HADMÉRNÖK

VII. Évfolyam 2. szám - 2012. június

Török Szilárd
totok.szilard@gmail.com

HUNGARIAN EXPERIENCES IN THE LIGHT OF CYBER ATTACKS IN 2011

Absztrakt/Abstract

2011 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.
Publikáció célja, hogy bemutassa a 2011-ben történt jelentősebb információbiztonsági eseményeken és a magyarországi etikus hack tapasztalatokon keresztül a biztonsági fenyegetéseket, ismertesse a sérülékenységek jellegét, majd ezekből kiindulva szakmai tanulságok levonására kerülhessen sor.

In my evaluation analysis I would like to present the published definition and regulation background of Critical Information Infrastructure and its possible cyber protection methods. Based on the public IT security incidents of year 2011, the extent 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 the IT security threats, the characteristics of vulnerability of the significant IT security events and Hungarian ethical hacking experiences taken place in year 2011, and these events may serve as a tool to summarize professional conclusions.

Kulcsszavak/Keywords: *kritikus információs infrastruktúra, APT, hacktivista, veszélyek, SCADA ~ critical information infrastructure, APT, hacktivist, threats, SCADA*

INTRODUCTION

In the last fifteen years the modern state as well its organisations and citizens became defenceless to computers and Internet and to diverse technological applications running on local or remote computers.

We realize the dependence on computers and mobile devices in our everyday life primarily regarding work and Internet usage. As a result, our life seems inconceivable without these devices. We store data necessary for our operation and in certain aspect we store confidential information in our computer and mobile devices.

It is fundamentally expected that these systems and thus every critical information infrastructure should be armed with the appropriate protection systems against terrorist acts or attacks and cyber attacks. The minimum expectation regarding these systems is that the operation and structure of the systems should not include at least the trivial security errors – e.g. allowing wrong password choice, the basic installation of web applications and access to their files, etc. Furthermore, following the installation of new applications and systems these errors should be filtered out of the developments through simple checks.

The establishment and development of a secure system results in more work for the operator and the developer, but it is not proportionate to the eliminated damages. The critical issue is the security awareness of the shareholders and the management in private or public companies/organisations, they should feel responsible for the stability and reliability of their own information system.

The above-mentioned security risks do not necessarily derive from the operation systems, and to be able to find the errors, the operator does not need general software testing or simple scanner programs. The security risks should be basically seeked in the development of the software; it depends on the developer environment and the planning strategy, moreover on the information security awareness and the proficiency of the program developers participating in the implementation.

Around 2010 this tendency intensified, meanwhile previously the general and widespread operation system errors, application and network device installations caused the majority of the problems.

The current issue of our age is whether to what extent the complex information systems in Hungary – and thus the Critical Information Infrastructures themselves – are able to defend themselves relying on their current IT devices, their thought-out alarm systems, and their effective regulations. The fundament of this issue is that the most important scene of modern warfare is the cyberspace itself, and the critical information infrastructures operating in it.

INTERNATIONAL CYBER ATTACK TENDENCIES

The tendencies of the attacks will be approached by introducing several outstanding international cyber attacks in 2011: what were the targets and what were the typical methods of implementation. Besides the types of their inorganization it is important to notice the hidden political and economic intentions and the providence of the necessary resources for the given attack.

EMC/RSA token

At the beginning of 2011 a serious cyber attack took place against the RSA division of the company called EMC, the attack was admitted by the company in the end of March 2011. [1] The company is well known for its synchronic and asynchrony token supporting two factor authentication. The basis of its popularity is that it is used all over the world with maximum confidence, and the goal of its usage is to eliminate the weaknesses of passwords.

