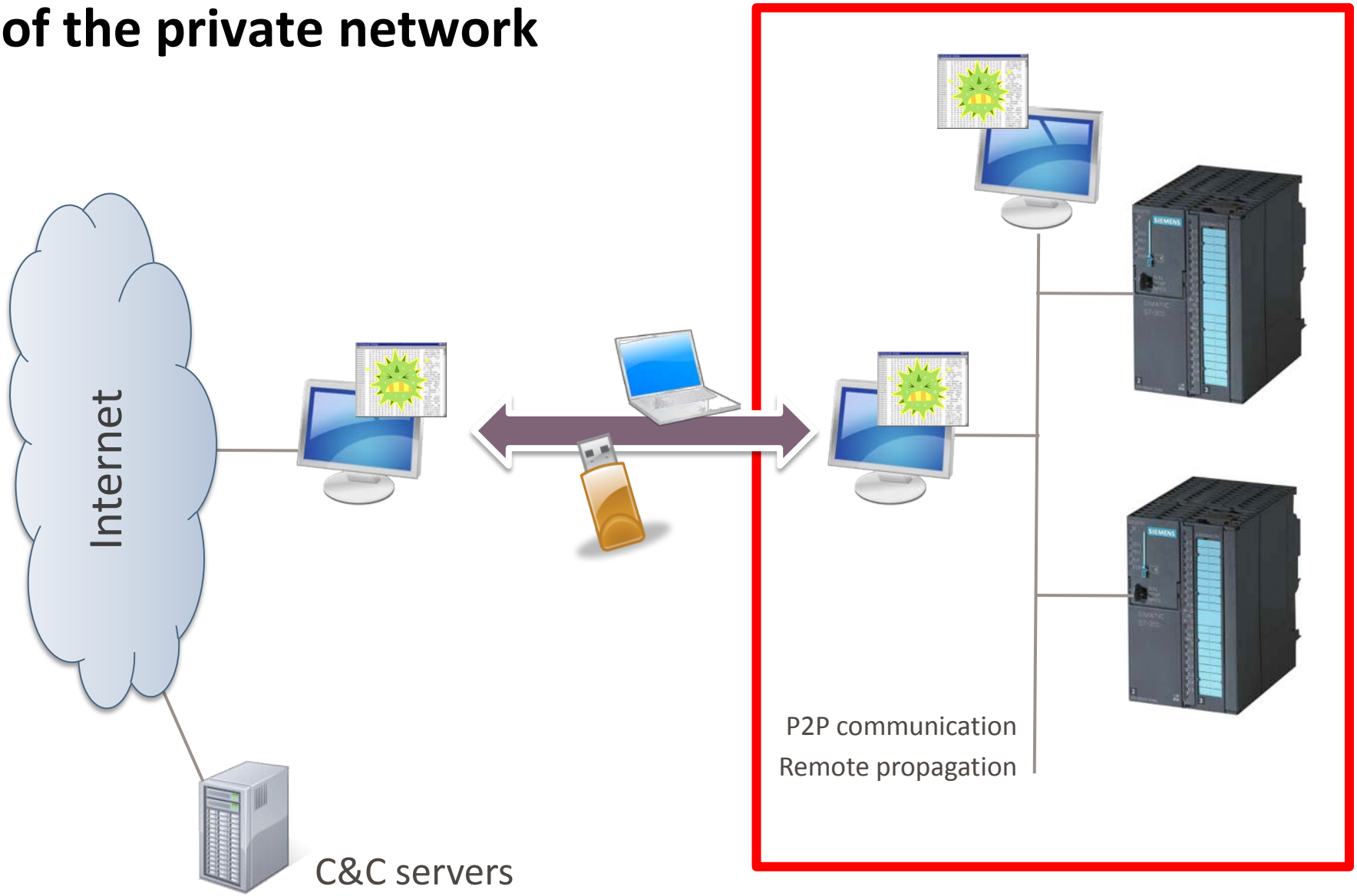
incidents

Threats

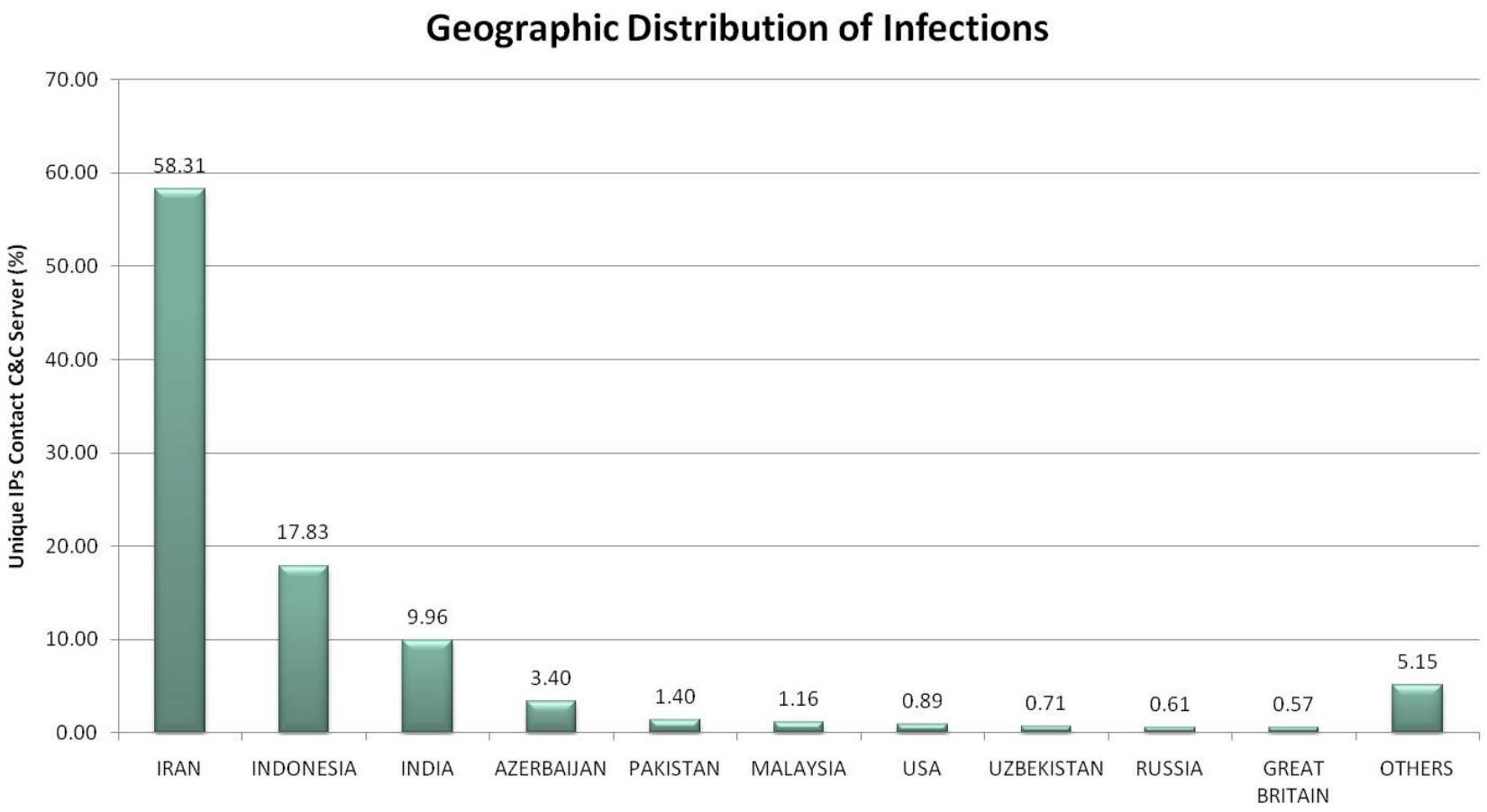
Stuxnet

- Windows worm discovered in **July 2010**
- Uses **7** different self-propagation methods
- Uses **4** Microsoft 0-day exploits + **1** known vulnerability
- Leverages 2 Siemens security issues
- Contains a Windows rootkit
- Used **2 stolen digital certificates** (second one introduced when first one was revoked)
- Modified code on Programmable Logic Controllers (PLCs)
- First known PLC rootkit

