

Advanced Persistent Threats vs. Defenders: That is why we keep losing this game

Nikos Virvilis



3rd ISACA ATHENS CHAPTER CONFERENCE
Emerging from Crisis - The risks, the opportunities and the real value of IT
ATHENS | 2 & 4 November 2013

Advanced Persistent Threats vs. Defenders: That is why we keep losing this game

Nikos Virvilis

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.

NIST: APT Definition

“... An adversary that possesses **sophisticated levels of expertise** and **significant resources** which allow it to create opportunities to achieve its objectives by using **multiple attack vectors** (e.g., **cyber, physical, and deception**)....

This presentation focuses on the cyber part.

APT Objectives

- Information Gathering / Data exfiltration
- Sabotage



Average Administrator vs. ...



NATO UNCLASSIFIED

...these guys



NATO UNCLASSIFIED

It is not all APT

APT:

- Stuxnet
- Operation Aurora
- More...

Unfortunately APT is misused as an excuse:

- For organizations which suffer a compromise due to a bad secure posture

June 2009: Stuxnet

Mission: Sabotage of the Iranian Nuclear Program (Natanz uranium enrichment plant)



(Photo: DigitalGlobe and Institute for Science and International Security)

Stuxnet: Payload

Stuxnet interfered with Industrial Control Systems (ICS) forcing centrifuges to operate outside limits and eventually destroy them.



NATO UNCLASSIFIED

Can you build Stuxnet?

- Skilled programmers
- Exploit Development (or access to 0-day market)
- Centrifuges? (Cannot find this on ebay...)
 - How do you operate them?
 - You need a test bed...
 - Each infrastructure is different so you need insider info!

Bottom line:

Significant financial - technical - intelligence resources

Random “APT” incident

- Download Poison Ivy
- Pack it (commercial packers work great).
- Craft a clever email and send it to HR ...

- Can we consider this an APT attack?

How do we fix that?

- No silver bullet
- A recipe to failure:
 - Focus on APT when you don't follow security best practices
 - You don't have the (right) people
 - You don't have C – Level Support

Security Best Practices

- Unpatched systems for 2+ years anyone? (Yes sure, you have a firewall in front)
- Network segmentation
- Inventory of authorized devices
- **Proper** log/event monitoring analysis
- Much much more...

<https://www.sans.org/critical-security-controls/>

People, People, People

Our average admins:

- The good: Skillful, willing make the difference, but usually they have a million other things to do...
- The bad: Limited skills but willing to learn... Need to invest significant time and resources for training.
- The ugly: My working hours are 08:00 – 14:30. If it works don't touch it. Not my problem. No technical skills...
- They need find and fix all vulnerabilities

And the APT:

- Advanced technical skills, Access to 0-day exploits
- Persistent, they are targeting **YOU** and they won't stop until they succeed
- Access to significant financial, technical and intelligence resources
- They only need to find and exploit one vulnerability

C-Level Executives

- C-Level executives have (hopefully) spent \$\$\$ buying all sort for fancy security solutions.
- Some of the products actually state that detect and block APT! (Don't you love pre-sales people?)
- After all, in the past incidents were clear: Defaced website, worm outbreak, virus infections. Now everything seems alright... Is it?
- When was the last time you hired someone to do a proper pentest? Did you defenses work?

Bad news

- “... Since **prevention is no longer effective**, detection must take a higher priority...” – E. Cole
- “**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

Utopia...

- So you have already implemented security best practices
- You have highly skilled, motivated people
- And you have C-Level Support
 - E.g. Financial Support
 - Willing to change the way the organization works

What are we trying to achieve?

- Prevention will eventually fail, thus we need to focus on detection
- Even if we detect the incident a few days after initial compromise!
- Don't forget, at the major APT incidents, attackers have spent months until they managed to get access to the information they wanted. (e.g. Operation Aurora)

Countermeasures

- The easiest to implement countermeasures (and probably cheaper too) are presented first.
- Remember, unless you already have a robust security posture, defending against APT it's a lost cause! Fix that first!