According to audits, the attack as a first step started with phising based on zero day exploit through e-mails, in other words with data mining. Thus remote access is gained in the target system, eg. „by installing Poison Ivy tool", then the intruder tries to explore the significant services, administrational surfaces and special systems within the system. Following the collection of data from the victimized server, the data is exported in encrypted files eg. through external FTP connections. [2]

This cyber attack method is also called APT (Advanced Persistent Threat) [3], it has three main typical phases:

1. social engineering, spear phising
2. zero day exploit [1]
3. staging attack - access to other systems within the network

In the specific case, the attack was directed towards acquiring the so-called „seeds" used in the token. The primary goal of the attack was to decrypt the secrets used during token authentications. [4]

Attacks against authentication providers

Almost parallel an abuse took place in the system of a well-known authentication certification provider. Signature certificates could be generated in the system without authorization. The benefit for the intruders was that the generated certificates were accepted as authentic by the significant operation systems and browsers. A perfect example for such a cyber attack can be the victimized Comodo authentication provider. [5]

Assumable, there was a short period of time between the above explained token abuse and counterfeiting the authentication certification service according to the communication of the companies regarding admitting the attack. The real danger in combining the two techniques is that following the „weakening" of passwords with the fakely generated verification of the authentication certification service it is easy to embed a harmful code in the systems, or in the computer of the user in a way that it is not detected by neither of the protection functions of the operation system.

EU carbon-dioxide quota system

In 2011 it was revealed that the Carbon-dioxide quota trade systems of the EU member states did not possess the necessary security systems, which would be proportionate to the frequency of transactions flowing through the system. It was typical of certain part of the attacks that targeted and organized attacks hit the systems providing quota trade. Austria, Denmark, Poland and Estonia were definitely involved in the attacks. [6]

The attribute of the attacks was also APT attack. Unfortunately they can be considered so „successful" that the intruders could steal $ 38 million worth of carbon-dioxide quota from the Czech dealer. Throughout the attacks control was taken over the trade system by sending a targeted keylogger to the computer of the operator administrator, and implemented illegal trade during an approximately 4 hour-long bomb drill.

Even a greater attack and loss took place within the EU: for example in Denmark where several billions of dollars were stolen. [7]

Duqu / Stuxnet

In 2010 the protection against viruses, trojans and other virulent programs reached a new milestone when a new trojan was discovered that was named Stuxnet. Not only was its

[1] Zero-day/zero-hour expression is used by experts for those computer security threats which exploit the unexplored, non-published vulnerability of a given computer application. There is no protection method against it (not even in an endpoint and network aspect), furthermore it represents a significant value to its developer, since all the computers/networks carrying this error will be accessible for him.

specialty that only spread in Microsoft operation systems, but also it was developed exclusively against SCADA systems.

Stuxnet could execute the reprogramming of automatic processes within SCADA systems, it attacks PLC2 software, and primarily targeted WinCC/Step 7 software. The real specialty of the program is that it searches industrial devices, namely frequency transformators of high velocity engines, and it only activates itself in case of those devices, which are involved almost exclusively in uranium enrichment. As a matter of fact, the eventual goal of the program is to cause failure in the uranium enrichment centrifuges, and distract uranium enrichment. [8]

In order to prepare the code, lots of internal information related to the targeted devices was needed. [9] Both the NATO and Russia could have interests related to the implementation of the attack. [10]

In September 2011 another virulent program became known: it was named DuQu (due to the created files starting with ~DQ). This discovery is linked to the team working in the CrySyS Data and System Security lab operating in the Department of Telecommunications at the Budapest University of Technology and Economics.

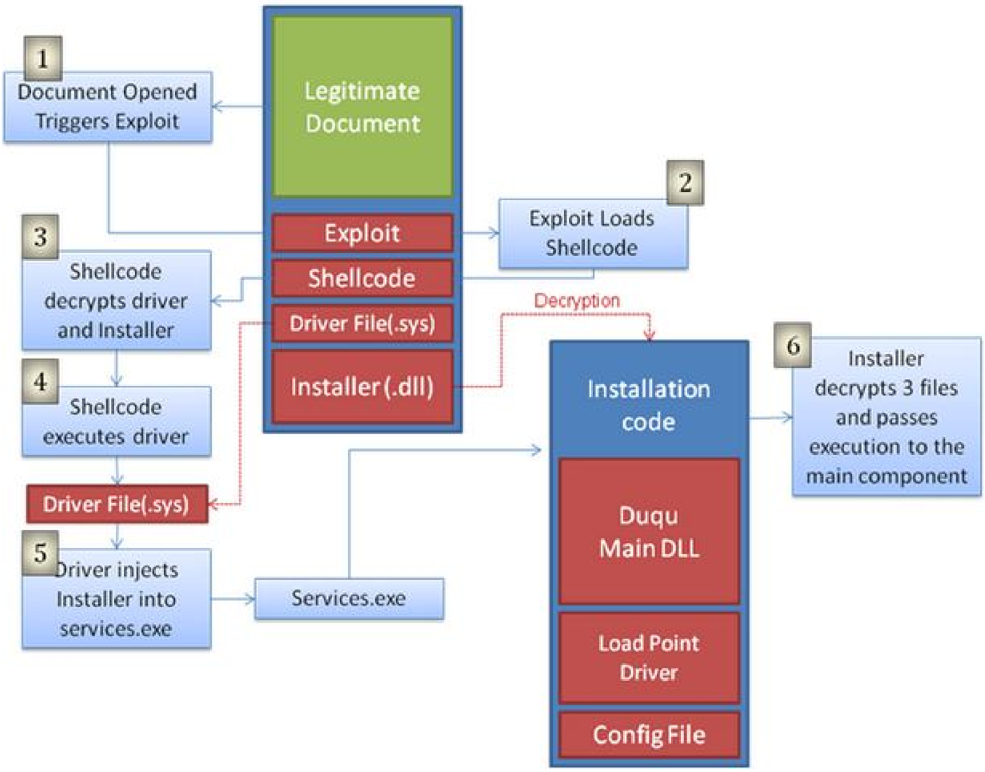
Although in those days Stuxnet could not be completely solved, the new mischievous program shows a lot of similarities to Stuxnet. Based on analyses, the creators of DuQu accessed the source code of Stuxnet, but the fact cannot be excluded that both programs were developed by them. [11]

However it is important to emphasize that the two softwares hardly have anything to do with each other: DuQu is a trojan enabling remote access, does not spread, does not use exploits to widen its latitude, and its goal is not to modify SCADA systems, but to leak information about the attacked system.

DuQu can be an example that the new mischievous programs, created by professional experts, were not detected by neither of the Anti-Virus applications. Although the Anti-Virus market reacted quickly, four new viruses were discovered in the following 48 hours.

It loads itself as a kernel driver when booting the computer; it tries to inject itself into the two most widespread browsers and into the process of the explorer exe, which is the basis of Windows. Following the successful injection none of the popular anti virus will detect it.

DuQu is also an important element related to certificate counterfeiting, since – following its predecessor – it uses valid, but stolen certificate: it has more kinds of fake driver programmes, among others the digital signature of JMINET7.SYS 2.1.0.14 kernel-mode Windows driver programme, thus it enables itself to install undetected viruses or trojans. [12]



1
Document Opened Triggers Exploit
Legitimate Document
Exploit
Shellcode
Driver File(.sys)
Installer(.dll)
2
Exploit Loads Shellcode
Decryption
3
Shellcode decrypts driver and Installer
4
Shellcode executes driver
Driver File(.sys)
5
Driver injects Installer into services.exe
Services.exe
Installation code
Duqu Main DLL
Load Point Driver
Config File
6
Installer decrypts 3 files and passes execution to the main component

1. figure. Duqu [13]

DOMESTIC EXPERIENCE

Based on the hack experiences in Hungary in 2011 the domestic security awareness and cyber protection level and accessibility of several Critical Information Infrastructure can be overviewed.

It is typical of the audits that they were executed with minimal information, so these were black box controls. Only the IP address of computers/servers to be audited was known, no other information was previously available about the systems and settings.

The tested systems all comply with the definition of domestic Critical Information Infrastructure.

The name of the audited companies and their systems are not disclosed due to confidentiality obligations and national security reasons, the audit methods and the types of revealed errors and conclusions are all public. Furthermore, the specific errors were corrected in the meantime, it does not imply danger to anyone in any other way.

National system

During the audit it took less than 3 days to take over 25 servers and to acquire Domain administrator authorization in some related systems

- seized servers: systems managing backups, databases, firewalls, web servers
- Taking over Windows Domain Controller, and Domain administrator authorized user was created
- digital signatures could be generated, the credibility of the service was damaged in its fundamentals

Health care/hospital

During the black-box testing basic configuration errors were revealed on more servers, which expose the data and information to potential danger. It has to be emphasized that no outstanding IT knowledge is required to exploit these errors. The applied passwords are very weak (3-6 characters), the system administrators' passwords could be decoded in a couple of minutes.

