

Removing T from APT: responding efficiently to modern threats

Alexandre Karlov

whoami

- Graduated from Swiss Federal Institute of Technology, Lausanne (EPFL)
 - MSc in Communication Systems Specializing in Information Security
 - PhD in Cryptology (PayTV Broadcast Schemes, Technical Means to Fight piracy)
- 9+ years at Kudelski Group, Switzerland
 - Cryptography expert in PayTV division
 - Program Manager for the cybersecurity division
- Currently
 - Professor at University of Applied Sciences Western Switzerland
 - Teaching various security courses at bachelor and master level (ethical hacking, security audit, web security)
 - Applied research and development - SmartGrid, SCADA and eHealth (in)security
 - Coaching University Capture-The-Flag team
 - Independent security consultant
- CISSP, OSCP, ISO27001 Lead Auditor



@bassbeat



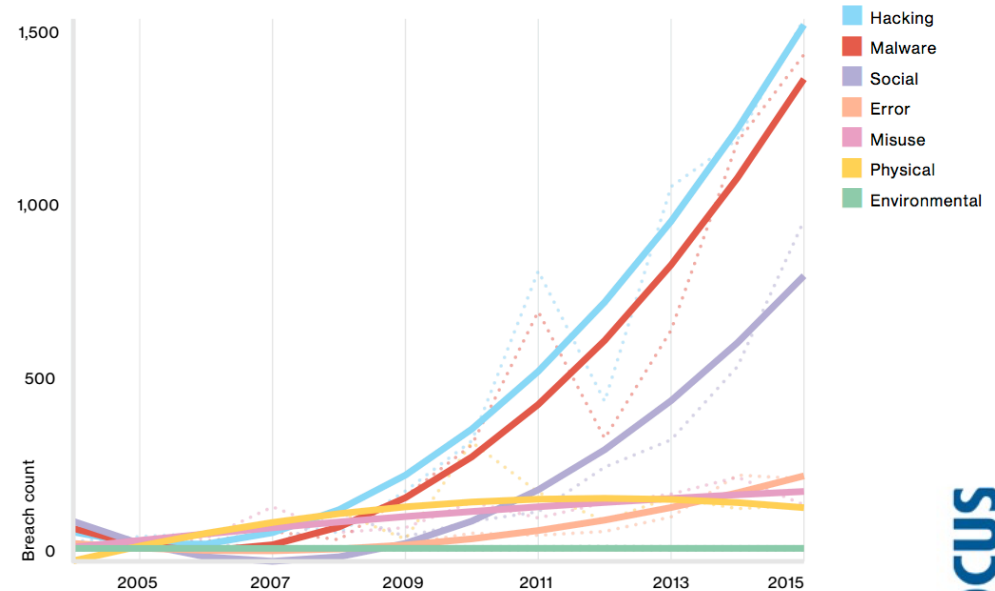
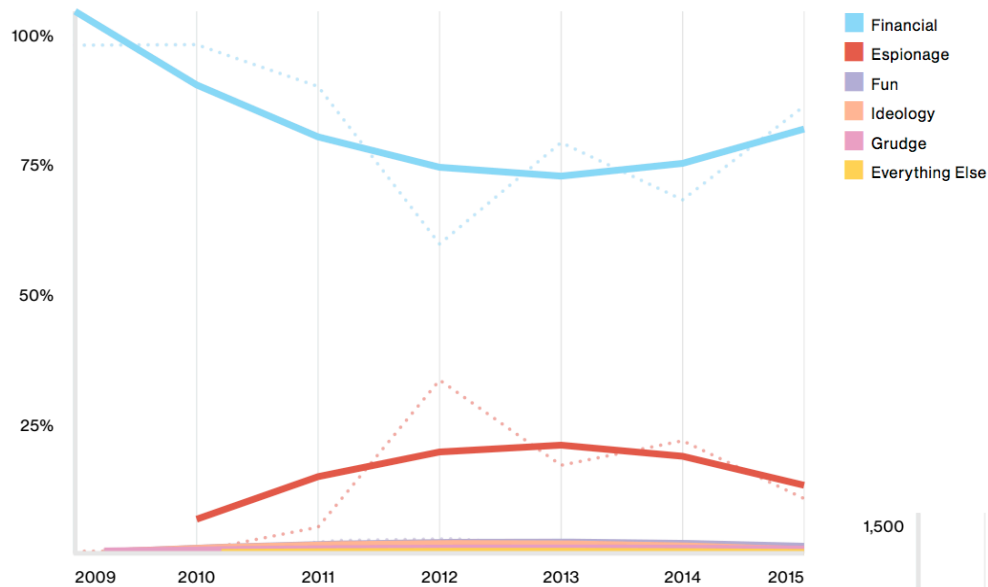
<https://ch.linkedin.com/in/alexandrekarlov>