Stuxnet and the myth of the private network

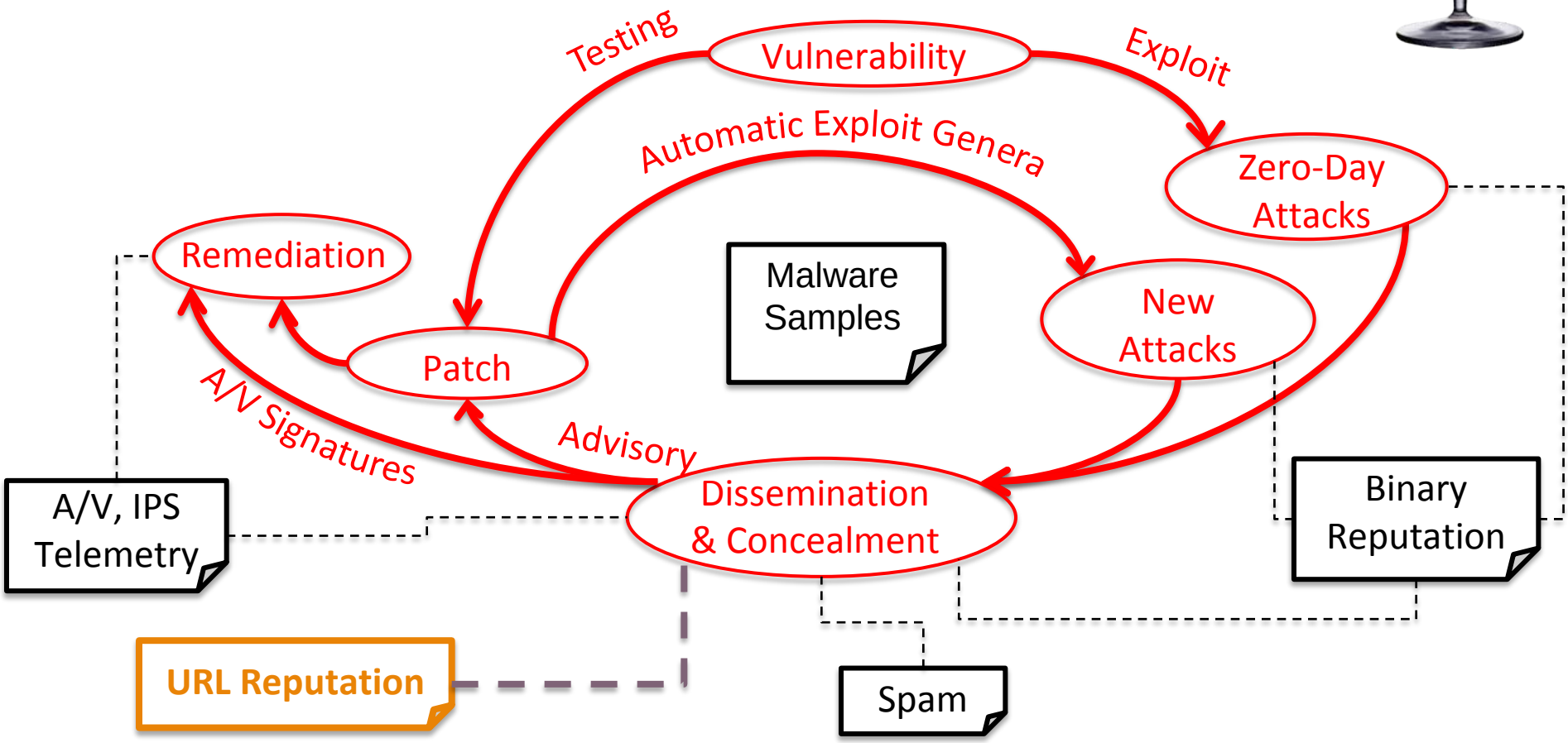


Dissemination of Stuxnet

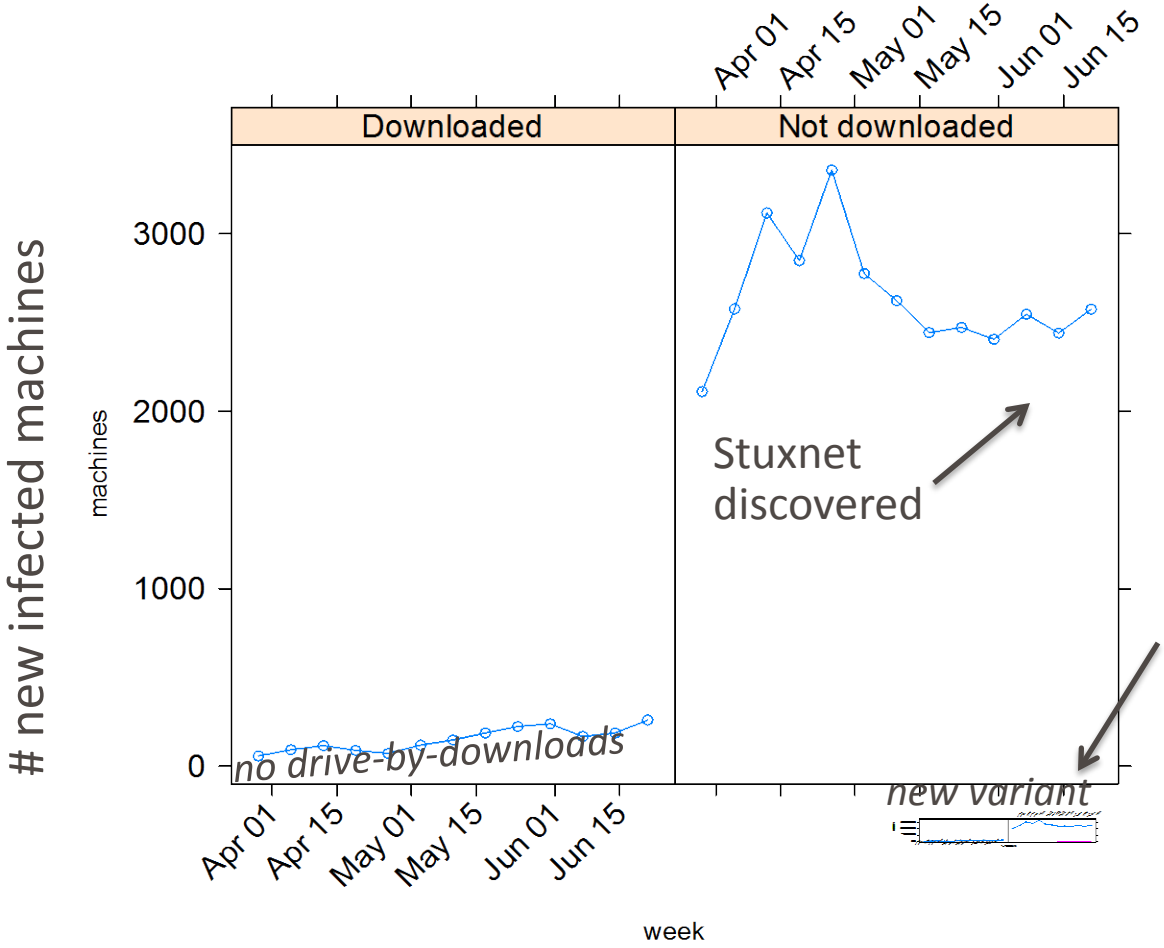


Let's add some WINE

(http://www.symantec.com/WINE)



Dissemination of Stuxnet



Exploits CVE 2010-2568 (well documented MD5 hashes)

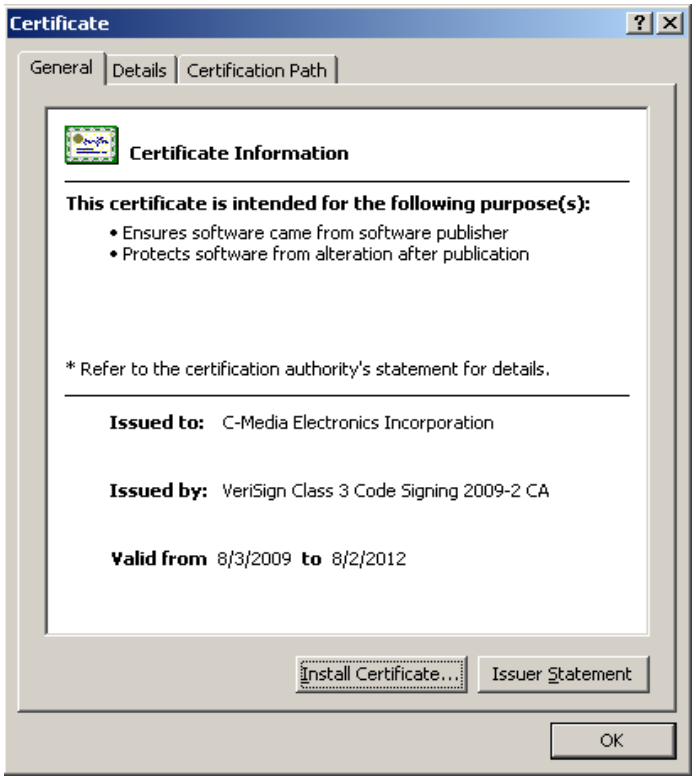
CVE 2010-2568 reported on Jul 16

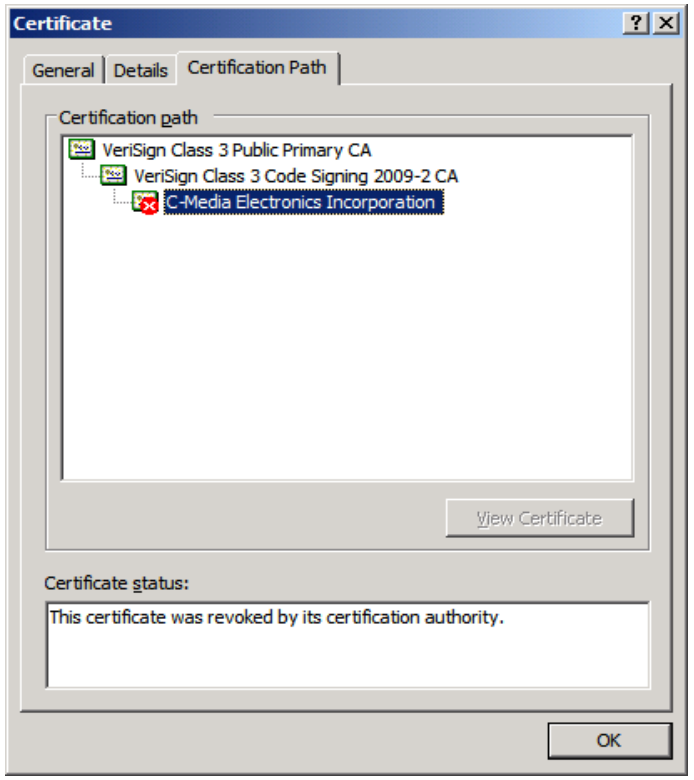
Weeks

Stuxnet: an isolated incident?

- **September 2011:** a European company seeks help to investigate a security incident that happened in their IT system, and contacts CrySyS labs (Budapest University of Technology and Economics)
- **October 2011:** CrySyS labs identifies the infection and shares information with major security companies
  - Duqu: named after the filenames created by the infection, starting with the string "~DQ"
  - A few days later, Symantec releases the first report on Duqu malware sample with the help of the outcomes of the original CrySyS investigators

Signed Drivers



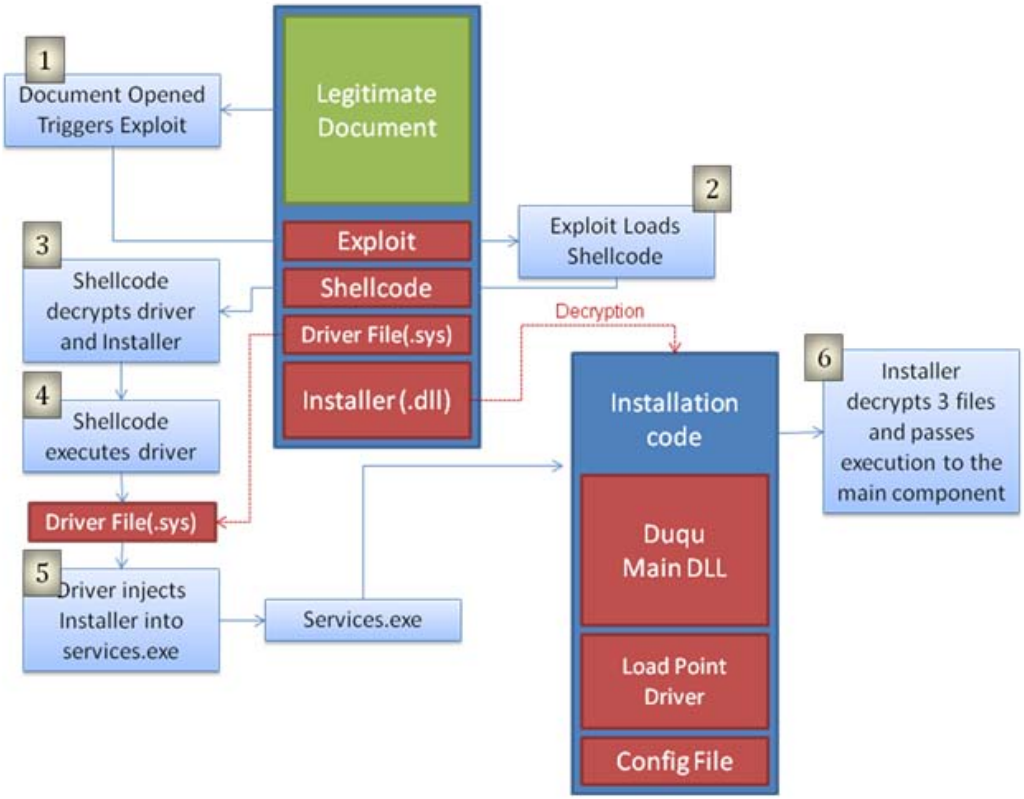


- **Some** signed (C-Media certificate)
- Revoked immediately after discovery

Extremely stealthy and targeted infection

Infection leaves almost no trace on hard drive: only the driver file is stored in stable storage!

- 0-day vulnerability in TTF font parser
- Shellcode ensures infection only in an 8 days window in August
- No self-propagation, but spreading can be directed to other computers through C&C
  - Secondary target do not communicate with C&C, communicate instead through P2P

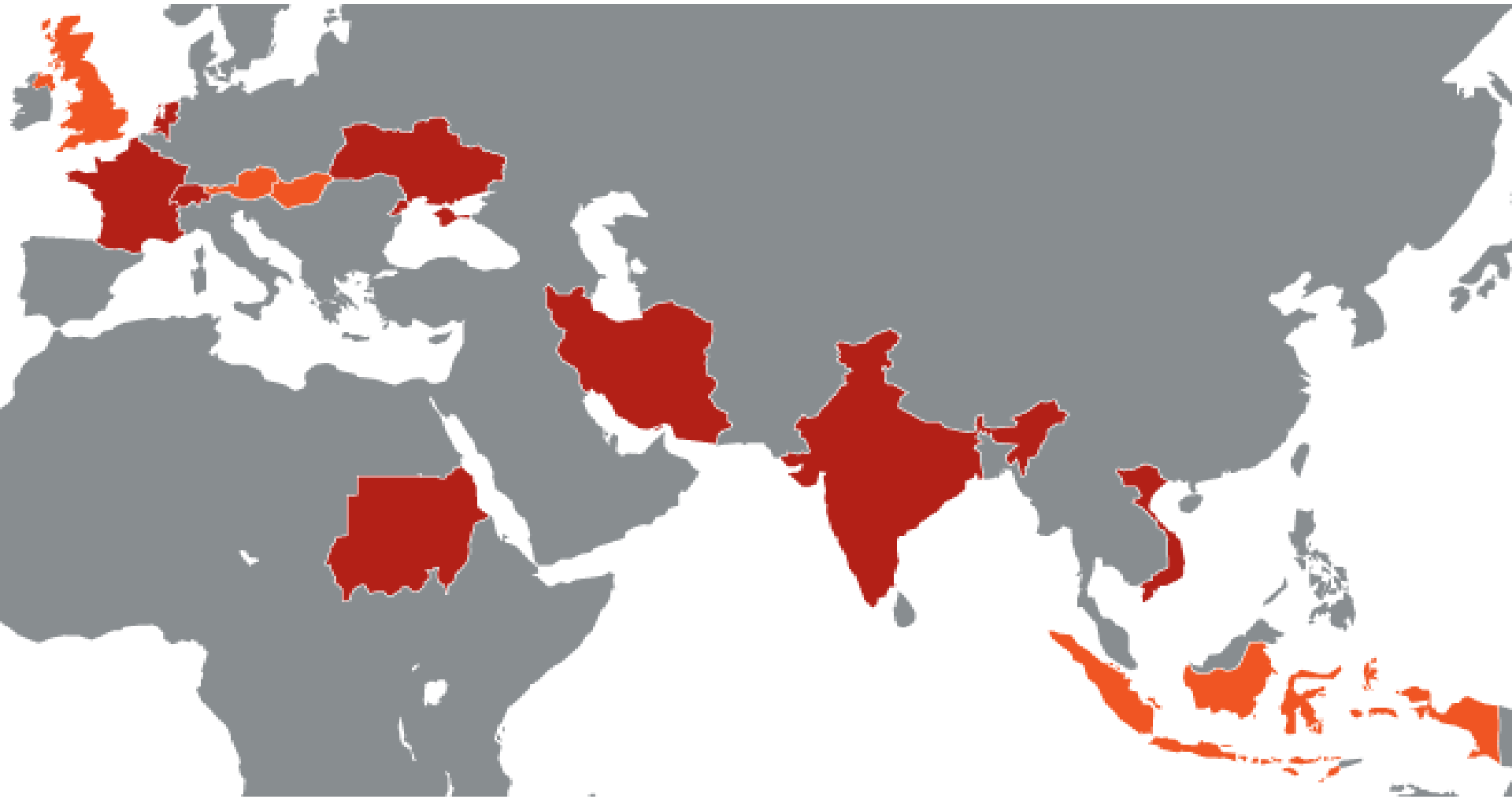


Command & Control Complexity

- Communication over TCP/80 and TCP/443
  - Embeds protocol under HTTP, but not HTTPS
  - Includes small blank JPEG in all communications
  - Basic proxy support
- Complex protocol
  - TCP-like with fragments, sequence and ack. numbers, etc.
  - Encryption AES-CBC with fixed Key
  - Compression LZO
  - Extra custom compression layer
- CnC server hidden behind a long sequence of proxies

Targets

6 organizations in 8 countries confirmed infected

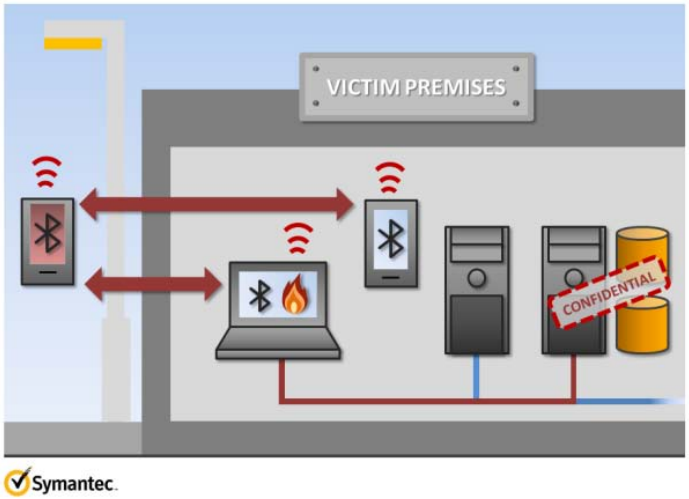


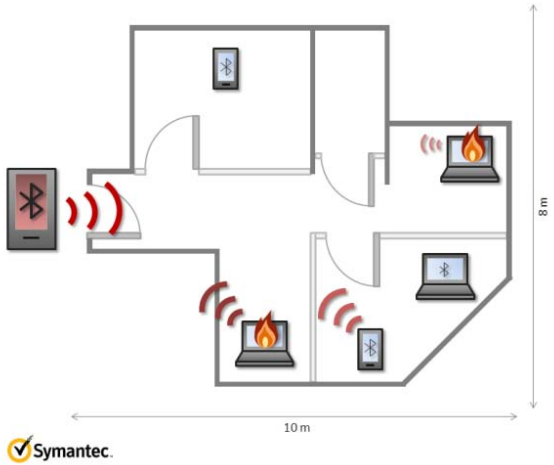
Duqu “strange clues”

- TTF Exploit
  - Font name “Dexter Regular” from “Showtime Inc.”
  - Only two characters defined:

W32.Flamer

- Recently discovered, but active for more than 2 years
  - Extremely high complexity
  - LUA Interpreter
- Comprehensive toolkit for data exfiltration
  - Ability to record from internal microphone
  - Bluetooth toolkit





What do we learn from all this?

1. **Attacker motivation:** no security practice is likely to make the intrusion **difficult enough**. New motivations for attackers (crime, cyber warfare) mean more resources and incentives to conduct attacks.
2. **Myth of the private network:** also because of 1. , relying on network isolation from the Internet as main security protection is ineffective. Physical security cannot be enforced in practice, and network isolation renders cloud-based security technologies impossible to apply (e.g. reputation, data analysis, signatures, …).
3. **From Intrusion Prevention to Intrusion Tolerance:** a layered approach is required with several safety nets and managerial procedures to handle fallback modes.

Thank you!

Corrado Leita

corrado_leita@symantec.com

➔ **CRISALIS: http://crisalis-project.eu**

➔ **WINE: http://www.symantec.com/WINE**

The CRISALIS approach