CYBERCRIME - A TREAT FOR SERBIAN ECONOMY

Goran Milovanovic, Nada Barac, Aleksandra Andjelkovic,
Faculty of Economics, Nis, Serbia

Cybercrime is a growing problem that negatively impacts Serbian economy. While a lot has been done to combat cybercrime over the then years, criminals still have the upper hand. Serbian IT experts are excited to be able to share their expertise with law enforcement around the world and join efforts in the fight against ccomputer crime.

***Keywords**: cybercrime, Mafiaboy, Russian Business Network, scope of cybercrimes in Serbia*

1. Cybercrime: Overview

Computer crime or cybercrime is a form of crime where the Internet used as a medium to commit a broad range of potentially illegal activities. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, and pornography.

Generally, computer crime may be divided into one of two types of categories: (1) crimes that target computer networks or devices directly (i.e. malware -malicious code, denial-of-service attacks, and computer viruses); (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device (i.e. cyber stalking, fraud and identity theft, phishing scams, and information warfare). Unauthorized use of computers tends generally takes the following forms: Computer voyeur; Changing data; Deleting data, and Denying service to authorized users (DoS attack).

A few well-documented cases include the following:

-The Yahoo! website was pinged at the rate of one gigabyte/second by MafiaBoy at 10:30 PST on Monday, 7 February 2000. The attack lasted for three hours. On February 9, the same technique was extended to Amazon.com, eBay.com, Buy.com and CNN.com.[1] As a result of the attacks, a number of firms formed a consortium to fight DDoS attacks.[2] Investigation by the RCMP and the FBI located a 15 year old child in Montreal who used a modem to control zombies in his DDoS escapade.[3] On April 15, 2000, the RCMP arrested a Canadian juvenile known as Mafiaboy for the

1 Richtel, M. and S. Robinson (2000), Several Web Sites Are Attacked on Day After Assault Shut Yahoo, New York Times (February 9, 2000); http://www.nytimes.com/library/tech/00/02/biztech/articles/09hack.html

2 Messmer, E. (2000), Web sites unite to fight denial-of-service war, Network World (September 25, 2000).

3 http://www.mekabay.com/overviews/history.pdf

February 8th DDoS attack on CNN in Atlanta.

-Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legal. The RBN, which is notorious for its hosting of illegal and dubious businesses, originated as an Internet service provider for child pornography, phishing, spam, and malware distribution physically based in St. Petersburg. By 2007, it developed partner and affiliate marketing techniques in many countries to provide a method for organized crime to target victims internationally. RBN has no official Web site of its own; those who want to buy its services must contact its operators via instant-messaging services or obscure, Russian-language online forums. It has been alleged that the RBN's leader and creator, a 24-year-old known as Flyman, is the cousin of a Russian politician. Because it is possible that recent cyberterrorism activities, such as the denial of service attacks on Georgia and Azerbaijan in August 2008, may have been coordinated by the RBN[4].

The global recession will lead to a rise of cybercrime worldwide. Security firm McAfee's annual Virtual Criminology report says approximately 1.5 million pieces of unique malware identified by the end of 2008, more than in the previous five years combined[5]. The United States has bypassed China as the biggest purveyor of malware as well as sends the most spam worldwide[6]. Not only is the United States relaying the most spam because too many of its computers have been compromised and are under the control of hackers, but it's also carrying the most malicious websites.

2. Cybercrime in Serbia

Organized cybercrime has taken root in Serbia. It doesn't have response mechanisms, laws, infrastructure and investigative support set up to respond to the threat quickly. It is evident that Serbia needs an organization that facilitates transnational law enforcement cooperation.

Serbia's Republic Agency for Telecommunications (RATEL) published on 21 July 2008 a document that contains the technical requirements for authorized monitoring of some telecom services and provides a list of obligations for the telecom operators. The Internet Service Providers (ISPs) are obligated to enable governmental bodies to access updated databases with personal data on users, contracts, maximum speed of data transfer, identification addresses as well as access to database about email users. Also, ISPs are obligated to provide hardware and software for passive monitoring in real time, collecting and analysing Internet activities, statistics, inter-

[4] http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html

[5] Matthew Harwood, Cybercrime Trends Will Worsen in 2009, According to Forecasts, Security Management, 12/10/2008.

[6] SOPHOS, Security Threat Report: 2009.

ception of email, attachments, web mail, IP video traffic, phone traffic, interception of IM traffic, peer-to-peer networks, service of email and forwarding the email content towards the centre of governmental bodies for supervision. ISPs will have to let the police access their databases, including users' e-mail content or browsing history[7]. This regulation seems to be the Serbian version of the data retention directive, since the scope is defined as fighting cyber crime and terrorism.

In Serbia cybercriminals are exploiting the global recession by luring in susceptible victims through the promise of easy money. While Serbian government and law enforcement have their attention diverted by the economy, the door is left open for cybercriminals to continue targeting bank balances and drop in consumer confidence, which is essential to Serbian economy recovery.

On 7 December 2009 an OSCE organized in Belgrade investigation training course for cybercrime experts in South-Eastern Europe on combating malicious software and worms. Fifteen computer crime experts from Serbia and neighboring countries took part in the course, which highlighted techniques used by computer criminals. The course marked the first time the OSCE's Strategic Police Matters Unit has partnered with the commercial sector to offer training for police officers[8].

In Serbia cybercriminals are increasingly focusing on Adobe PDF and Flash files, to infect victims with malware. In addition, they use rich content applications such as Flash files to distribute malicious code. Flash-based ads on the Web, because their binary file format, enable the cybercriminals to hide their malicious code and later exploit end-user browsers to install malware.

Three developments will influence the increase in cybercrime in Serbia. First, as more IT experts get laid off, some will shift into illegal activity to make money. Second, cybercriminals will be a main beneficiary of Serbian government's pledge to bring broadband Internet access to every Serbian citizen. Finally, cybercriminals will increasingly to exploit the best Web 2.0 technologies, such as Trojan technologies, to maximize their illicit gains.

Hackers have been breaking into Facebook and MySpace and implanting malware to distribute to a victim's social network. Serbian IT professionals are already aware of this risk.

The solution is increased coordination between national governments. Serbian government needs to commit to funding the resources

[7] Danica Radovanovic, Serbia: New Instructions and Law Regulations on Online Privacy, Global Voices, July 26th, 2008

[8] http://www.osce.org/spmu/item_1_41924.html

needed to combat cybercrime, and to involve in actions across national borders. Consequently, every government, business and individual must play their part in a global battle.

Conclusion

As Serbian economy begin to enter recession it will be more important for individuals and businesses to ensure that they are on guard against internet attack. The optimal way to prevent malicious files is real-time content inspection technologies that can inspect each and every piece of Web content in real-time which may be malicious.