Advanced persistent threat incident handling

Handbook, Document for teachers

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

Table of Contents

1 Introduction

Goal

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 building CERT capability to deal effectively with and resolve the problem of APT attacks within an organisation.

Target audience

Incident handlers and technical staff responsible for organising security measures and providing incident handling within an organisation

Course Duration

3 hours

Frequency

Once per new CERT member; additionally, repeated yearly

Structure of this document

	Task	Duration
	Introduction to the exercise – explaining the anatomy of the APT attacks	20 min
	Task 1: *Possible identification of APT attacks*	20 min
	Task 2**:** Developing countermeasures against APT attacks	60 min
	Task 3: Evaluating countermeasures values	30 min
	Task 4: *Group exercise to counter APT threats*	30 min
	Summary of the exercise	20 min

2 General Description

During the exercise you 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 you will learn:

- What are the characteristic aspects of the APT attacks?

- What resources are usually attacked during APT attacks?
- How to evaluate proposed security countermeasures?
- How to build simple security strategy?

3 EXERCISE COURSE

Follow the instruction and explanation provided by the trainer.

3.1 Introduction to the exercise

To define the common language for discussing the APT attacks you should learn the definition of it. The proposed one is the definition from Dell SecureWorks1:

"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."[1]

For understanding this kind of attack in details it is worth to get familiar with explanation of all three aspects of the APT[2].

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 barrage 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

---

[1] the definition is a combination of three different sources: Anatomy of an Advanced Persistent Threat (ATP)". Dell SecureWorks. Retrieved 2012-05-21 (http://go.secureworks.com/advancedthreats), "Are you being targeted by an Advanced Persistent Threat?". Command Five Pty Ltd. Retrieved 2011-03-31 (http://www.commandfive.com/research.html) and "The changing threat environmnt...". Command Five Pty Ltd. Retrieved 2011-03-31 (http://www.commandfive.com/research.html).

[2] "What's an APT? A Brief Definition". Damballa. January 20, 2010 (https://www.damballa.com/knowledge/advanced-persistent-threats.php).

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.

