HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Török Szilárd
torok.szilard@gmail.com

SOME ASPECTS OF CYBER ATTACKS IN 2011

Absztrakt

Az elmúlt évek publikus informatikai biztonsági incidensei alapján a támadások mértéke, technológiai háttere jelentős átalakuláson esett át. A célzott, precízen előkészített támadások kerültek előtérbe, az okozott kár vagy a lehetséges veszteség mértéke többszörösére emelkedett. Jelen publikáció célja, hogy bemutassa a 2011 első félévében történt jelentősebb információbiztonsági eseményeken keresztül a biztonsági fenyegetések technológiai változását, ismertesse a támadások jellegét és hátterét, rávilágítson a célzott hacker és a hacktivista támadások közötti különbségre, majd ezekből kiindulva szakmai tanulságok levonásával összegezze a lehetséges, jövőben alkalmazható biztonsági megoldásokat.

Based on the public IT security incidents of the past few years the extents of the attacks and the technological background have gone through an immense change. The targeted, precisely prepared attacks gained ground, and the extent of the caused damage and possible loss has multiplied. The goal of this publication is to present and demonstrate the technological changes of IT security, the background and characteristics of attacks, and to highlight the differences between targeted hacking and hacktivist attacks through the significant IT security events taken place in the first term of 2011. These events will serve as a tool to summarize professional conclusions concerning possible future security solutions.

Kulcsszavak: *token hitelesítés, APT, böngésző tanúsítvány, hacktivista, social engineering, korai észlelés, nulladik nap kihasználása ~ token authentication, APT, browser certificate, hacktivist, social engineering, early detection, zero day exploit*

INTRODUCTION

In the first term of 2011 the world encountered such cyber-attacks that have never taken place before. In an organizational and technological sense such a background could be observed which unambiguously demonstrated that organized crime, or the support of certain states supposedly provide a solid background through the media to the people and groups called hackers.

Previously isolated attacks could be observed, through which the method of the attacks could be detected more easily, and the extent of caused damages was significantly lower.

On the contrary, the tendencies of the past 1-2 years demonstrate that throughout the selection of the targets the hacker obviously intended to acquire great volume of financial or informational value. Their tools include self-developed codes to which the IT security systems of organizations do not provide sufficient protection.

Throughout the setup of the attack the human and application level factors are used contrary to the previously typical network and operational system level errors. The goal of this study is to present those IT security abuses which had the greatest impacts, the attack methods used throughout these abuses, to analyze the steps taken for protection and its deficiencies, and draw conclusions.

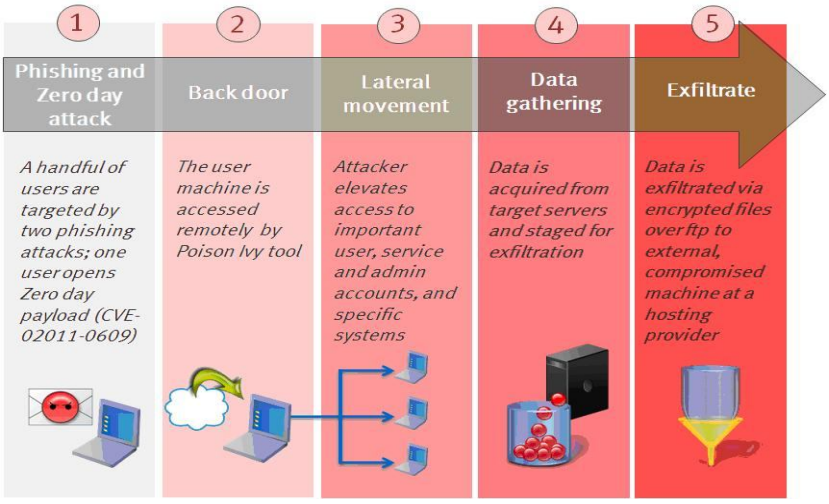
REVIEW OF ATTACKS

EMC/RSA token

The first significant attack took place against the RSA division of EMC. One of the most important products of this company is the synch and a-synch token which supports two-factor authentication. This product is used worldwide with maximum confidence. The goal of token usage is to eliminate weaknesses of passwords.