Security AND Obscurity

- I said **AND**
- Attacker gains a foothold to the network:
 - She needs to find where the information that she is interested in is located.
 - In a medium to large organization there are several hundred systems.
- **Active Defense Harbinger Distribution (ADHD)**
<http://sourceforge.net/projects/adhd/>
- <http://www.honeynet.org/>

Its time for your first NSM

Don't you have/cannot afford a commercial IDS/Full Packet Capture/Log collection and correlation infrastructure?

Enter Security Onion:



Free, Open source, Click and Run!

(But please, spend a few days fine tuning the IDS rules and review the alerts at least once daily!

Baseline your network protocols

- Create baselines of your network / systems and look for anomalies!
- Protocol Distribution!
 - Average_DNS_requests = X
 - If Average_DNS_requests > 10 * X:
 - print “DNS Tunnel??”

Baseline - HTTP

- Test case HTTP:
 - Legitimate browsing:
 - Client to Server: Small data packets (GET requests)
 - Server to Client: Large (multiple) data packets (web page contents)
 - Data exfiltration: The opposite!
 - Monitor for long lived TCP connections
 - Monitor where (countries) your systems are connecting to.

Baseline Workstations/Servers

- Workstations/Servers:
 - Running Services
 - Running Processes
 - Connections: Why is THAT workstation connecting to all our servers?

Whitelisting

- **Hopefully** you can only access the internet through a proxy server
- Exfiltrate data → Upload it somewhere on the internet
- Whitelisting:
 - Ask your employees for their favorite 10 websites
 - Include those and all work related ones. Block everything else!

Do you know what you are protecting?

- Do you actually know where your sensitive information is located?
- Assuming that you do (!), do you protect equally well your backups?
- Risk assessment (and yes you need to read the report in the end!!)

Lots more but...

- The key point to remember is that security solutions will never address the issue effectively
- It's people against people
- So...

Invest

Invest

Invest in

in

Invest in your

your

Invest in your people

people

References

- [1]. Bejtlich, R., *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, USA, 2013.
- [2]. Cole, E., *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Syngress, USA, 2012.
- [3]. Doumas, A., Mavrouidakis, K., Gritzalis, D., and Katsikas, S., "Design of a neural network for recognition and classification of computer viruses", *Computers & Security*, Vol. 14, No. 5, pp. 435-448, 1995.
- [4]. Katsikas, S., Spyrou, T., Gritzalis, D., and Darzentas, J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
- [5]. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., and Gritzalis, D., "An Insider Threat Prediction Model", in *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business*, pp. 26-37, Springer (LNCS 6264), Spain, 2010.
- [6]. Kandias, M., Virvilis, N., and Gritzalis, D., "The Insider Threat in Cloud Computing", in *Proc. of the 6th International Workshop on Critical Infrastructure Security*, pp. 93-103, Springer (LNCS 6983), Switzerland, 2011.
- [7]. Soupionis, Y., and Gritzalis, D., "Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony", *Computers & Security*, Vol. 29, No. 5, pp. 603-618, 2010.
- [8]. Virvilis, N., Dritsas, S., and Gritzalis, D., "Secure Cloud Storage: Available Infrastructure and Architecture Review and Evaluation", in *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, pp. 74-85, Springer (LNCS 6863), France, 2011.
- [9]. Virvilis, N., Dritsas, S., and Gritzalis, D., "A cloud provider-agnostic secure storage protocol", in *Proc. of the 5th International Workshop on Critical Information Infrastructure Security*, pp. 104-115, Springer (LNCS 6712), Greece, 2010.
- [10]. Virvilis, N., and Gritzalis, D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in *Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing*, IEEE, Italy, 2013.
- [11]. Virvilis, N., and Gritzalis, D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in *Proc. of the 8th International Conference on Availability, Reliability & Security*, pp. 248-254, IEEE, Germany, 2013.