Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

RISKS OF ADVANCED PERSISTENT THREATS AND DEFENSE AGAINST THEM

SMIRAUS, M[ichal] & JASEK, R[oman]

Abstract: *The paper focuses on methods of Advanced Persistent Threat (APT) in connection with current cyber network attacks. It contains examples of major cyber-attacks which were associated with APTs over the past years. Methodology of an ATP attack is discussed and current trends are used to predict future APT targeting. In conclusion the options of base security policies are provided that could help to protect or enhance the defense against these modern worldwide cyber threats.*
Key words: *cybercrime, advanced persistent threat, network attacks, IT security, zero-day exploit*

1. INTRODUCTION

Advanced Persistent Threats (APTs) represent a real risk of contemporary world, in particular that of Internet enabled targeted espionage. Each part of this term is relevant. Advanced means the ability to maintain access to well-protected network and persistent indicates that the nature of possible threats is difficult to prevent access. Recognized modes of attack include infected media, supply chain compromise, and social engineering. Most of all attacks are led and organized in larger groups. Individual hackers usually cannot attack the system which is secured strong they more often choose vulnerable targets because they do not have enough money and equipment for the successful intrusion (Borders, 2007).

APTs on the other hand are not only well resourced and capable, but also persistent in their covert attempts to access sensitive information from their chosen targets, such as intellectual property, patent plans, negotiation strategies, financial results or political information. APTs are sophisticated attempts of intrusion which depend on the attacker's objectives, the tools and techniques available to them, and the anticipated ability of their target both to detect and defend against this kind of attack.

The intrusion activities performed by APT are not necessarily sophisticated, but the attackers have the possibility to upgrade their sophistication in order to obtain or maintain access to computer systems on which they are interested. The level of accomplishment may depend on many factors such as the anticipated ability of the target to detect the activity, the anticipated response of the target should the targeting be detected, the level of risk which the hacker is willing to accept, their timeframe to gain the desired information and the effects on their longer term goals.

2. WORLDWIDE CYBER THREATS

Currently, the APT is a term commonly used in relation to the dangers posed by foreign intelligence services and organized crime groups with links to the traditional espionage. Public reports of APT attacks date back to at least 1998, when the Pentagon, National Aeronautics and Space Administration (NASA), the United States (US) Energy Department, research laboratories and private universities were targeted. The last two years has seen increase in the number of organizations coming forward, admitting they have been targeted. It has also seen an escalation in US Securities and Exchange Commission (SEC) filings warning shareholders about the risks of new cyber-attacks.

First known targeting of an unnamed organization occurred using the Stuxnet worm. Numerous organizations, primarily in Iran were targeted. The worm appears to have been part of a coordinated effort to reprogram a specific industrial control system, such as a gas pipeline or power plant (Farlliere, 2011).

Australian parliamentary computers were accessed over a period of at least one month. During that time several thousand emails may have been accessed including those of the Australian Prime Minister, Foreign Minister and Defense Minister (Kobie, 2011).

Google detected a highly sophisticated and targeted attack on corporate infrastructure that resulted in the theft of intellectual property. This event is believed to have been part of a coordinated attack, known as Operation Aurora, in which hackers sought source code from Google, Adobe Systems and dozens of other high profile companies (Zetter, 2010).

Attack against RSA showed that sensitive information were stolen in order to facilitate the subsequent attacks against organizations that use RSA tokens as security for two factor authentication. This is also related to the U.S. Department of Defense which operates in secret projects (Coviello, 2011).

Based on the current trend of increasing use of cloud computing, virtualization is often used for separate data belonging to different customers. It could also make it easier for malicious software to escape from virtualized analysis platforms and infect connected systems.

This suggests that along with the growing virtualization ATPs will appear more often. Even though details of APT attacks are scarce in the media, the released information is not quite informative and concrete.

The most of companies that have come forward and admitted they are among the victims have not been approaching with the details. This is apparently because they do not want to provide the hackers with feedback, or cause additional awkward situation to their organization (company's reputation or share price). It is adverse that these potential negative consequences of detailed reporting are often seen to outweigh the community benefit of sharing lessons learned.

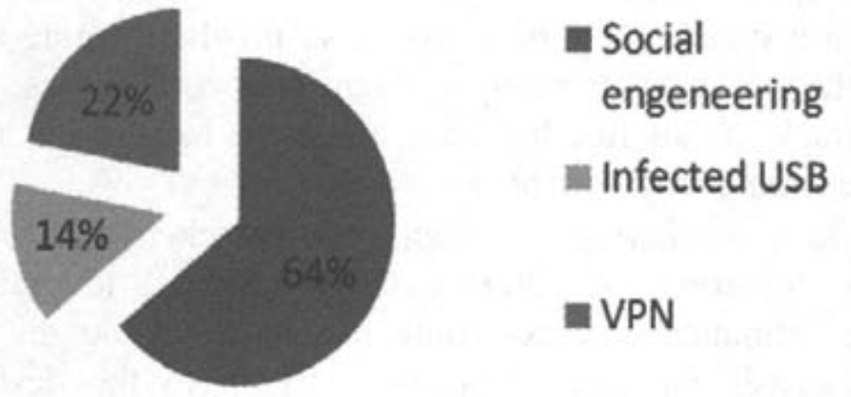

Fig. 1. The most common methods of attack based on APTs

3. METHODOLOGY OF THE APT ATTACK

As can be seen on Figure 1 the most common type of APT attack is social engineering, especially by social engineered emails or in combination with zero-day exploit which is tried to exploit computer application vulnerabilities that are unknown to others or the software developer. Many victims of modern cybercrime do not provide any details about the attacks against them, but RSA Securities with its algorithm for public-key cryptography is one of the few who has provided quite detailed information of occurred attack which was based on ATP. The attack methodology observed in a case of RSA can be quite similar as in other cases. Individual phases of attack are shown in Figure 2. (Rivner, 2011).

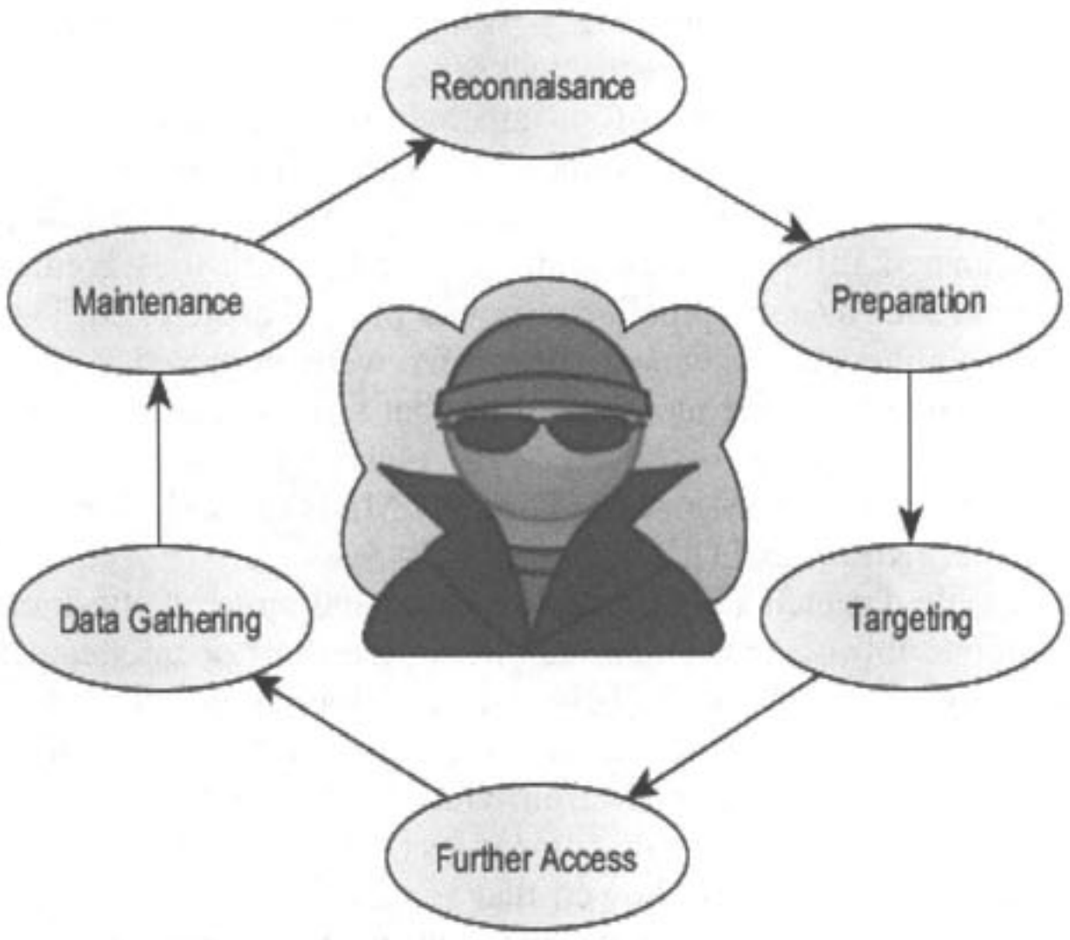

Fig. 2. Life cycle and methodology of APT attack

- Reconnaissance – passive information collection about target's offices, the location of their computers, their employees, interests and contacts to identify the best targeting method.
- Preparation – active preparation for the attack which may include developing appropriate tools and testing techniques to target their intended victim.
- Targeting – start of the attack when the attacker may try to connect remotely to a server to exploit vulnerability of the system, strategically place a USB flash drive or give one to a target, send socially engineered emails and if possible, check for bounce back notifications.
- Further Access – after successfully gained access to a computer network it is important to identify where in the network the attackers are and then move laterally within the network to access data of interest and to install additional backdoors. This will usually require a return to step 2 (Preparation) and step 3 (Targeting), the upload of tools and malicious software, privilege escalation, network enumeration and identification of vulnerable hosts on which to install backdoors. It may also involve gaining access to the domain controller to obtain password hashes, covering tracks by altering logs, and accessing mail or file servers to enable data gathering.
- Data Gathering – once an attacker has identified information of interest they will try to gather this information and ex-filtrate it. They may do this using a "smash and grab" approach, trying to the desired data before it is detected, or they may opt for a "low and slow" approach in which they ex-filtrate the data in small quantities over a longer period.
- Maintenance – once an attacker has gained access to a network for information gathering purposes they will usually attempt to maintain their access. This may affect the amount of malicious activity generate on the network to avert detection, periodically communicating with backdoors on the network to confirm they are working as advised and making changes as appropriate. If automated data gathering tools are in use, it may also involve modifying search terms or the exfiltration path. Maintenance also requires maintaining callback domains and any interceding infrastructure used to communicate with the backdoors. If access is lost, the attacker may return to step 1 (Reconnaissance) or step 2 (Preparation) in an attempt to regain access.

4. CONCLUSION

To improve organizational measures for protect against the modern Advanced Persistent Threats is necessary to employ also advanced security practices and policies such as those described below.

- Educate users and collaborate with IT staff to prevent threats of social engineering methods.
- Define multiple layers of security, affording the most sensitive information the most protection.
- Store more sensitive information offline if it is possible, or on a network with separate access.
- Patch operating system and program applications regularly
- Set users rights correctly and define network access restriction for computers which can be connected on the corporate network via wired and remote access methods.
- Control USB drives which can be used on corporate networks and develops policies on permitted usage and set up minimum encryption requirements.
- Conduct intrusion analysis (both host based and network based) to detect anomalous activity.
- Restrict user access using least privilege methodology, encourage good password control, regularly audit access logs, and review access levels.
- Employ the Sender Policy Framework to help protect against spoofed emails.

5. REFERENCES

Borders, K. (2007). Building a Threat Model: Hackenomics, *Available from:* http://www.straightsectalk.com/?p=16 *Accessed:* 2011-09-18

Coviello, A. (2011). Open Letter to RSA SecurID Customers, *Available from:* http://www.rsa.com/node.aspx?id=3891 *Accessed:* 2011-09-18

Farlliere, N., O Muchu, L., & Chiente, E. (2011). W32.Stuxnet, *Available from:* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf *Accessed:* 2011-09-18

Kobie, N. (2011). Lone Iranian claims credit for Comodo certificate has been hacked, *Available from:* http://www.pcauthority.com.au/News/252662,loneirianclaimscreditforcomodocertificatehack.aspx *Accessed:* 2011-09-18

Rivner, U. (2011). Anatomy of an Attack, *Available from:* http://blogs.rsa.com/rivner/anatomy-of-an-attack/ *Accessed:* 2011-09-18

Zetter, K. (2010). Google Hack Attack Was Ultra Sophisticated, *Available from:* http://www.wired.com/threatlevel/2010/10/operationaurora/ *Accessed:* 2011-09-18