Supposedly the intruder intended to acquire the so-called "seeds" used on the tokens. In case of acquiring these seeds the secrets used throughout the token authentications become decipherable. [1] The success of the attack was acknowledged by the company at the end of March 2011 and communicated toward its clients „this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack." [2]

The essence of the methodological process of the attack is demonstrated in the following graphic:



1. figure. (Source: blogs.rsa.com)

EMC as a security company pays significant attention to its protection solutions, inspite of this it became a victim of a targeted attack. This called the attention of the IT field to the fact that expectedly aligned IT attacks can take place on significant targets.

Comodo authentication provider

Simultaneously the abuse on the system of an authentication provider called Comodo transpired. It turned out that such signature certificates can be generated in the system without authority which are accepted as authentic by significant operation systems and browsers. [3]

The real danger in this is that even a mischievous code can be sent to the user's computer and neither of the protection functions of the operation system alarms to it, since it considers it authentic. [4]

These acquired sets of information made it possible for the authentication process to be compromised throughout the target attack.

APT Attacks

The RSA referred to the fact in its announcement that it became a victim of a so-called Advanced Persistent Threat – APT. Throughout an APT a group potentially backed by state support launches a targeted attack against a significant target which generally has proper IT protection. The goal of the attack is to acquire information that represents directly or indirectly significant value to the group or to the organization behind them. The APT attacks include a wide range of extremely developed and precisely prepared IT penetration techniques and technologies, telephone and satellite surveillance methods. [5]

The acquired information was presumably used throughout internet espionage as the security incidents that can be related to some armaments industry firms in the USA and the affected IT systems of Lockheed Martin, L-3 and Northrop Grumman suggest. [6]

There is no exact information on the leaked data, just as well the method of the attacks is unknown, however according to some press and media organizations it can be linked to the attacks made on the systems of RSA and Comodo.

Sony PlayStationsystems

In this period the press also dealt a lot with the security incidents related to Sony networks which were made public continuously from April until June 2011, and it affected different types of systems. [7]

The series of attacks was directly prevented by the legal measures against George Hotz (geohot) who broke into the security system of Playstation 3 produced by Sony. This hack made it possible – after long years of useless efforts – that anybody after updating the special firmware of the system, copied game DVD-s could be used on the console. The series of attacks cannot be directly linked to this man, but the Anonymous group supported him during the trial, and later explicitly took responsibility for certain cyber-attacks against Sony. [8]

These apparently do not belong to the category of APT attacks. This can be based on the fact that the attacks were based on the weak IT security system of the firm, no special professional APT typical preparation was required, and based on the announcements and publications of the past few months the acquired information was not used, furthermore this information is not suitable for APT usage. Moreover apparently this could be a hacker activity.

Carbon-dioxide quota systems

In the first half of 2011 a series of abuses regarding carbon-dioxide quota trading in the EU were revealed. It was typical of the attacks that the quota trading systems were hit by targeted and organized attacks.

[10] Most of the abuses took place in 2010 and Austria, Denmark, Poland and Estonia were affected. 38 million dollars worth of carbon-dioxide quota was stolen from the Checz dealer. Throughout the attacks with the help of a keylogger that was sent to the operator administrator's computer, took over control of the trading system, and approximately during a 4 hour bomb alarm the illegal transactions were carried out. In December 2010 Denmark got wind warded by couple of billion dollars with a similar APT attack.

THE METHOD OF APT ATTACKS

An APT attack typically has 3 main phases

- *social engineering, spear phishing:* The main difference is in the well-organized social engineering type attack during the first phase compared to the hacker attacks used previously. A targeted, confidential person is chosen as a victim, whom they send a targeted mischievous code in a personal e-mail, which exploits the earlier unknown deficiency of a widely used boxed product. It is almost impossible to set up a protection against such an attack. This method is called spear phishing, targeted data exploration. [11]
- *zero day exploit:* The second phase is that through the running of the embedded - typically zero day – exploit, taking over control of the target's computer. Zero day exploit in many cases is based on the exploitation of a weeks or months long default, however the exploited default is not published, possibly the solution itself is not publicly available. In this case the exploit as a matter of fact is a backdoor program which enables remote access and control for the hacker through legally used firewall ports.
    - *staging attack–advancing to other systems within network:* The third phase of the attack is riskier for the hacker, since he has to occupy and attack other computers (possibly servers) through the occupied computer and within the internal network. However, based on the well prepared first phase (social engineering) the hacker might have the necessary information, thus knows the accessibilities, designations of the final, real target systems, since the acquisition of these through the used backdoor program is not necessarily a complicated hacking process.