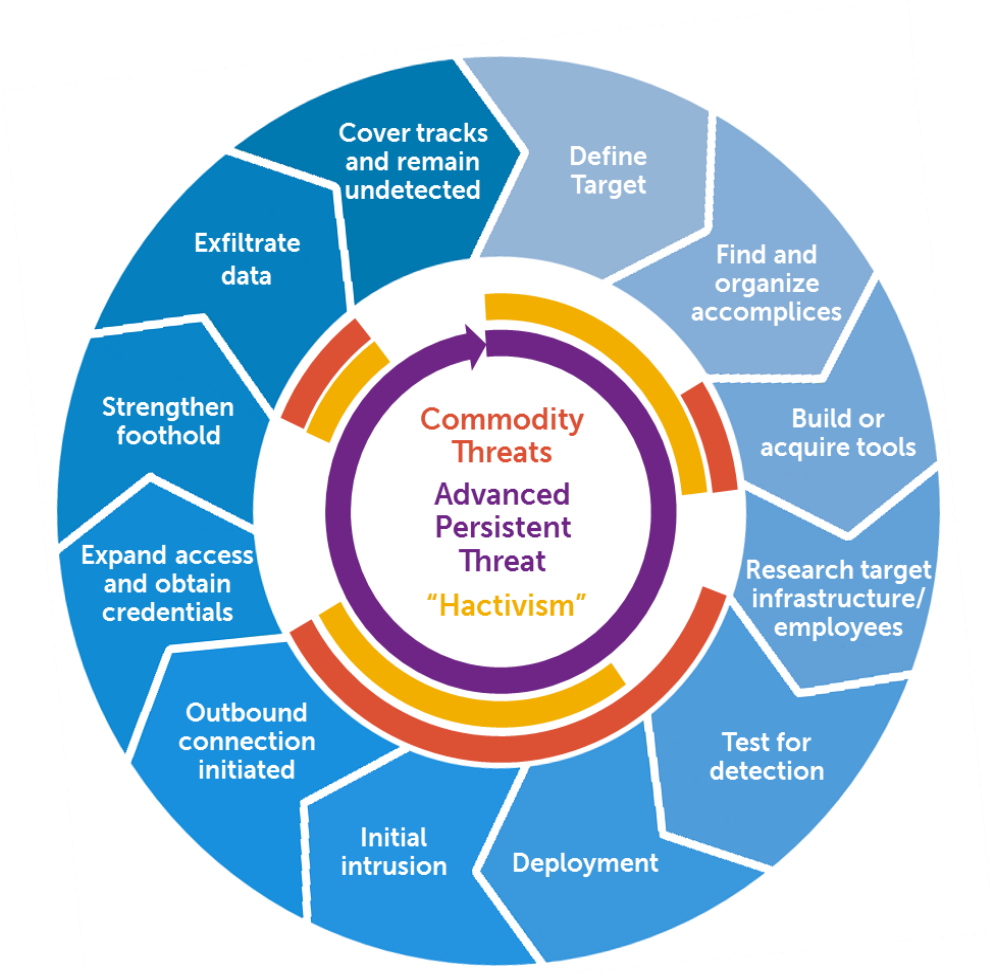

Figure 1 - Anatomy of the APT attack[3]

Now, knowing more about the APT attacks, it is good to discuss the examples of such attacks. The trainer will provide you few of them. Maybe you can add some more from your knowledge or even your own experience.

3.2 Task 1: Possible identification of APT attack

Now, the trainer will outline number of past attacks. Your task is to decide if they are APT or not. Use the table below to mark your choices.

[3] http://en.community.dell.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-46-04/7711.Advanced_5F00_Persistent_5F00_Threat_5F002D005F00_APT_5F002D005F00_Lifecycle.png

No	Year	Attack short description	APT yes or not?
1	2001	Anna Kurnikova virus. Massive PS infections after opening the attachment[4].	
2	2003	SQL Slammer massive infections including DDoS attack effect against many servers[5]	
3	2008	Chanology Attack on Scientology website by Anonymous[6]	
4	2009	Conficker worm massive infections including number of governmental security level networks[7]	
5	2010	Anonymous attack on Paypal and Mastercard[8]	
6	2011	YouTube channel of Sesame Street hacked and streaming pornographic content[9]	
7	2011	Attack on the Dutch Ceritificate Authority - DigiNotar[10]	
8	2011	Ghost Click infections. Approximately 4 mln infections in more than 100 countries[11]	
9	2012	DDoS attack on WikiLeaks by AntiLeaks Hacker Group[12]	

3.3 Task 2: Developing countermeasures against apt attacks

[4] „Kurnikova computer virus hits hard" - http://news.bbc.co.uk/2/hi/science/nature/1167453.stm
[5] „Virus-like attack hits web traffic" - http://news.bbc.co.uk/2/hi/technology/2693925.stm
[6] http://en.wikipedia.org/wiki/Project_Chanology
[7] „Worm infects Millions of Computers Worldwide" - http://www.nytimes.com/2009/01/23/technology/internet/23worm.html
[8] „Operation Payback Attacks Target MasterCard and PayPal sites to Avenge WikiLeaks" - http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sites-to-avenge-wikileaks/
[9] "Sesame Street YouTube Channel Hacked With Porn" - http://abcnews.go.com/blogs/headlines/2011/10/sesame-street-youtube-channel-hacked-with-porn/
[10] „DigiNotar Hacked by Black.Spook andIranian Hackers" - http://www.f-secure.com/weblog/archives/00002228.html
[11] „Operation Ghost Click DNS servers to remain online until July" - http://reviews.cnet.com/8301-13727_7-57392756-263/operation-ghost-click-dns-servers-to-remain-online-until-july/
[12] „WikiLeaks shut down by American hackers" - http://rt.com/usa/news/wikileaks-attacks-antileaks-group-293/

Task 2 for you is to develop various 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 [13]. This is a group work and the best size for groups is 3-4 participants and it is recommended not exceed to number of 4 groups to limit time for group presentations during the next phases of the exercise. A trainer should divide participants into groups also avoiding participants from the same organisation in one group.

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

- Network monitoring
- Email protection
- Protection against the spread of malware
- System and network configuration
- Security awareness

Instruct participant that they should propose practical and concrete ideas. They should avoid general solutions like:

- Intrusion detection system or intrusion protection system
- Spam filtering
- Antivirus solution
- Automatic patching

This list does not include all possible kind of solution, e.g. employee's awareness, but an intention is to focus on the most technical aspects.

To give to participants ideas and inspiring them what kind of concrete measures should be provided, you can give the following examples:

- *Monitor outbound traffic to particular set of domains which are recognised as "bad sites",*
- *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,*
- *Monitor SMTP traffic with content related filters and discover words often used in APT attacks, like: "budget" AND "salary", "organisational changes", etc.*
- *Monitor network traffic with repeatable characteristic, e.g. regular request from the same internal host in the equal time slots.*

Participants should use the form presented below for presenting their proposals. It included to not self-explanatory columns – ES and EF. These are shortcuts for Easiness (of implementation) and Effectiveness (of usage). But do not explain these meanings to participants, as for this task they should not deal with these evaluation metrics.