APT - definition

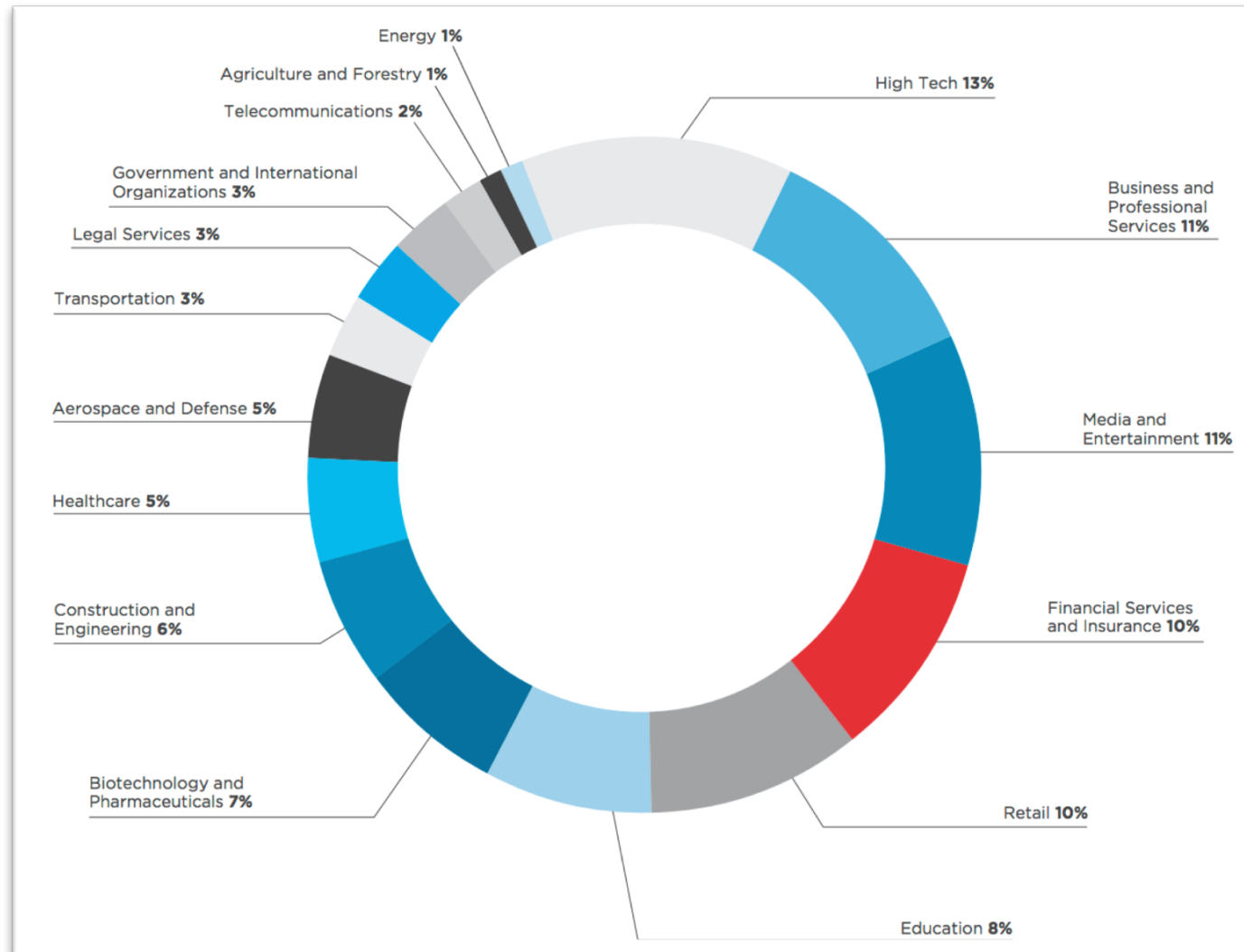
- Term first appeared at USAF
 - Advanced: the adversary knows what he is doing, is organized, motivated and/or funded
 - Persistent: the adversary has a clear goal in mind
 - Threat: the adversary intends to get what he wants
- Since several years became a marketing hyped term
- The goal is
 - Take an objective view on the phenomenon
 - Independently analyse what can be done to mitigate it



APT – in numbers



APT – in numbers

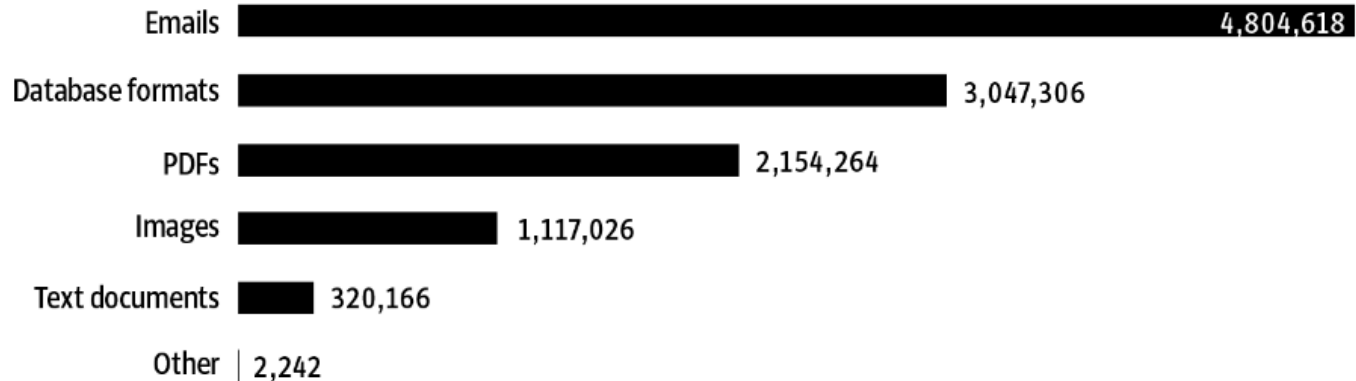


APT – in words

- Mossack Fonseca controversial hack
- 2.6 TB of data, 11.5 Mio documents syphoned
- Bigger than Wikileaks, Offshore leaks, Lux leaks and Swiss leaks combined

