Lab 6. Advanced Persistent Threat Incident Handling

1. Possible identification of APT attack
2. Developing countermeasures against apt attacks
3. Evaluating countermeasures values
4. Group exercise to counter APT threats

This exercise provides students with information about methods commonly used by attackers during the Advanced Persistent Threat (APT) attacks as well as methods of discovering and protecting internal resources against these attacks. Examples used in the exercise are based on real incidents and observations. The objective is also to involve participants in creative approaches to establishing computer security system to deal effectively with and resolve the problem of APT attacks within an organisation.

During the exercise students will have a chance to learn how to develop and implement a good methodology for implementing security measures in an organisation, not only against APT attacks, but countering a variety of threats.

Specifically, during the exercise students will learn:

1) What are the characteristic aspects of the APT attacks?
2) What resources are usually attacked during APT attacks?
3) How to evaluate proposed security countermeasures?
4) How to build simple security strategy?

Background

Advanced persistent threat (APT) usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

For understanding this kind of attack in details it is worth to get familiar with explanation of all three aspects of the APT.

Advanced – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly “advanced” (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.

Persistent – Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a flood of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats that only need access to execute a specific task.

Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well-funded.

Detailed phases of the attack are presented on the figure below:

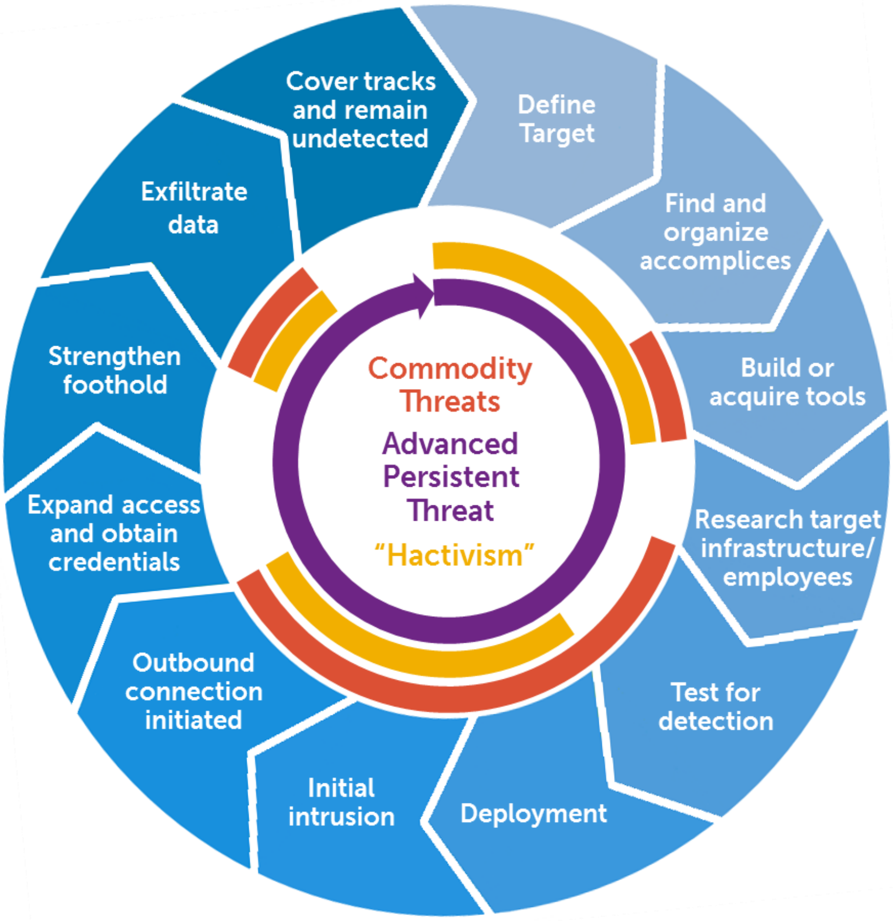
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Fig. 1. Phases of the APT attack

Exercises:

Task 1: Possible identification of APT attack

Look at the list of attacks. Your task is to decide if they are APT or not. Use the table below to mark your choices.

Table 1

№	Year	Description of the attack	APT (yes or no)
1	2003	SQL Slammer massive infections including DDoS attack effect against many servers Source: http://news.bbc.co.uk/2/hi/technology/2693925.stm	YES
2	2008	Chanology Attack on Scientology website by Anonymous Source: http://en.wikipedia.org/wiki/Project_Chanology	NO
3	2009, 2011	Aurora: a cyberattack against the information systems of a number of companies. The attackers attacked software configuration management systems that contained information from Goolgle, Adobe, and many others. Source: https://web.archive.org/web/20120911141122/http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others	YES
4	2009	Conficker worm massive infections including number of governmental security level networks Source: http://www.nytimes.com/2009/01/23/technology/internet/23worm.html	YES
5	2011	Attack on the Dutch Ceritificate Authority – DigiNotar Source: https://archive.f-secure.com/weblog/archives/00002228.html	
6	2011	Ghost Click infections. Approximately 4 mln infections in more than 100 countries Source: https://www.cnet.com/news/operation-ghost-click-dns-servers-to-remain-online-until-july/	YES
7	2012	Anonymous attack on Paypal and Mastercard Source: https://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court	NO
8	2012	DDoS attack on WikiLeaks by AntiLeaks Hacker Group Source: https://www.rt.com/usa/wikileaks-attacks-antileaks-group-293/	NO
9	2014	BlackEnergy attack targeting specific Ukrainian government facilities Source: https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf	YES

Task 2: Developing countermeasures against APT attacks

These countermeasures should be recognised as those which can limit the probability of successful APT attacks as well as those which increase the capability of better incident handling process after the APT attack has occurred.

The task for you is to propose **three countermeasures** into five following groups:

1. Network monitoring
2. Email protection
3. Protection against the spread of malware

4. System and network configuration
5. Security awareness

You should propose practical and concrete ideas. ***You should avoid general solutions like:*** Intrusion detection system or intrusion protection system, Spam filtering, Antivirus solution, Automatic patching

Focus on the most technical aspects.

Here are examples:

1) *Monitor outbound traffic to particular set of domains which are recognised as "bad sites",*
2) *Monitor existence in "your network" examples of short named executable files, e.g. a.exe or b.exe, which are quite often used in malware distribution,*
3) *Monitor SMTP (Simple Mail Transfer Protocol) traffic with content related filters and discover words often used in APT attacks, like: "budget" AND "salary", "organisational changes", etc.*
4) *Monitor network traffic with repeatable characteristic, e.g. regular request from the same internal host in the equal time slots.*

You should use next form presented below for presenting your proposals. It included columns – ES and EF. These are shortcuts for Easiness (of implementation) and Effectiveness (of usage).

Table 2

	COUNTERMEASURE PROPOSAL	**EES**	**EEF**
	NETWORK MONITORING		
1	PCI DSS monitors incoming traffiv and blocks all hacking attempts	1	3
2	domain whitelisting	2	2
3	Virtual testing for unknown malicious code	3	3
	EMAIL PROTECTION		
1	Filtering incoming emails to prevent spam and phishing attacks targeting network	2	3
2	Never follow a link to a secure site from an e-mail—always enter the URL manually	3	2
3	Use the anti-phishing features offered by email clients and web browsers	1	3
	SPREAD OF MALWARE		
1	Dynamic malware analysis (i.e., sandboxing)	1	3
2	A WAF feature that takes a novel approach to backdoor detection	2	2
3	DDoS Protection secures all your assets at the edge for uninterrupted operation	1	1
	SYSTEM AND NETWORK CONFIGURATION		
1	Monitor all network traffic	1	2
2	Custom sandbox analysis	3	3
3	System integrity monitoring and Behavioral monitoring and virtual patching	2	2

Task 3: Evaluating countermeasures values

The next task is to make the evaluation of proposed countermeasures. There are two, earlier mentioned metrics of this evaluation: **easiness (ES) and effectiveness (EF).**

Easiness is a metric describing how easy is to implement a particular countermeasure (considering factors like budget, technical sophistication or people and management resistance in solution acceptance).

Effectiveness is understood as overall evaluation of how good the solution will be in terms of protection against APT attacks.

The algorithm for preparing evaluations is the following:

- ES is valued from 1 (difficult) to 3 (easy)
- EF is valued from 1 (low effective) to 3 (high effective)

Pay attention to the countermeasures that received the lowest and highest scores. Why do you think a particular idea is so ineffective or why another is very effective?

Answer:

Task 4: The exercise to counter APT threats

Here is presented the list of fictional organizations and their most important assets:

1) Bank
   a. customer account information
   b. integrity of web banking interface
   c. financial assets of customers
   d. integrity of bank's website
   e. availability of web banking interface
2) University (or/and) Research Institute
   a. Integrity of research data
   b. Access to data processing centres
   c. Access to students accounts
3) Military
   a. Communication lines between military divisions
   b. Command centres availability
   c. Command centres integrity
4) Contractor
   a. Confidentiality of contracts
   b. Confidentiality of financial data
   c. Availability of production systems
   d. Availability of IT services for customers

Imagine that you are a security officer in each of the proposed organizations. Answer next questions:

№	Tasks	Results
1)	What are the most dangerous attacks against every other type of organization?	financial assets of customers
2)	Choose one particular attack which you consider to be the most dangerous against every other organization and create countermeasures against those attacks.	Data encryption,Anti-phishing,Biometrics Physical access control,Second factor authentication
3)	Suggest one attack scenario against one chosen group.	High impact operational risk scenario
4)	Ask the other students in your group to rate their defense system against the attack scenario you have planned in 3).	5
5)	Similarly, evaluate your own countermeasures (described in 2)) against the attacks of your teammates. If there is no countermeasure against the attacks other students suggested, the attack is considered successful. Were your countermeasures effective?	yes

References:

1. “Assessing Outbound Traffic to Uncover Advanced Persistant Threats” – SANS Technology Institute - http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf

2. “A Detailed Analysis of an Advanced Persistent Threat Malware” – SANS Institute - http://www.sans.org/reading_room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware_33814

3. Computer Security Fundamentals: Computer Security Fundamentals, 2/Edition, William (Chuck) Easttom, II. (2012, Pearson Education Company), ISBN-13:9780789748904