      In case the hacker does not have sufficient information in order to advance within the internal network, and does not get busted within a short time for example by log analysing, DLP or other security systems, then he can deal with the third phase for a long time. It is typical of the internal security settings of the IT systems that they are more open to the internal usage and entrance, thus a well-chosentarget person's computer can be a guarantee for success. [12]

SUMMARY

Based on the attacks, abuses presented in the first chapter two attack types can be distinguished:

- APT hacker attacks
- hacktivism

The prevention of APT attacks is currently almost impossible due to the fact that it targets internal confidential people and due to the exploits which are specifically made for these attacks. The current preventive security systems are typically not suitable for beating off such attacks quickly and efficiently. Instead early detection needs to be emphasized, this can result in real solution.

The security of application development, the security elements of the applied development method, IT security courses in higher education can be the guarantee elements in decreasing the risks of such attacks.

The development of security awareness of IT operators, developers and users has to be the basic element of defence against social engineering and spear phishing, moreover the internet self-examination of companies, meaning what is available about them on the internet, what can be found by a simpler search on social websites about their IT systems and employees.

REFERENCES

[1] Art Coviello: Open Letter to RSA Customers, In: RSA website, (22 Mar.2011); http://www.rsa.com/node.aspx?id=3872

[2] Comodohacker: A message from Comodo Hacker, In: Pastebin, (26 Mar.2011), http://pastebin.com/74KXCaEZ

[3] DeclanMcCullagh: Comodo hack may reshape browser security, CNET, (04 Apr 2011), http://news.cnet.com/8301-31921_3-20050255-281.html

[4] Advanced Persistent Threat (13 May 2011), In: Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Advanced_Persistent_Threat (http://en.wikipedia.org/w/index.php?title=Advanced_Persistent_Threat&oldid=428898501)

[5] Kevin Poulsen: Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks(31 May 2011), In: Wired, http://www.wired.com/threatlevel/2011/05/l-3/

[6] PlayStation Network outage, In: Wikipedia, The Free Encyclopedia, downloaded: 20 Jun 2011, http://en.wikipedia.org/wiki/PlayStation_Network_outage (http://en.wikipedia.org/w/index.php?title=PlayStation_Network_outage&oldid=434632625)

[7] George Hotz Bibliographic in Wikipedia, The Free Encyclopedia, downloaded:20 Jun 2011, http://en.wikipedia.org/wiki/George_Hotz http://en.wikipedia.org/w/index.php?title=George_Hotz&oldid=437166342

[8] Anonymous Operation Sony in Wikipedia, The Free Encyclopedia, downloaded: 21 Jun 2011
http://www.youtube.com/watch?v=IpfK7ADqL1Q (21 Apr 2011)
http://en.wikipedia.org/wiki/Anonymous_%28group%29#Operation_Sony
(http://en.wikipedia.org/w/index.php?title=Anonymous_(group)&oldid=438148872)

[9] James Kanter: Emission Permits Theft Estimated at $37.7 Million (20 Jan 2011),In: The New York Times, downloaded: 20 Jun 2011
http://www.nytimes.com/2011/01/21/business/global/21carbon.html

[10] Uri Rivner: Anatomy of an Attack (01 Apr 211), In: Speaking and Security: The RSA blog and podcast, downloaded: 20 Jun 2011,
http://blogs.rsa.com/rivner/anatomy-of-an-attack/

[11] Microsoft: “What is spear phishing?”, In: Microsoft, downloaded: 20 Jun 2011
http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx

[12] PánczélZoltán and Buherátor: “Betörés megrendelésre” – Ordered Hacking, Silent Signal Ltd., Ethical Hacking Conference (12 May 2011)
http://tv.computerworld.hu/video/ethical-hacking-20114-betores-megrendelesre-8211-buherator-es-panczel-zoltan