	COUNTERMEASURE PROPOSAL	**EES**	**EEF**

[13] please check the exercise „Cost of ICT incident calculation".

	NETWORK MONITORING		
1			
2			
3			
	EMAIL PROTECTION		
1			
2			
3			
	SPREAD OF MALWARE		
1			
2			
3			
	SYSTEM AND NETWORK CONFIGURATION		
1			
2			
3			

Once you have participants ready with their proposal, ask group representatives to present their ideas. Each participant should shortly describe, explain their technical implementation, why they decided to put it on the list. Additionally they should, if possible and they agree to share this information, whether they have implemented such solution in their network and what are their experiences from using it. Try to keep a report from the group work short and concrete. If ideas repeat in more than one group, ask to provide only new description and explanation in comparison to an initial presentation by other group.

During this presentation you should write down all ideas on a blackboard, but only unique ones. In your table on a blackboard also add columns ES and EF.

Remember that for this task and especially for presentations by groups, the most important is to give participants a chance as much as possible about various methods of protection against APT attacks.

3.4 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). Explain the metrics telling participants that 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), and telling them that 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)
- ES is valued only by ideas owners, if more than one group proposed the same idea, all of them propose their value
- ES is proposed on the original form used in the task 1 and as mentioned above – this evaluation is prepared only by ideas owners, so it will be documented only on their forms
- EF is valued from 1 (low effective) to 3 (high effective)
- EF is proposed for all groups, which did not develop a particular idea. The proposed value based on the idea explanation, provided by ideas owners and presented at the end of the task 1. Other groups try to evaluate their real values.
- EF is proposed on the same form (as used during the Task 2)

After this evaluation gather information from all groups, by simply providing numbers by them, and write it down on the blackboard in the earlier prepared columns ES and EF. Apply the following algorithm:

- For ES value of an idea use a value proposed by the idea owner. If more than one group valued the idea – use the average value.
- For EF value of an idea use a value which is an average value of all notes[14]

3.5 Task 4: Group exercise to counter APT threats

Teacher will present the list of fictional organization and their most important assets:

a) 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
b) University (or/and) Research Institute
    a. Integrity of research data

[14] for easier counting and presenting, as well as the further discussion, you can prepare as many columns for EF as groups

b. Access to data processing centres

c. Access to students accounts

c) Military

a. Communication lines between military divisions

b. Command centres availability

c. Command centres integrity

d) Contractor

a. Confidentiality of contracts

b. Confidentiality of financial data

c. Availability of production systems

d. Availability of IT services for customers

Use the groups formed earlier and assign every group to be a different organization.

Instruct students to be in the same way defender and ask them also to discuss what are the most dangerous attacks against every other type of organisation. At the end of their internal discussion they should choose one particular attack which they consider to be the most dangerous against every other organisation. Also their task is to create countermeasures against attacks and one attack scenario against every other group.

Asks group leaders to write the defences on the blackboard and then let then describe the attacks. If there is no countermeasure against the most dangerous attacks, the attack is considered to be successful. Let the group discuss the outcome afterwards.

4 Summary of the exercise

The exercise ends with summary which mainly consists in presentation of the results of evaluation metrics. Also during the summary you can discuss the implementation of countermeasures. Firstly try to identify those ideas which received extreme judgments. Ask owners of the notes why they think that particular idea is so ineffective and at the same time the other group thinks is very effective (and vice versa). This is a good methodology to of discuss the real value of countermeasures and convince each other about particular solutions.

After the discussion you can propose a simple strategy for implementation. Count the value of each idea by using values of ES and EF. Then you can group ideas in three (possibly) equal groups with the highest, medium and low values. The obvious strategy is to start with the group of highest scored ideas and finish the process with lowest ones.

5 REFERENCES

- "Detecting Advanced Persistant Threat" – Splunk Corporation - http://www.splunk.com/web_assets/pdfs/secure/Splunk_for_APT_Tech_Brief.pdf
- "Assessing Outbound Traffic to Uncover Advanced Persistant Threats" – SANS Technology Institute - http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf
- "Advanced Persistent Threats: A Decade in Review" – Command Five Pty Ltd - http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf
- "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

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu