COMP6224: Foundation of Cyber Security

Gérard Tio Nogueras

October 18, 2016

Contents

1 I¡ntroduction

Teacher: : Vladimiro Sassone
"People are the weakest node in network and systems"

1.1 what is cyber security?

Very important to make risk management:
"How much spend to defend, depending on the risk and power of the possible attacker on given target"

Some definitions:
Cyber security: protection of the cyberspace against cyber threats and vulnerabilities.
Cyber space: complex of activities carried out through networks of computers.
Cyber threat: typical threats include unauthorised access, destruction, system overrun and takeover, propagation of malicious code, data thieving and fabrication, ...
Cyber vulnerability: the presence of weaknesses or loopholes in systems which may lead (systematically) to cyber attacks.
National security: attacks to critical infrastructures such as Transport, Energy and Communications can have devastating effects, and are now regular part of warfare and terrorist scenarios.
Gvt and public bodies: the robustness to intrusion and tamper of electronic services, which typically hold very sensitive information.
The economic processes: the protection of industrial secrets and practices, the confidentiality of business information and tenders; the viability of the network economy, just think of the banking system.
The citizen: the privacy and legitimate use of personal data against deanonymisation and impersonation attacks from all sources; the challenged from cybercrime.

1.2 Challenges ?

To create a strong learning and teaching programme to limit threats and vuln.

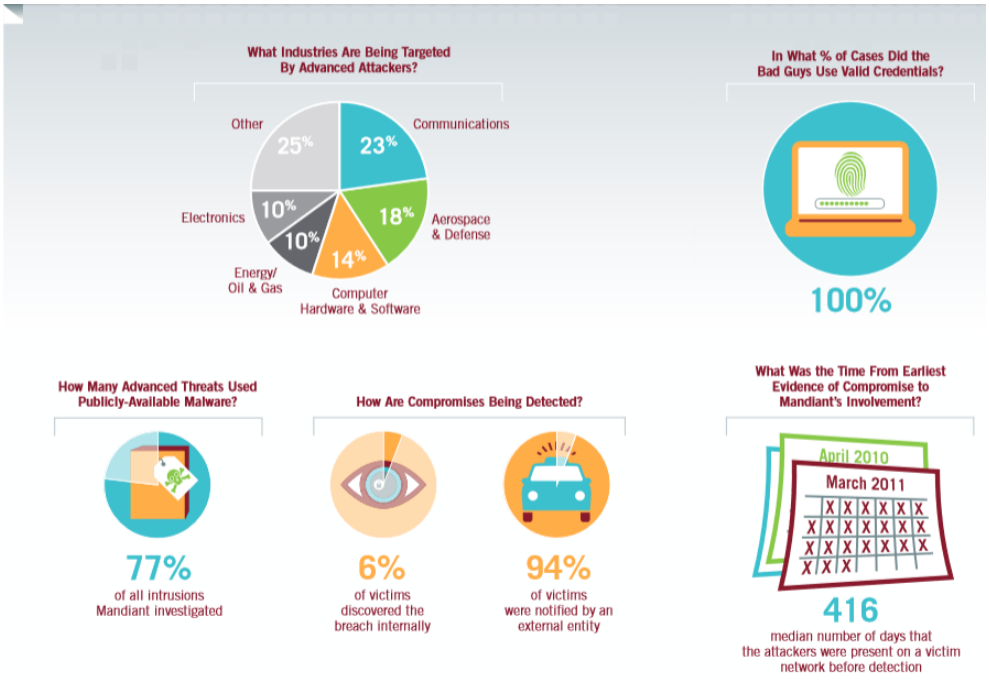
1.3 Unfair ?

Because even if the computers are maintained by the smartest people, they can't prevent the user's mistakes.

1.4 What is needed ?

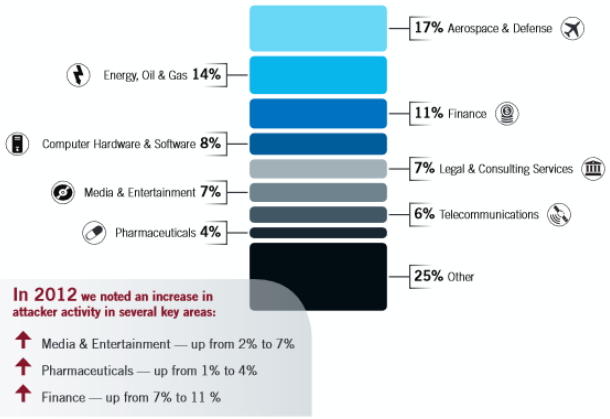
Education

1.5 Numbers


What Industries Are Being Targeted By Advanced Attackers?
Other
25%
Communications
23%
Electronics
10%
18%
Aerospace & Defense
10%
14%
Energy/ Oil & Gas
Computer Hardware & Software
In What % of Cases Did the Bad Guys Use Valid Credentials?
100%
How Many Advanced Threats Used Publicly-Available Malware?
77%
of all intrusions Mandiant investigated
How Are Compromises Being Detected?
6%
of victims discovered the breach internally
94%
of victims were notified by an external entity
What Was the Time From Earliest Evidence of Compromise to Mandiant's Involvement?
April 2010
March 2011
416
median number of days that the attackers were present on a victim network before detection

VICTIMS BY THE NUMBERS

Industries Being Targeted by Advanced Attackers



In 2012 we noted an increase in attacker activity in several key areas:

- Media & Entertainment — up from 2% to 7%
- Pharmaceuticals — up from 1% to 4%
- Finance — up from 7% to 11 %

How Compromises Are Being Detected

1.6 Malware is only half of the story

Malware explain half of what happend, but you still have to analyse and research the registry entries, event logs, scheduled tasks logs, inventory mgnt logs, network traffic capture and finaly file system artifacts.

1.7 Old is the new door

Backdoors were used as backdoors to be resilient against detection and remote access.
Lately these backdoors became passive backdoors meaning that they don't generate any network traffic and are harder to detect. They don't generate traffic work. Here are 2 example of passive backdoors:
Port Listeners: