MITIGATING ADVANCED PERSISTENT THREATS

Noor Azwa Azreen Abd Aziz and Zahri Yunos
CyberSecurity Malaysia
azreen@cybersecurity.my; zahri@cybersecurity.my
(*This article was published in the Computerworld Malaysia on 11 Oct 2012*)

INTRODUCTION

Technological threats in terms of security could be defined as any circumstances or events with the potential to adversely impact organisational operations (including mission, functions, image or reputation), organisational assets or individuals through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service. Advanced Persistent Threats (APTs) is one of the most common technological threats the world faces today. In Malaysia, there are growing concerns regarding the increase of incidents in the country. Organisations are urged to find counter measures in resolving the matter and should also step forward to create a safer cyber environment in the country.

CYBER SECURITY TRENDS IN MALAYSIA

The number of Internet users coming forward to report cyber security incidents to CyberSecurity Malaysia's Cyber999 Help Centre increase sharply over the last four years. Each year, the number of incidents handled by the centre has increased substantially. It has increased from 8,090 incidents in the year 2010 to 15,218 incidents in 2011. Even for the period between January to August this year, about 7,100 incidents has already been reported. This may be due to the increase of awareness among Internet users and also with adoption of standard and compliance such as ISO 27001 ISMS in the organisations. ISO 27001 ISMS provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS). The breakdown of these cyber

security incidents can be categorised as cyber harassment, fraud, content related, denial of service, intrusion, intrusion attempt, malicious codes, and spam. However, the statistics provided aforementioned is only the tip of the iceberg. There could be more unreported incidents in the country.

ADVANCED PERSISTENT THREATS (APTS)

In the digital age, intellectual property, personal and financial information, and other sensitive data types are at an increasing risk. Targeted attacks by Advanced Persistent Threats (APT) are becoming more and more widespread. APTs are the modern electronic versions of covert intelligence operations. *Advanced* here is defined as "sophisticated combination of multiple targeting methods, tools and techniques in order to reach and compromise target and maintain access to it." On the other hand, persistent is defined as "conducted through continuous monitoring and interaction in order to achieve the defined objectives". Threats comprise of both capability, intent and a level of coordinated human involvement.

A good case study for APT is the Stuxnet attack which occurred in 2010. Stuxnet is a sophisticated computer worm that infected Siemens' SCADA systems. This is a classic example of cyber attack targeting critical sectors. The attacks were primarily directed towards Iranian nuclear facilities, but there were also reports claiming that other countries such as India, Indonesia and Russia were also affected. Stuxnet is said to be the first known worm designed to target real-world critical sectors such as nuclear plant, power station and industrial unit. Some experts even believe that that Stuxnet is a government produced worm.

APT EXPLOITATION LIFE CYCLE

The APT exploitation life cycle involves reconnaissance, initial intrusion into the network, establishing a backdoor into the network, obtaining user credentials, installing various utilities, privilege escalation/lateral movement/data exfiltration and maintaining persistence. The explanation of each life cycle is explained below:

- Reconnaissance – Identify individuals of interest and develop methods of access. The targets range from executives to researchers to assistants.
- Initial intrusion into the network – Utilise several techniques to gain initial access. The most common form is social engineering combined with e-mail; e.g. spear phishing.
- Establishing backdoor into the network – Establish footing in the system using malware and move laterally to install multiple backdoors.
- Obtaining user credentials – Obtain domain controller credentials to allow operation within the network.
- Installing various utilities – Utility programs install backdoors, dump passwords, obtain e-mail from servers and list running processes to steal targeted information.
- Privilege escalation/Lateral movement/Data exfiltration – Exfiltrate data by compressing into smaller files and moving to a server in the APT's command and control infrastructure.
- Maintaining persistence – When backdoors are discovered, it will continuously evolve to gain additional footing and maintain position.

CHALLENGES

There are numerous challenges in achieving the high level of vision and knowledge required in order to address the threat of a targeted attack. Some of these challenges include:

- Organisation usually has an extremely large database and information management environment. Trying to find certain information is like *looking for a needle in a haystack*. It is very difficult, if not impossible to find among everything else around it.
- Attackers are skilled at hiding in plain sight
- Anti-forensic techniques are being used more frequently
- Complexity, diversity, and lack of standardisation are often a factor

Possible questions that should be thought about regarding specific information security practices are as follows:

- How do we track what digital information is leaving our organisation and where that information is going?
- How do we know who's really logging into our network, and from where?
- How do we control what software is running on our devices?
- How do we limit the information we voluntarily make available to a cyber adversary?

INCIDENT RESPONSE AND HANDLING

As attacks on information systems become more sophisticated and severe, it is important to develop a well-defined incident response capability. A dependable incident response program helps to quickly detect security incidents, minimize losses and destruction, identify weaknesses, and restore information technology operations rapidly.

There are four possible stages in incident response and handling as follows:

- Preparation – Ready to respond before an incident actually occurs. This stage is extremely important because many of today's incidents are so complex and time consuming that preparation is a necessity, not a luxury. Some basic notions behind preparation are setting up a reasonable set of defences/controls based on the threat that presents itself, creating a set of procedures to deal with incidents as efficiently as possible, obtaining the resources and personnel necessary to deal with the problem and establishing an infrastructure to support incident response activities.

- Detection and Analysis - Detection determines whether malicious code is present, files or directories have been altered, or other symptoms of an incident are present and, if they are, what the problem as well as its magnitude is. Detection is very important. Without detection, there is no meaningful incident response and detection triggers incident response. Sometimes, very small

symptoms may indicate that an incident is in progress and therefore, analysing every anomaly that can be found is a very good measure.

- Containment, Eradication and Recovery - Containment is to limit the extent of an attack and thus the potential damage or loss. Containment-related activity should occur only if the indications observed during the second stage conclusively show that an incident is occurring. Eradication is to eliminate the cause of the incident, while recovery involves system and data recovery as well as providing back-up files.

- Post-Incident Activity - To review and integrate information related to an incident that has occurred. This stage is extremely critical, in that it is hard to envision a successful incident response effort if it is omitted.

CONCLUSION

Cyber space is borderless and difficult to control, and it is seemingly vulnerable to criminal and terrorist attacks. It provides the room for individuals with the necessary skill and capability to cause damage; even to a nation. Cyber attacks are relatively so much easier to launch compared to conventional military attacks. The constantly increasing number of security incidents in Malaysia is indeed worrying, given the high and rapidly growing rate of Internet usage in the country. Technological threats such as cyber crime and cyber terrorism require immediate attention and critical analysis by nations worldwide. For example, there is still a need for improvement of cyber laws and regulations in the country. At the same time, the competency level of the enforcement agencies must also be further improved to deal with the growing sophistication involved in cyber threats. Malaysia is committed in countering cyber crime and cyber terrorism by implementing and enhancing critical information infrastructure protection to ensure a trusted, secure and sustainable online environment. Cyber security requires both national and transnational mechanism to deal with threats.