System administrator authorisations could be obtained in more servers within a short amount of time. At the beginning of the audit many systems froze down due to the effect of a basic port scanner, which was caused by the improper updating of the operation system.

On more database servers the database administrator was not given a password or the user name was the same. On more database servers on behalf of the database administrator it is possible to run a system administrator order on the given computers thus compromising the given server or other computers of the network if the shared passwords are applied. The passwords of SQL databases are easy to obtain or to reveal, since they do not operate with proper settings.

Companies owned by Capital City, Budapest

During the audit of external website several serious security errors and setting problems were identified, which made the access possible to the internal, closed network and managed to obtain a Domain Administrator authorization in the internal network.

- One third of the users' password managed in the system could be decoded within four hours
- typically less than 2 days were necessary to acquire Domain Administrator authorization in the internal network
- during the audits the critical systems of the companies could be accessed, including SCADA systems. This involves huge risks, since a professional intruder can take control over a SCADA system and would have the opportunity to stop the service, shut down or ruin the system or the supply of consumers
- typically, the internal attacks could be successfully repeated from the rooms which were separated in an IT and network sense (meeting rooms)

Systems related to transport

During the external audit serious security errors were identified on website. Through these errors the following could be accessed:

- the database of the website
- partner data
- ticket ordering (with the highest authorization)

Furthermore, during the internal audit administrator authorization could be acquired on almost 20 virtual and real servers within 1 day.

Complex Trading System

During the audit of the trading system 7 problems with outstandingly high risk were identified, from which several were so serious that they would have made system inefficient for any kind of trading.

- it was possible to modify the main page in a way that the intruder can access the trading items of any entering user, and can execute any kind of operation on behalf of the user while the user is not being aware of the fact
- it was possible to carry out transfers from one account to another with one arbitrary user while the user is not being aware of the fact
- it was possible to enter the user multiple times
- it was possible to modify the user having only reading authorisation to a complete authorisation user

- the system administrators operating the server had minimal security knowledge, furthermore the settings of the server only complied with the settings of a system used in an internal, development environment, not an activated and critical system

Financial system

The examined system ensures the IT system of some 30 financial systems in form of outsourcing

The most important problems from the identified high risk security problems:

- it was possible to take over a website providing minimal service with an SQL injection [14] attack following a PHP [15] shell [16] upload (it was possible to create an interactive shell)
- on the taken over server the certification and settings necessary for the VPN access of the internal network could be found in the folder left behind by the system administrator over a year ago
- typically the same passwords and settings were used on virtual servers
- due to the identical and defective SSH settings, the source codes of the softwares running on the servers of the financial service provider were accessible

SUMMARY

Based on the overviewed international tendencies and experiences of domestic information security audits, it can be concluded that the planners of the attacks strive for even more professional implementation; they execute their cyber operations with complex and detailed methods. Even certain steps of the attacks include unique developments and solutions. Paralell can be drawn among more attacks, which can indicate political, economic or military interest.

Based on the experience gained in the same year it can be concluded that our domestic cyber protection preparedness is not even appropriate against medium level trained information security experts.

During the execution of the security audits and studies the most typical IT security risks and related errors were the following:

1. Typically the critical systems were accessible from every location – weak or faulty separation
2. The services available on the servers, which can be accessed through the internet are often vulnerable to so called „SQL injection" attacks – typically no ethical hack audit took place, neither source code audit
3. Through the servers taken over during external audits, the majority of the systems operating within the internal network typically became exposable to attacks – faulty settings, data and passwords forgotten on the external server, usage of identical and weak passwords and settings in the internal network
4. Acquiring administrator authoriazation on domain type networks and/or taking over the domain controller within a short period of time (maximum 1-2 days) is possible – network and authorization structure have no concept, faulty settings
5. Security errors published years ago can be also exploited – lack of IT security control

The domestic errors – according to own experiences – are based on the fact that responsible managers improperly think that their systems are safe. Meanwhile, they do not carry out annual or other frequent IT related audits on their systems. With the security loopholes in their IT systems, in case of an attack personal data – sometimes digitalized signatures, contracts, etc.- and business data can be easily and quickly acquired.

Security issues are not only left out of consideration during security controls, but during developments and planning, thus sometimes fundamentally – security wise – faulty systems are created. It can occur that only the complete redesign and redevelopment of the software can be the secure solution to eliminate security errors.

In case an attack similar to the ones carried out in international attacks would be executed against Hungary, assumably we would be in a very vulnerable situation. The sufficient security awareness and technical preparedness of the operators is not typical, and security issues are ignored during developments, on decision making levels the IT risks are assumably not seen and realized. At the same time the situation of managers and decison makers is even more difficult, since the quality of IT security audits can show quite a difference.

In the past few years during IT security audits websites were successfully attacked and taken over (through fundamental errors) which had the certifications of the biggest auditor companies. It would be practical to define general ethical hack audit regulation levels and descriptions. A possible approach for the levels is the following:

- minimal audit – running automatic devices
- medium audit – automatic devices and manual control
- complex audit – automatic devices, manual control and creation of unique attacks

References:

[1] Art Coviello: *Open Letter to RSA Customers*, RSA, download: 30 November 2011, http://www.rsa.com/node.aspx?id=3872

[2] Uri Rivner: *Anatomy of an Attack*, RSA Blog, download: 20 December 2011, http://blogs.rsa.com/rivner/anatomy-of-an-attack/

[3] Advanced Persistent Threat (13 May 2011), In: Wikipedia, The Free Encyclopedia, download: 20 December 2011, http://en.wikipedia.org/wiki/Advanced_Persistent_Threat http://en.wikipedia.org/w/index.php?title=Advanced_Persistent_Threat&oldid=428898501

[4] Mark Diodati: *The Seed and The Damage Done: RSA SecurID* (02 Jun 2011), In: Gartner Blog, download: 20 December 2011 http://blogs.gartner.com/mark-diodati/2011/06/02/the-seed-and-the-damage-done-rsa-securid/

[5] DeclanMcCullagh: *Comodo hack may reshape browser security*, CNET, download: 20 December 2011, http://news.cnet.com/8301-31921_3-20050255-281.html

[6] „Carbon Criminals" - The international trading of carbon emission permits, Osztrák Parlament Szenátusi Bizottsága, p.12-15. download: 20 December 2011, http://www.aph.gov.au/senate/committee/scrutinynewtaxes_ctte/carbontax/report/c03.pdf

[7] James Kanter: *Emission Permits Theft Estimated at $37.7 Million*,In: The New York Times, download: 20 December 2011, http://www.nytimes.com/2011/01/21/business/global/21carbon.html

[8] Berzsenyi Dániel, Szentgáli Gergely: *STUXNET: a virtuális háború hajnala*, download: 20 December 2011, http://www.biztonsagpolitika.hu/index.php?id=16&aid=932

[9] Gállfy Csaba: *Budapesti csapat találta meg a Stuxnet utódját*, download: 20 December 2011, http://www.hwsw.hu/hirek/47582/duqu-crysys-biztonsag-stuxnet-bme-muszaki-egyetem-symantec.html

[10] Panayotis A. Yannakogeorgos: *Was Russia Behind Stuxnet?* download: 20 December 2011, http://the-diplomat.com/2011/12/10/was-russia-behind-stuxnet/?all=true

[11] Cserháti András: *A Stuxnet vírus és az iráni atomprogram*, Nukleon IV. évfolyam 1. szám Budapest, Marc 2011, p.:85, ISSN 1789-9613

[12] Alexander Gostev: *The Mystery of Duqu: Part One* (20 October 2011), Kaspersky Lab, download: 20 December 2011 http://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One

[13] Duqu (03 January 2012), In: Wikipedia, The Free Encyclopedia, download: 06 January 2012, http://en.wikipedia.org/w/index.php?title=Duqu&oldid=469383972

[14] SQL Injection (02 April 2012), In: Wikipedia, The Free Encyclopedia, download: 02 April 2012, http://en.wikipedia.org/w/index.php?title=SQL_injection&oldid=488517068

[15] PHP (02 April 2012), In: Wikipedia, The Free Encyclopedia, download: 02 April 2012, http://en.wikipedia.org/w/index.php?title=PHP&oldid=488393047

[16] PHP (02 April 2012), In: Wikipedia, The Free Encyclopedia, download: 02 April 2012, http://en.wikipedia.org/w/index.php?title=Shell_%28computing%29&oldid=485757335