Advanced Persistent Threats: The Empire Strikes Back!

Nikos Virvilis
Senior Information Assurance Scientist, NCI Agency

Prof. Dimitris Gritzalis
Director of the Information Security & Critical Infrastructure Protection (InfoSec) Laboratory

March 2015
Advanced Persistent Threats: The Empire Strikes Back!

Nikos Virvilis
Senior Information Assurance Scientist
Disclaimer

The views expressed in this presentation are those of the presenter and do not reflect the official policy or position of NATO Communications and information Agency, nor does it represent an endorsement of any kind.
Agenda

• Major APT incidents
  – Did we learn anything from them?

• Why we keep failing:
  – Security vendors
  – Consultants
  – Academia

• Countermeasures?
“Skilled, resourceful hackers, state employed or working for the higher bidder, whose full time job is to compromise CIS, in order to exfiltrate information or sabotage them.”
State of the (Malware) Art

<table>
<thead>
<tr>
<th>Malware Name</th>
<th>Public Disclosure Date</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stuxnet</td>
<td>2010</td>
<td>Sabotage</td>
</tr>
<tr>
<td>Duqu</td>
<td>2011</td>
<td>Information Gathering</td>
</tr>
<tr>
<td>Flame</td>
<td>2012</td>
<td>Information Gathering</td>
</tr>
<tr>
<td>Red October</td>
<td>2012</td>
<td>Information Gathering</td>
</tr>
<tr>
<td>MiniDuke</td>
<td>2012</td>
<td>Information Gathering</td>
</tr>
<tr>
<td>Regin</td>
<td>2014</td>
<td>Information Gathering</td>
</tr>
<tr>
<td>Equation Group Malware</td>
<td>2015</td>
<td>Information Gathering</td>
</tr>
</tbody>
</table>

1 Older samples have been discovered. In some cases they had been active for several years

• Each one has been called “the world’s most advanced malware” (until the next one was detected).
Did we learn anything?

- Before Stuxnet, cyber attacks were not taken seriously:
  - Mostly script-kiddies defacing web sites
  - “Computers are for playing games”

- Stuxnet proved that cyber attacks can impact physical world

- The APT malware, made it clear that current security solutions are **basically useless** against sophisticated attackers
National Efforts

• **China:** China’s long term plan is to achieve electronic dominance by 2050 (Andreasson 2011)

• **UK:** A clear cyber-strategy has been defined, with its main goals to make the UK one of the world’s most secure places to do business (Gov.uk 2014b)

• **USA:** Since 2009 has created the U.S. Cyber Command, an armed-forces command, focused on cyberspace operations. U.S. short term plans include to grow the Cyber Command to 6000 people by 2016 (and in 2015 the cyber budget is expected to exceed 5 billion USD)

• **Most developed nations:** Large Cyber security teams (hundreds or thousands)
Greek Efforts

This page has been intentionally left blank
Part II - Challenges
Challenge 1: Cyber Security is hard to measure

• Hire someone to build a new web site
  – Is the web site up?
  – Does it have all the information you have asked for?
  – Is it designed the way you like?
  – Test it/Benchmark it

• Hire someone to do a web app pentest on your web site
  • Did he/she find all the vulnerabilities?
  • Has he/she any idea what he/she is doing?
Edge cases

• A high quality report will stand out
  – Still no guarantee that the Pentester has found all vulnerabilities

• A terrible report will also stand out
Edge cases

**Critical finding:** We managed to get the public key of the web server!
I HAVE NO IDEA WHAT I'M DOING
So what do you do?

• If you feel like the report / outcome, is not up to your expectations, speak up!
  – Be careful though, you may lose you job...

• Next time hire two companies, to do the same assessment
  – Yes I know, you don’t have the budget but...
  – There will always be deltas! However big deltas should raise warnings
  – Don’t forget skilled individuals / universities
Challenge 2: Hello Industry (a.k.a. Security Vendor Snake oil)

- Unbreakable (a.k.a. Bulletproof) software: vendors and developers alike, have claimed their software does not have any vulnerabilities

- Our system is protected by 1,000,000 bit crypto...

• **We detect APT** (Sure... after the malware samples have been submitted to Virus Total)

• Our AV/IDS/IPS/* detects 100% of all threats
  – Fred Cohen has **proven mathematically** that there are infinite ways of writing a (malicious) software program and **thus, foolproof detection is impossible** (Cohen 1987)
  – You can only make such claims if you are using whitelists!
TRUST ME, I'M A SECURITY VENDOR
NOOOOOOO !
But there are also exceptions

• “Antivirus is dead... as it detects a mere 45 percent of all attacks”
  - Brian Dye, Symantec's senior vice president for information security (Symantec 2014)

• Is this news to any of the techies?
• What about the management?
So do we need Industry?

• Of course we do!
  – There are excellent solutions
  – And yes, they are expensive
  – But we need to be honest about what these solutions can or can’t do!

