CURRENT APPROACHES TO INCREASED PROTECTION AGAINST TROJAN HORSES IN CLOUD SERVER SOLUTIONS

Peter Veselý,[1] Michal Greguš,[2] Eleonóra Beňová[3]

Abstract: IT companies are presenting to their customers cloud computing as a technology that will give them a competitive advantage if they implement it faster than their competitors. It is true that cloud computing can improve the businesses capability to access, share, and protect their company's data, particularly when they have a limited capacity to manage on-site modern technology resources. Using cloud services or simply only thinking of moving data to the cloud creates a wide set of concerns, starting with basic security concerns, and going as far as to the availability of cloud services, that is the company would not be able to get to the data when it needs it. Small and medium companies do not have enough resources to fight cyberattacks, but they can implement policies that will minimize the risk of the loss of their valuable data. The aim of this paper is to describe the current threats companies are facing when they use cloud services and to give them advice how to minimize the risk of these threats. We will specify a set of rules especially for small and medium companies and organizations that should help them to be able to choose more secure cloud services for their particular needs.

UDC Classification: 004.49; **DOI:** http://dx.doi.org/10.12955/cbup.v5.1076

Keywords: cloud, security, Trojan horses, 0-day, hack

Introduction

Every day we use the connection to a cloud server. A large proportion of people do not even know, that they are connected to cloud server solutions. And not considering this, they use any functions of standard computers or smartphones (Davidekova, 2016). Companies are increasingly switching to cloud server solutions and implement various services to their corporate infrastructure. The threat of a cyber-attack does not surface until they become a victim (Kumar, 2017). The use of cloud server solutions brings many benefits but also a large number of new security risks. The whole world is currently in a great cyber war and it is only a matter of time before we become a target (Wenli, 2015). However, the primary targets shift towards cloud infrastructure and services based on cloud server solutions, where there are many users, a lot of data traffic, and personal data (Somani et al., 2017). There is currently a number of documented Trojan Horses, which are likely formed by state governments for the purpose of entering foreign computer systems to damage them, or more likely, in order to be used for a massive data collection. Cyber-attacks have evolved from simple ones to sophisticated and devastating Advanced Persistent Threats (Redondo-Hernandez et al., 2015), such as the Stuxnet attack was (Farwell and Rohozinski, 2011). These threats have the capabilities to stop business operations and even cause physical damage (Bajramovic and Gupta, 2017). Effective IS/IT security must ensure an adequate level of confidentiality, integrity, availability, authenticity and nonrepudiation (Karovic et al., 2015).

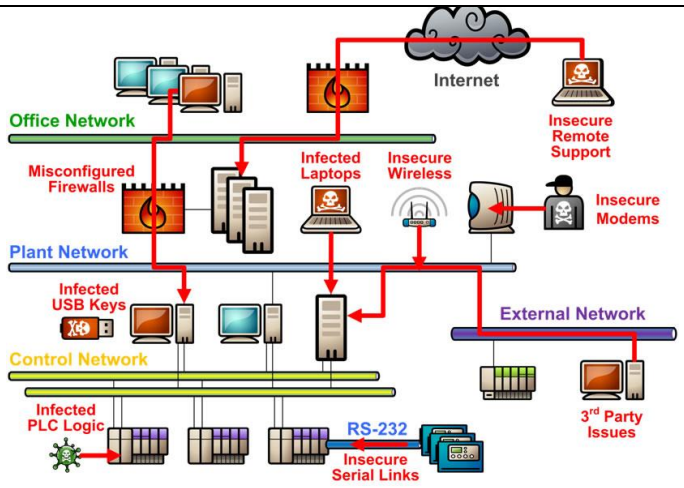
Stuxnet

The super virus Stuxnet is considered the first virus developed by intelligence services to track other countries or to damage the technologies of other countries. It is estimated, that more than 100,000 computers were infected by Stuxnet. The main goal, however, was initially only one target, the Natanz enrichment facilities in Iran. This is generally considered to be the first strike in the global cyber war. According to the reports, diaries and subsequent analysis of a number of authors like Fiaidhi and Gelogo (2012), Byres (2016), or Kenney (2015) including ESET, a leader in antivirus solutions, it is clear that the development of Stuxnet could be contributed to US intelligence agencies, the NSA and an Israeli military unit known as UNIT 8200. The virus itself was a relatively sophisticated solution that contested alone the core of the Windows operating system using a 0-day exploit. At the same time, it was a cross-platform solution, which after analysis of the virus infecting other systems, especially the Siemens PLC systems, where a firmware upload in particular centrifuges, which then changed parameters to lead to their physical destruction. A comprehensive solution indicates, that the virus itself must constitute more people versed in multiple systems. The biggest threat is currently

[1] Faculty of Management, Comenius University in Bratislava, peter.vesely@fm.uniba.sk
[2] Faculty of Management, Comenius University in Bratislava, michal.gregusml@fm.uniba.sk
[3] Faculty of Management, Comenius University in Bratislava, eleonora.benova@fm.uniba.sk

using a 0-day exploit Windows operating systems. The use of these errors means that the virus conceals itself perfectly and had existed several years before it was discovered

Figure 1: Possible ways to infect system with Stuxnet



Source: Byres (2016)

The technology is relatively simple, based on the recognition that the target group uses Windows in several versions and these versions are called 0-day bugs, errors which have not yet been discovered, not even by the manufacturer of the operating system. In the world, there are several companies that specialize in finding just those errors and sell them to governments. For example, a company VUPEN according to Forbes magazine in November 2011, received the amount of 250 000 USD for the supply of information on software vulnerabilities from the US government (Bohdalova and Kurdyova, 2013). Stuxnet itself according to the version contains an analysis of approximately 15,000 lines of code that is written quite sophistically and includes a section for introducing a different code to the PLC equipment.

Duqu and Flame

The new super virus Duqu and Flame are successors to Trojan horses produced by state organizations. Trojan Duqu is able by means of false digital signature certificate update the system by running the document to take control of the Windows kernel. Duqu is able to thereby change the computer to a botnet zombie. To function it is sufficient to have only about 3000 lines of code, unlike Stuxnet which depends on libraries having a size of approximately 20 megabytes. Already there is a visible shift from a pure Trojan horse technology, that is Duqu and Flame is a mixture of worms and Trojan virus and relies on the use of libraries of the Windows operating system itself. The Trojan Horse Flame collects information not only on the computer's local network but due to undocumented bugs in Bluetooth, also collects data from mobile devices (BYOD abuse). Then it sends the information on to more than eighty servers. When analyzing these sites with Symantec, there has been issued a statement, which the efforts and plans to create Duqu and Flame requires government approval. It also proves the track of the eighty servers registered to cover German and Austrian companies around the world. Based on Flame there were created several generations of Ransomware viruses that also exist today and commit great damage in cybersecurity. Creating a Windows protection against the types of attacks such as the Duqu and Flame took a few weeks for Microsoft programmers. In doing so, they had to change part of the core system, in particular authentication and encryption of the core system, so that the 0-day exploits did not continue to abuse it.

FinFisher

The FinFisher software was sold legally by company Gamma International Ltd. worldwide to governments. For example, according to available information, Slovakia has purchased 49 licenses, which is more than Hungary. According to published information, there are several versions of FinFisher according to the degree of difficulty in the implementation of the target system. Malware/Trojan horse then actively analyses all available documents and databases, and extensive data is sent to the attacker. FinFisher is also known to actively exploit a security loophole in the

iTunes system for spreading itself. It took three years, until Apple has resolved the issue of its services - operated by its private cloud iTunes. In addition, a frequently used masking technique is used to attack Mozilla Firefox. Gamma had created an espionage program that was entitled Firefox.exe and even provided a version number and trademark claims that appear to be a legitimate Firefox software. Currently it is very difficult for detection since the algorithm is constantly changing as well as techniques for masking the Trojan Horse FinFisher.

Future Trojan Horses and Other Cracking Tools

It would be naive to think that after the success of Stuxnet, Duqu and Flame, the creators decided not to continue further in their development. At present, intensive work in the legal sphere of cross platform security and privacy is needed, since various solutions that seek to decrease vulnerability, e.g. Microsoft.NET, are being implemented for all operating systems. For policy makers that means the possibility of a smooth entry into the system. However, the authors of the operating system try to improve the security of the operating system core. For example, Ubuntu has agreed with Microsoft to implement running Bash on Ubuntu on Windows.

It is assumed that at the moment different versions of Trojan Horses are being tested and that the new version of Stuxnet, Flame and Duqu are already in circulation and are detectable.

Infection Storm with Locky

A new kind of infection ran like a chain reaction across the globe. Abused to distributing the 4th most popular operating system in the world - Linux Mint, combined with the most widespread misuse of the web applications from WordPress. The attackers have changed the distribution from the 20.2.2016 to their own for several distribution servers. As a result, over 20 million distributions of Linux Mint began to spread the ransomware Locky. It is estimated that over 2 days Locky infected over 250 million computers. Its sophisticated code first deletes all kinds of backups on disk, including shadow copies of Windows and then scans all drives attached external drives as well as any local network connection. Then it crypts in a quite sophisticated way (Davidekova and Farkas, 2014) individual files, and demanded 0.5 per Bitcoin ransom per file.

Figure 2: Official warning in Germany

Source: Author

Using Cloud Server Solutions

Currently, cloud solutions is based on several projects such as OwnCloud, or OpenStack Zential. There are other solutions, but number of these solutions lead to large multinational companies. In addition, the functioning of the cloud server solutions rely upon e-Government solutions in world.

Cloud Server Protection

One of the possibilities of protection is the consistent prevention of security incidents, the consistent application of antiviral agents, keeping and updating the list of installed programs. However, in the cases described above, such prevention is meaningless. An attacker familiar with the company's internal affairs enforces and infects the standard security measures. In addition, standard antivirus solutions recognize only the threats that already have been analyzed, despite the fact that they dare to try to do a heuristic analysis.