The structure of the leak

The 11,5 millionen contain the following file types



APT – visually

World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 6th May 2016)

interesting story

YEAR

BUBBLE COLOUR

YEAR

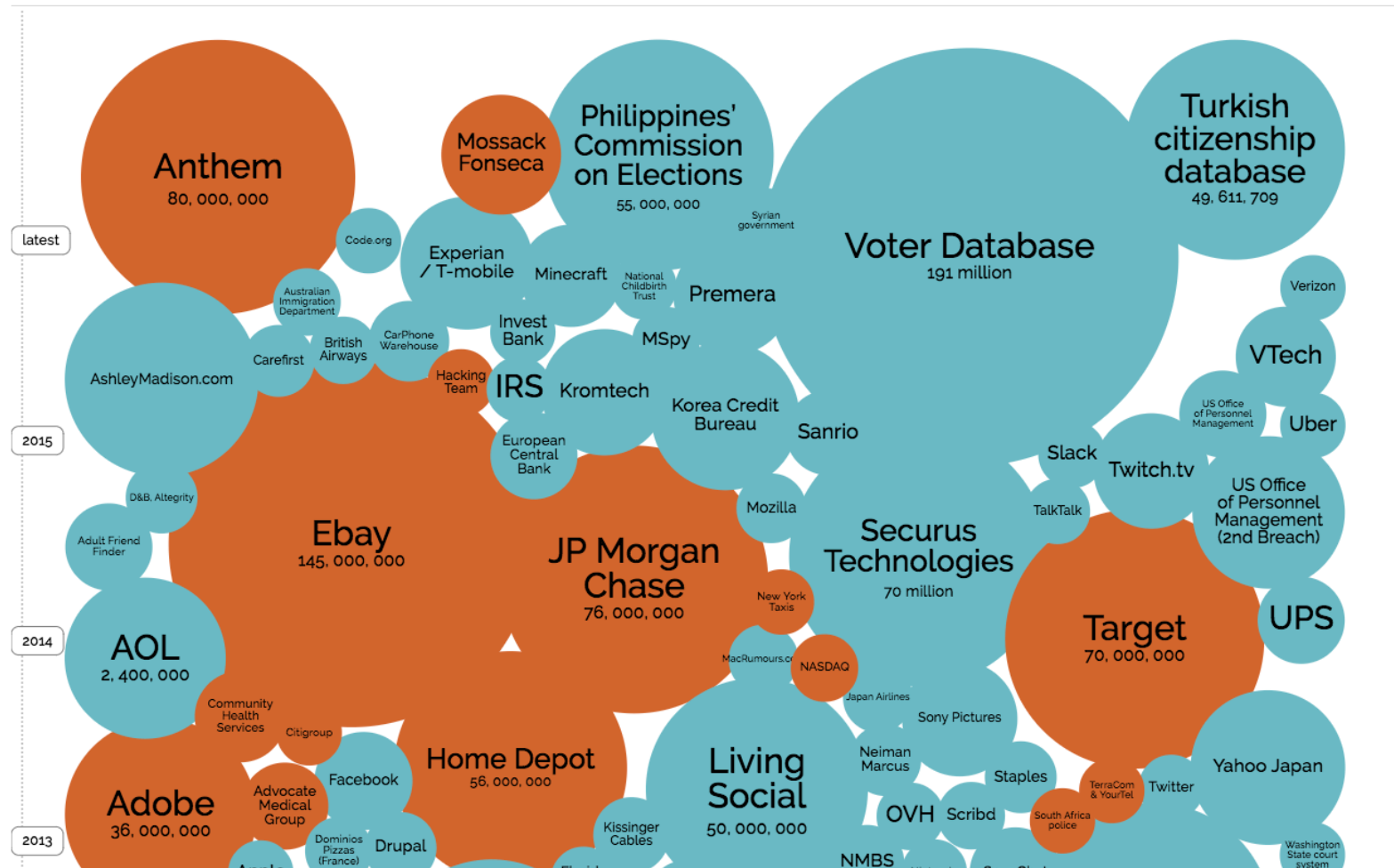
METHOD OF LEAK

BUBBLE SIZE

NO OF RECORDS STOLEN

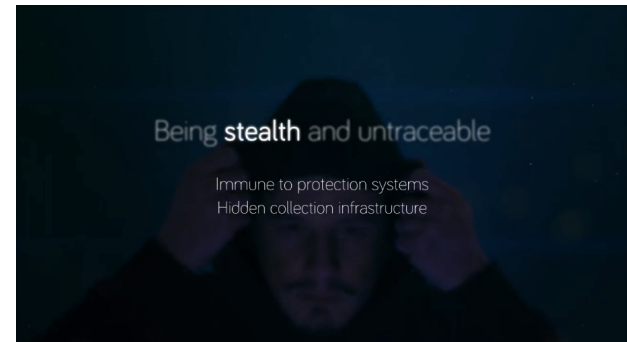
DATA SENSITIVITY

SHOW FILTER



The Hacking Team case

- Italian company founded in 2003, ~50 employees
- Selling Govware (spyware) – Remote Control System (RCS)
- Hacked on July 5th 2015
 - Emails, RCS source code, 0days, and other files exposed over Internet
 - over 400 GB
 - Hacking Team twitter taken over and used to distribute the leaked files
- Phineas Fisher, a hacker known for breaking into Gamma International UK Ltd., another Govware company took credit for the attack



The Hacking Team case

- Phineas Fisher made a writeup of how he hacked Hacking Team

----[3.2 - Attribution]-----

In the news we often see attacks traced back to government-backed hacking groups ("APTs"), because they repeatedly use the same tools, leave the same footprints, and even use the same infrastructure (domains, emails, etc). They're negligent because they can hack without legal consequences.

I didn't want to make the police's work any easier by relating my hack of Hacking Team with other hacks I've done or with names I use in my day-to-day work as a blackhat hacker. So, I used new servers and domain names, registered with new emails, and payed for with new bitcoin addresses. Also, I only used tools that are publicly available, or things that I wrote specifically for this attack, and I changed my way of doing some things to not leave my usual forensic footprint.

Advanced ?

----[5.3 - Technical Exploitation]-----

After the Gamma Group hack, I described a process for searching for vulnerabilities [1]. Hacking Team had one public IP range:

inetnum: 93.62.139.32 - 93.62.139.47
descr: HT public subnet

Hacking Team had very little exposed to the internet. For example, unlike Gamma Group, their customer support site needed a client certificate to connect. What they had was their main website (a Joomla blog in which Joomscan [2] didn't find anything serious), a mail server, a couple routers, two VPN appliances, and a spam filtering appliance. So, I had three options: look for a 0day in Joomla, look for a 0day in postfix, or look for a 0day in one of the embedded devices. A 0day in an embedded device seemed like the easiest option, and after two weeks of work reverse engineering, I got a remote root exploit. Since the vulnerabilities still haven't been patched, I won't give more details, but for more information on finding these kinds of vulnerabilities, see [3] and [4].

[1] <http://pastebin.com/raw.php?i=cRYvK4jb>
[2] <http://sourceforge.net/projects/joomscan/>
[3] <http://www.devttys0.com/>
[4] <https://docs.google.com/presentation/d/1-mtBSka1ktdh8RHxo2Ft0oNN1Ip7WmDA2z9zzHpon8A>

--[6 - Be Prepared]-----

I did a lot of work and testing before using the exploit against Hacking Team. I wrote a backdoored firmware, and compiled various post-exploitation tools for the embedded device. The backdoor serves to protect the exploit. Using the exploit just once and then returning through the backdoor makes it harder to identify and patch the vulnerabilities.

The post-exploitation tools that I'd prepared were:

1) busybox

For all the standard Unix utilities that the system didn't have.

2) nmap

The worst thing that could happen would be for my backdoor or post-exploitation tools to make the system unstable and cause an employee to investigate. So I spent a week testing my exploit, backdoor, and post-exploitation tools in the networks of other vulnerable companies before entering Hacking Team's network.

Persistent ?

----[13.2 - Persistence]-----

Once you have access, you want to keep it. Really, persistence is only a challenge for assholes like Hacking Team who target activists and other individuals. To hack companies, persistence isn't needed since companies never sleep. I always use Duqu 2 style "persistence", executing in RAM on a couple high-uptime servers. On the off chance that they all reboot at the same time, I have passwords and a golden ticket [1] as backup access. You can read more about the different techniques for persistence in windows here [2][3][4]. But for hacking companies, it's not needed and it increases the risk of detection.

[1] <http://blog.cobaltstrike.com/2014/05/14/meterpreter-kiwi-extension-golden-ticket-howto/>
[2] <http://www.harmj0y.net/blog/empire/nothing-lasts-forever-persistence-with-empire/>
[3] <http://www.hexacorn.com/blog/category/autostart-persistence/>
[4] <https://blog.netspi.com/tag/persistence/>

Threat ?

----[13.3 - Internal reconnaissance]-----

The best tool these days for understanding windows networks is Powerview [1]. It's worth reading everything written by it's author [2], especially [3], [4], [5], and [6]. Powershell itself is also quite powerful [7]. As there are still many windows 2000 and 2003 servers without powershell, you also have to learn the old school [8], with programs like netview.exe [9] or the windows builtin "net view". Other techniques that I like are:

1) Downloading a list of file names

With a Domain Admin account, you can download a list of all filenames in the network with powerview:

```
Invoke-ShareFinderThreaded -ExcludedShares IPC$,PRINT$,ADMIN$ |  
select-string '^(.*) \t-' | %{dir -recurse $_.Matches[0].Groups[1] |  
select fullname | out-file -append files.txt}
```

Later, you can read it at your leisure and choose which files to download.

2) Reading email

As we've already seen, you can download email with powershell, and it has a lot of useful information.

3) Reading sharepoint

It's another place where many businesses store a lot of important information. It can also be downloaded with powershell [10].

4) Active Directory [11]

It has a lot of useful information about users and computers. Without being Domain Admin, you can already get a lot of info with powerview and other tools [12]. After getting Domain Admin, you should export all the AD information with csvde or another tool.

5) Spy on the employees

One of my favorite hobbies is hunting sysadmins. Spying on Christian Pozzi (one of Hacking Team's sysadmins) gave me access to a Nagios server which gave me access to the rete sviluppo (development network with the source code of RCS). With a simple combination of Get-Keystrokes and Get-TimedScreenshot from PowerSploit [13], Do-Exfiltration from nishang [14], and GPO, you can spy on any employee, or even on the whole domain.

To recap

- The attacker
 - was highly motivated to break into the specific target
 - spent good amount of time for reconnaissance
 - developed a custom exploit for one of the edge appliances
 - was able to easily perform lateral movement once inside
- The target
 - A company with fair amount of security skills
 - Little external exposure
 - Network segregation

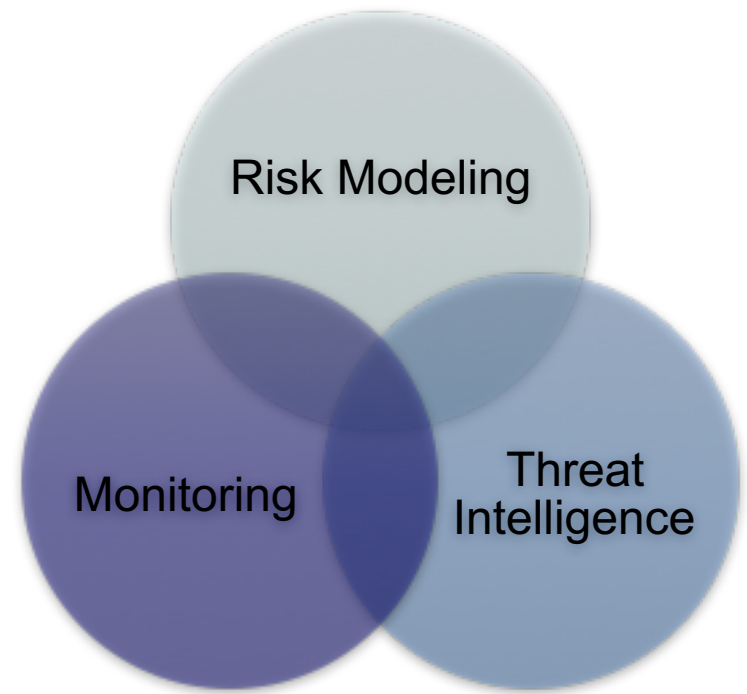


Lessons learned

- There could have been some monitoring in place, but was it analyzed regularly ?
 - Perhaps not
- Patching was not properly implemented
 - The attacker was able to exploit the Nagios server which monitored the 'segregated' network which contained the source code for the main product
- Proper segregation
 - Not a panacea
 - Air gap networks are just slow-latency networks 😊
- Egress monitoring
 - The attacker was able to download all mails, confidential files and other sensible information (btw egress connection was unencrypted)

What can be improved

- Risk profiling and baseline
 - Risk analysis
- And only then implementation of controls
- Threat intelligence
- Monitoring
 - Getting the data
 - Processing the data
 - Analyzing the data
- Reassess the risk
- Vulnerability assessment and penetration tests
 - Actionable reports are crucial
- Wargaming and redteaming



What is your threat model ?

1. Identify your assets
 - Responsibility
2. Topology/architectural view
3. Identify and document the threats
 - Why will some threat agent (aka bad guy) target us ?
 - It isn't a threat if it doesn't impact your business
4. Rate the threats

Proper risk management



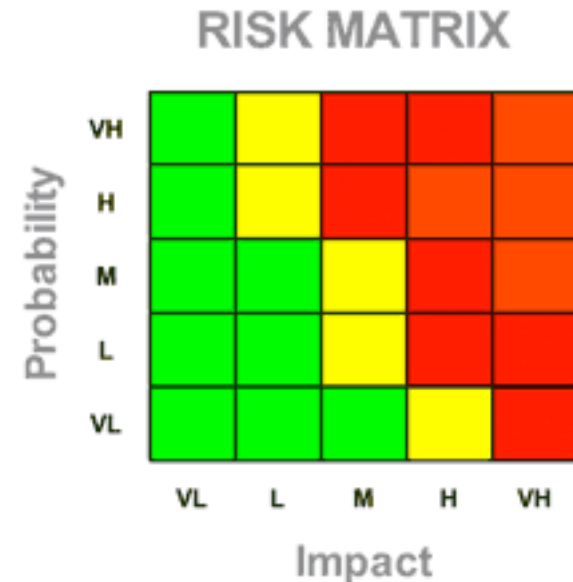
"WE'VE NARROWED OUR SECURITY RISKS DOWN TO THESE TWO GROUPS."

Risk analysis – start with the basics



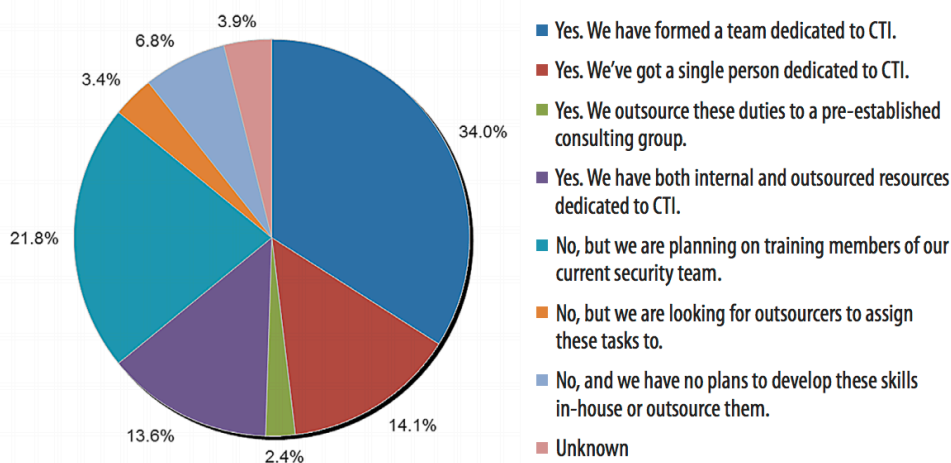
Getting a clear risk picture

- Prioritize
- Which controls have to be implemented/updated in the first place ?
 - Pushing most of the cases downwards left
- Appoint responsibility
- Keep in mind:
 - This matrix is dynamic
 - Things will have the tendency to move upwards right...
- Not enough
- How to keep things under control ?



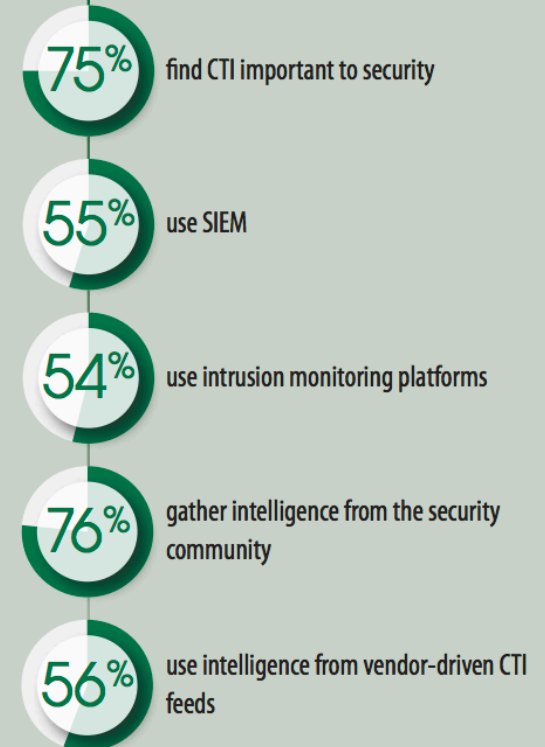
Threat Intel

- The set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators [SANS]
- This is how you monitor what's happening out there
- Discover new threats
- Feedback loop to your dynamic risk management program



Staffing for Threat Intelligence programs across organisations surveyed by SANS

Tools to aggregate, analyze and present CTI



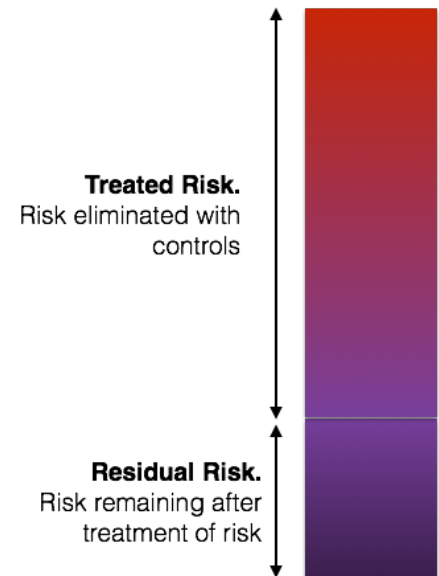
Monitoring

- Traffic Analysis
 - Ingress/egress traffic
 - Internal traffic
- Log Analysis
 - Privileged Users
- Honeypots
- Analysis – means some human interaction and interpretation of data
 - Reporting
- Vulnerability scans
 - Gives you a snapshot at a time T
 - Diff snapshots and find outliers - any new ports open ? Missing patches ?
- Continuous tuning
 - Update your IOC
- It's a process



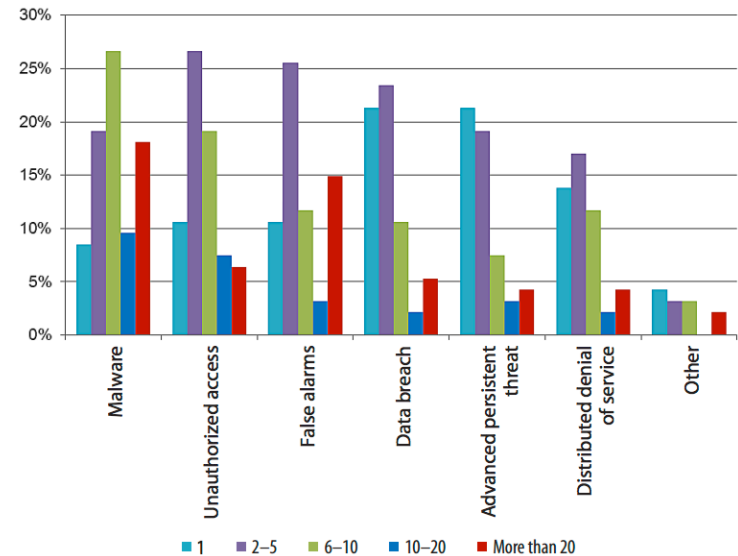
Residual risk - cyberinsurance

- What about residual risk ?
- Cyberinsurance is a highly hyped phenomenon
 - In 2015 market estimated at \$2.5 billion
 - For 2020 between \$5 billion and 10\$ billion
- The challenge:
 - Information security risk difficult to model
 - Threats and risks evolve
- Insurance coverage and premium are a mess
 - Misunderstanding between insurers and customers
 - What is covered ?
 - Direct vs indirect damage
 - Damage to reputation, stolen files, Intellectual Property are not covered
 - In case of widely exploited 0day – domino effect
 - Small companies vs large companies
- You better know well your risk model & read the insurance policy before subscribing



Incident response

- Removing threat from your organization
 - Investigation and remediation
- It is just a question of “when”, not “if”
- Responsibility – Computer Incident Response Team (CIRT)
 - Clear Mission
 - Planning
 - Communication
 - Practice
- Know your data
 - Monitoring

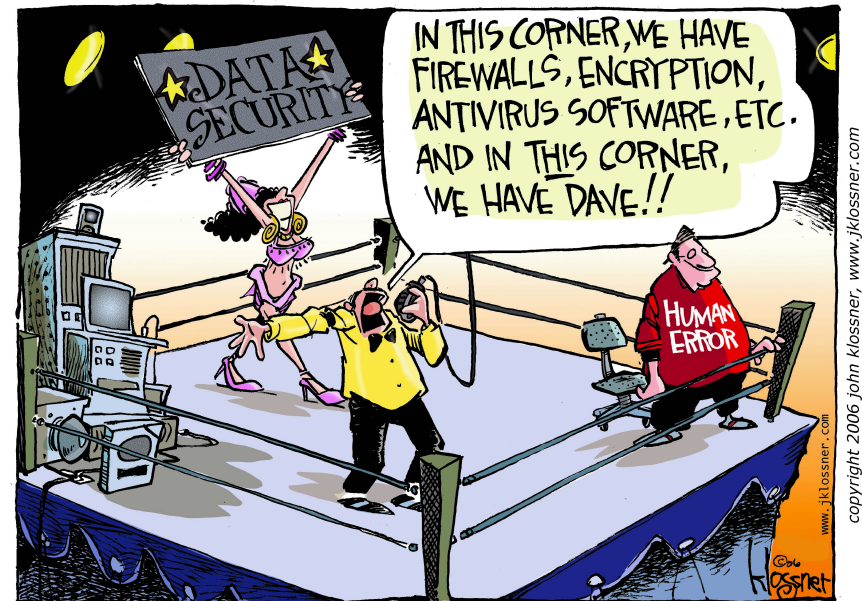


Wargaming and {red, purple} teaming

- Additionally to 'standard' vertical pentests and vulnerability scans
- Red Teams
 - Scenario-driven
 - Simulating a real attack (TTPs used by various threats)
 - Throughout test of controls
 - Correction recommendations
- Blue Teams
 - Your monitoring and IR team
- Purple Teams
 - New industry trend
 - Aimed to synergize collaboration between red & blue teams
 - How do you know remediation is working?
- Wargaming
 - Multidisciplinary
 - 'Playing' scenarios and situations that might arise and have impact on business
 - Excellent way to review risks

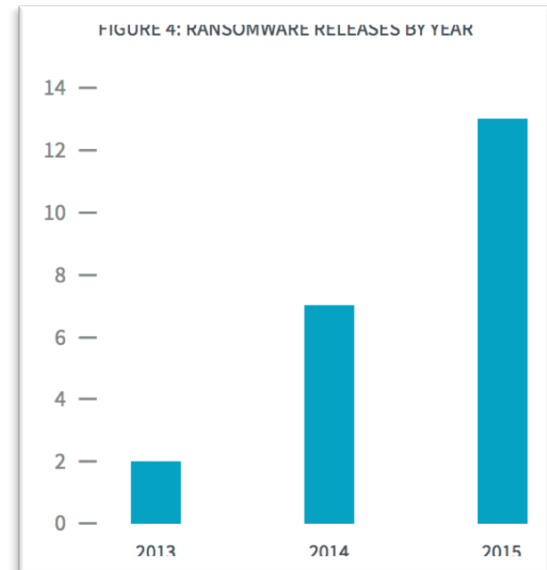
User awareness and education

- One of the most challenging parts
 - Many model that breach has already occurred because of user
 - Don't exclude it from your threat model!
- Threats
 - Phishing attacks – that's the most efficient vector for targeted attacks today
 - Client-side vulnerabilities
- Part of preventive 'controls' to implement
- Continuous process
- Importance of measurement during assessments
 - Should be part of manager's KPI



Cryptolockers and ransomware

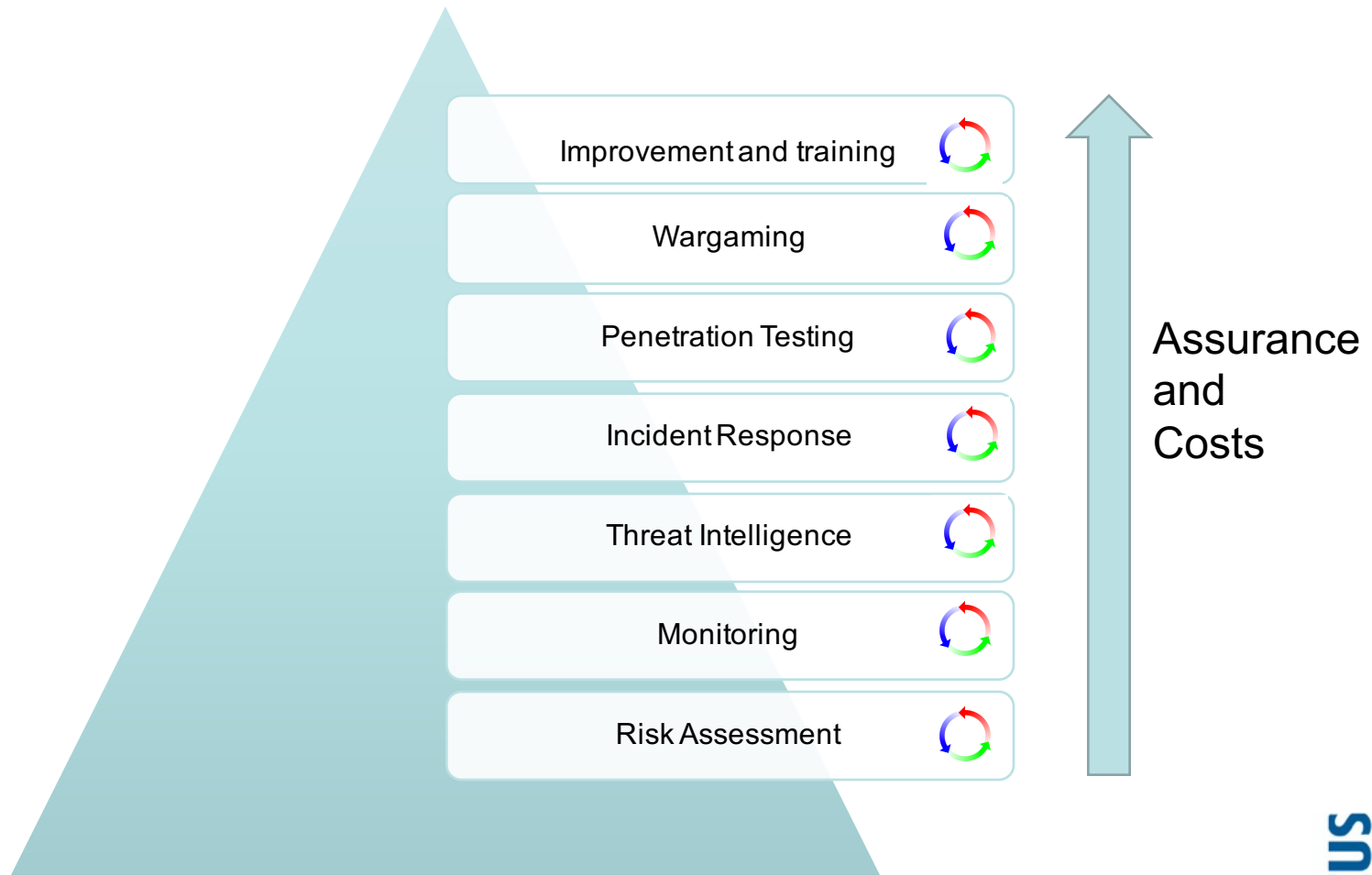
- Threat trend on the rise
 - Not really an APT, but rather a well-established business model by cybercriminals
 - ‘Product’ becoming better with every iteration
 - Ransomware-as-a-Service
- Usually spread using email phishing
 - User awareness
 - Monitoring
 - Backups
- But also on Android devices
- With modern ransomware your chances of decrypting your files yourself are less than 10%



Continuous training and keeping skills sharp

- Attackers learning continuously
 - We need to improve our TTP
- OSINT Threat Intel Sources
- Capture-The-Flag competitions
 - SANS regular CTFs
 - Various CTFs with different difficulty levels
 - Writeups
- Many challenges and vulnerable VMs
- Certifications
 - SANS has an excellent portfolio
 - Offensive security pentesting certifications (for self-learning)

Pyramid of information security needs



Concluding remarks

- APTs are here to stay
- Whether coming from Governments or Dedicated/Motivated/Persistent attackers
- Discovery of APT is a challenge in itself
- Not a single battle, but many ones
 - Understanding your organization
 - Understanding the threats

Thank you for your attention

***e*FOCUS**