• The risk owners need to know the truth about the risks that the organization is facing, in order to make the correct decisions
Challenge 3: Academia

• Too focused on theory
  – AUEB has introduced penetration testing & VA, wireless security and web application security modules, for several years
  – Only a few other universities have followed

• Quote from a lecturer:
  “By using endpoint protection on all systems, IDS/IPS, Firewalls and a Secure Email Gateway the network is attack proof”...
Challenge 4: In the hunt for cyber warriors

• One of U.S.’s major challenges is the shortage of cyber security professionals within the United States (LIBICKI et al. 2014)

• That’s weird!
  – MSc in Information Security are so popular nowadays
  – Even Bachelor degrees!

• Have you visited LinkedIn recently?
  – Security Evangelists
  – Cyber Gurus
  – Ethical Hackers
Not the average Security Guy

- They are not looking for just another *<put certificate name here>*

- Neither someone with an MSc in InfoSec and a couple of security books under his belt

- Not another cyber philosopher
Skilled technical people are hard to find!

- Can you find attacks in a multi gig network capture file?
- Can you analyze advanced malware (!= sandbox | uploading it to VirusTotal)
- Can you write your own tools?
- 5 out of 200?
Challenge 5: C-level executives / management

• "There are two kinds of big companies in the United States. There are those who’ve been hacked and those who don’t know they’ve been hacked." - James Comey, FBI director

• “Prevention eventually fails. Some readers questioned that conclusion. They thought that it was possible to prevent all intrusion if the right combination of defenses, software security or network architecture was applied ... Those who still believe this philosophy are likely suffering the long-term (APT) compromise that we read about in the media every week” – R. Bejtlich, CSO @Mandiant
Part III - Countermeasures

KEEP CALM AND DEFEND YOURSELF
There are no silver bullets

• But there are some clever tricks that can buy you time...
  – So you can detect ongoing attacks
  – Block them before the attackers reach their end goal

• Or call someone who knows how
Before you start, make sure that:

- You have already implemented security best practices
- You have highly skilled, motivated people
- And you have C-Level Support
  - (Adequate) Budget
  - Willing to change the way the organization works
All war is based on deception.

(Sun Tzu)
Deception

• When an attacker gains foothold to a network:
  – She needs to find where the information that she is interested is located, break into the system and exfiltrate it
  – In a medium to large organization there are several hundred systems
  – So... change the rules
Honeypots

- Honeypots have been proposed for attack detection for decades
- For targeted threat detection, there is limited value in having internet facing honeypots (noisy)
  - But they are great for attack detection on internal networks
  - Any (old) pc will do!
  - Ready to use: http://bruteforce.gr/honeydrive
Honey files, Honey records

• Honey files: “passwords.docx” on your file server
  – Enable file system auditing first

• Honey records on DB:
  – Add a table (or just new records) with fake but realistic data
  – Enable DB auditing
  – *If you see something like that you have a problem:*
    » `SELECT * FROM FakeUserData;`

Honey Users / Hashes

• Honey users: Create a few user accounts as baits
  – Make sure they look interesting and real (Can be domain, web app or standalone system accounts).
  – Potentially combine this with honey files (i.e. a file with fake username:password)

• Honey Hashes are also cool!¹
  – Perfect for detecting pass-the-hash attacks!

• Monitor for authentication attempts from these accounts², if you see any, you have a major problem!

• For more info, see (Virvilis, 2014a)

¹ [https://isc.sans.edu/diary/Detecting+Mimikatz+Use+On+Your+Network/19311](https://isc.sans.edu/diary/Detecting+Mimikatz+Use+On+Your+Network/19311)
Network statistics (i.e. Netflow)

- Create baselines of your network / systems and look for anomalies!
- Protocol Distribution!
  
  \[
  \text{Average\_DNS\_requests} = X \\
  \text{If Average\_DNS\_requests} > 10 \times X: \\
  \text{print "DNS Tunnel??"}
  \]

  – Monitor for long lived TCP connections
  – Monitor where (countries) your systems are connecting to
  – Monitor for connection between workstations
  – Check http://sourceforge.net/p/sansfor572logstash/wiki/Home/
Basic system auditing

• Why has user X logged in 10 different systems today?

• Why was user X logged in at 23:00 last night?

• Why there are 3 failed authentication attempts for all the users in your AD?

• Why a user has accessed 50 files on the file server today?

• Why a user has accessed X records on the DB today?
Whitelisting Executables

• The vast majority of APT attacks use (mostly) custom malware (i.e. executables) (Virvilis 2013a, Virvilis 2013b)

• Not foolproof (i.e. Shellcode will still execute)
  – Same with PowerShell etc.
  – Still you have significantly raised the bar!

• Excellent commercial solutions
  – Can’t afford them? No problem use the build-in ones!
Conclusion

• No easy solutions
  – We need skilled technical people
  – We need to be honest regarding our skills
  – C-level executives need to know the truth, they are the risk owners!

• Only if we accept our weaknesses we will be able to build stronger defenses
References

20. [http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf)