2016/January

COMMENTARY

Cybercrime- A growing threat for Macedonia

www.analyticamk.org

The world has never been more interconnected than it is today. For all of the advantages that this interconnectivity brings, there are also new threats that arise. One of these threats that have been taking over the news headlines and growing in size is cyber threats.

As humankind becomes more reliant on technology, we also become more exposed to cyberattacks. Each one of us while doing our daily activities such as using social media, sending e-mails, checking our bank statements, and other activities that are increasingly carried out online, we are sending out sensitive information which in the wrong hands can be very costly to us. Criminals can steal one's bank credentials, abuse people's private information or simply damage their technological devices. Law enforcement agencies are trying to combat this growing problem, but more and more people are becoming victims of cyber criminals.

Any crime committed through the Internet is defined as cyber crime. There are many types of cyber crimes with the most common being the following: **Hacking**, where the criminal uses a computer to gain unauthorized access to a system, **Phishing**, where criminals impersonate a business to trick people into giving out their personal information, **Identity Theft** ,where criminals use a person's sensitive information for their own financial benefit, and **Malicious Software**, which is harmful software that corrupts and destroys data that is sent out by cyber criminals in the form of a download that is meant to trick victims"[1].

McAfee Intel Security (a global computer security software company), in their report "Net Losses: Estimating the Global Cost of Cybercrime" estimates that the likely annual cost to the global economy from cybercrime is more than 400 billion USD. They also estimate that cybercrime has a negative effect on employment in developed countries."[2]

The forecast is that the cost of cybercrime will continue to increase in the future due to more and more businesses starting to work online, which has seen rapid growth in the developing world. One of the reasons why cyber crime is growing is due to the fact that it encourages attacks and makes it hard to defend. Criminals tend to get high returns at low cost, and the risks are lower. Compared to traditional crime, chances are smaller for offenders to get caught, and if caught they do not face as much prison time. Cybercriminals are also often located internationally, and the process of tracing them and extradition tend to be quite difficult. These traits make cyber crime a very attractive form of crime.

The Republic of Macedonia also faces the challenges from this sophisticated form of crime. In order to better combat this phenomena, Macedonia adopted the law for Ratification of the Convention for Cyber Crimes.[3] Macedonia has also ratified an Additional Protocol to the Convention on Cybercrime, which criminalizes racist and xenophobic acts committed in the cyber realm[4]. The incorporation of the convention into Macedonia's legal framework enables better international cooperation and the ability to adapt adequately to any new form of cyber crime. Article 251 from the Criminal Code sentences criminals up to three years in prison for unauthorized access to computer systems in order to gain a certain financial benefit for themselves or others[5]. Ministry of Interior (MOI) also has a special unit in charge of tracking cyber crime.

Due to its low cost and high benefits, combined with the easiness to conduct it, cyber crime has been on the rise in the Republic of Macedonia. According to data from the MOI, in 2013 there were 100 cyber-crimes committed in Macedonia, which is twice as much as the previous year. According to reports several companies in Macedonia have been scammed through the process of phishing, and the damage to the Macedonian economy has been in the hundreds of thousands (EUR).[6] One can expect this number to

1 The Windows Club. Types of Cybercrime Acts and Preventive Measures http://www.thewindowsclub.com/types-cyber-crime

2 Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. June 2014 http://www.mcafee.com/jp/resources/reports/rp-economic-impact-cybercrime2.pdf

3 Law for Ratification of Convention for Cybercrime, 24.06.2004 http://www.pravo.org.mk/documentDetail.php?id=5616

4 "Macedonian path towards cyber security". Predrag Tasevski. Information and Security: An International Journal, vol.32, 2015 http://procon.bg/system/files/3204_macedonia.pdf

5 Official gazette of the Republic of Macedonia 37/1996

6 Robert Mitevski. "Во сајбер-пеколот изгореа десетици македонски фирми (Dozens of Macedo-

rise as more and more businesses move to the cyber realm, and more citizens use the internet for online shopping.

In order to find out more about how cybercriminals operate and how easy it is to be a cyber criminal I looked at a forum where criminals of all levels of experience can find useful instructions on how to perform their criminal activities[7]. The forum also serves as a platform for the exchanging and selling of stolen data. Here, criminals can purchase stolen credit cards; stolen PayPal accounts, and acquire services from hackers (crackers). The reason why I decided to look more closely at this particular forum is the fact that there seems to be a dozen or so members from the Balkan region. These individuals are usually active in a sub-forum for people from ex-Yugoslavia. They work with each other on acquiring stolen data and using it to cash out. Many of them are still relatively new and inexperienced at what they are doing, but they seem to be eager to learn. They use ICQ (an instant messaging program popular with cyber criminals) to communicate between each other.

While going after the criminals is important and necessary, more priority should be given to strategies of prevention. It is important, especially in developing countries like Macedonia, to raise awareness of the dangers of unsafe internet usage. Individuals should be aware of the potential risks they face when using the internet, and they should know how to protect themselves online. It would be beneficial if the relevant authorities started a campaign where they raise awareness by having short videos online and on TV about the different types of cyber crime and how citizens should recognize them and protect themselves.

Another important aspect would be training of employees. It is crucial that employees, especially those working with sensitive information, have safe working habits that will be regulated with cyber-procedures. All employees must be adequately trained in how to use the internet, the work network, how to treat sensitive information, how to back-up files, how to report a breach, how to take steps for prevention etc. This is particularly important because cyber criminals show tendency of targeting usually the weakest link in the organization, that being someone who is not very tech-savvy. By training the employees, we minimize the chances of cyber criminals exploiting them.●

nian companies burnt in cyber hell)". Nova Makedonija, 21.02.2014 http://novamakedonija.com.mk/NewsDetal.asp?vest=22114737453&id=12&setIzdanie=23107

7 Disclamer: while doing this on-line research, no laws were broken.

WRITTEN BY,
FILIP STOJKOVSKI
fstojkovski@analyticamk.org
Research Fellow at the Security and Foreign Policy Programme

Analytica
Thinking Laboratory
www.analyticamk.org
info@analyticamk.org