The second option is a consistent cataloging of each file in the system with consistent hardware and software tracking. In practice, there are few systems for monitoring complex information systems, but they are mostly based on Windows technology. This means in practice that most of the hybrid networks can be controlled and protected. But not the whole hybrid network. Comprehensive cataloging of hardware and software on the corporate network should be able to check up and control the security of complex IS/IT, including BYOD. In fact, each file would be analyzed, compared to the file catalog of existing systems, and if a system kernel file would differ, the file would be refused to be copied down or it would be evaluated in detail as a threat. Currently, for example, Linux editions have a completely described file system, including the CRC checksum for system checking. The only exploitable weakness would be that the state starts publishing its own editions of operating systems that will have cataloged files in the part of the system, so the comparison will go well, but it will actually pose a security risk.The third option is to use other operating systems that are different from Windows. For example, there exist many variations of the system Linux as is documented by Karovic (2013), a vivid example is Scientific Linux that is used by scientists at CERN laboratories. Or the existence of Linux Ubuntu Kylin, which is approved by the Chinese government, and the standard version of Ubuntu is for example recommended by the UK Government as a safe one. The problem of the cloud solution however, is that there are currently several cloud server solutions based on only a few operating systems. So, the attacker only needs the knowledge of the given operating system, and basically the attacker does not have to deal with the other operating systems to get into a specific cloud server solution.

Conclusions

Currently as is documented especially by Lifars (2017), the development of super viruses and Trojan Horses is progressing faster than we are willing to admit. Individual countries are investing hundreds of millions in development, and over 150 states are developing solutions to protect against intruders from the internet. The war in cyberspace has already begun, and the protection against is becoming increasingly difficult and costly. Paradoxically the most efficient solutions now - cloud server solutions - are currently in the position as the most vulnerable ones because they are often the primary aim of attackers and use only a narrow set of solutions for their operation.

References

Bajramovic E. & Gupta D. (2017). Providing security assurance in line with national DBT assumptions. AIP Conference Proceedings 1799, 050005 (2017); doi: 10.1063/1.4972939

Bohdalova M. & Kurdyova E. (2013). Dataminingova analyza na priklade jazykovej agentury. Forum Statisticum Slovacum, 9 (5), 3-9.

Byres E. (2016). Using Tofino™ to control the spread of Stuxnet Malware, MTL Network security, AN-Byres 119, rev 2, Eaton 2016. https://www.mtl-inst.com/images/uploads/AN-BYRES119_Rev_2.pdf

Davidekova M., & Farkas P. (2014). On the Cross-Correlation Properties of Complete Complementary Codes of Different Families (N, N, N2) and (N, N, N). In Proceedings of International Scientific Conference for Ph. D. students of EU countries, Comparative European Research, LONDON. 2014, 117-120.

Davidekova, M. (2016) Digitalization of Society: Smartphone–a Threat. In: 8th International Research Conference Management Challenges in the 21st Century: Digitalization of the Society, Economy and Market: Current Issues and Challenges. 2016. 314-320.

Farwell J. P. & Rohozinski R. (2011). Stuxnet and the future of cyber war, *Survival, 53*(1), 23-40.

Fiaidhi, J. & Gelogo, Y. E. (2012) SCADA Cyber Attacks and Security Vulnerabilities: Review, ACN, Advanced Science and Technology Letters, SERSC 14(2012), 202-208.

Karovic V. (2013). Linux, Digital Science Magazine 2 (4) 10, http://digitalmag.sk/linux/

Karovic V., Drahosova M., Karovic V.ml. (2015). Information security. CER Comparative European research 2015: The fourth International Scientific Conference for PhD students of EU countries, vol. 2, London: Sciemcee publishing, 2015, 134-137, http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf

Kenney M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis, 59(1),* 111–128

Kumar M. (2017). Cyber Warfare: New Dimension in Security and Strategy. Available at SSRN: https://ssrn.com/abstract=2915653 or http://dx.doi.org/10.2139/ssrn.2915653

Lifars (2017). The Importance of a Corporate Culture Built Around Security (2017). Retrieved April 27, 2017 from LIFARS LLC. https://lifars.com/2017/04/importance-corporate-culture-built-around-security/

Redondo-Hernandez A., Couce-Vieira A. & Houmb S.H. (2015). Detection of Advanced Persistent Threats Using System and Attack Intelligence, Emerging 2015: The Seventh International Conference on Emerging Networks and Systems Intelligence, IARIA, 2015. 90-94.

Somani G, Singh M., Sanghi D., Buyya R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30-48, https://doi.org/10.1016/j.comcom.2017.03.010,Wenli S. (2015). Study on the Vulnerability Analysis Method for Industrial Embedded Devices. *Automation Instrument, 36,* (10), 63-67.