Cybercrime in the Middle East

الجريمة الإليكترونية في الشرق الأوسط

By Mohamed N. El-Guindy – ISSA Egypt Chapter President

A first-hand look at cybercrime in the Middle East by the ISSA Egypt chapter president.

Cybercrime is a worldwide problem; no country is immune. The Middle East has seen a phenomenal growth in Internet connectivity in recent years and likewise a similar increase in cybercriminal activities requiring an increased effort across the region to strengthen the information infrastructure, educate users in security awareness, and develop cybercrime regulations.

You might not find the word "cybercrime" in the dictionary, but it is very popular term describing the criminal activities related to cyberspace or the cyberworld. According to Council of Europe,[1] cybercrime is a criminal offense committed against or with the help of computer networks; an offense against the confidentiality, integrity and availability of computer data and systems."

State of information security

To understand why cybercrime in the Middle East differs from other areas in the world, we should understand the state of information security in this region which is affected by factors such as growth of user base, poor security awareness, lack of training for law enforcements, and lack of regulations.

Growth of user base

With the increasing availability of broadband connections and the decrease in subscription fees, the number of new online users in the Middle East is outpacing the rest of the world. According to Internet World Stats,[2] Internet use in the Middle East had reached 2.5% of the total worldwide use by December 2007. Middle East use from 2000 to 2007 increased by 920.2% compared to 259.6% for rest of the world! This large number of users in Middle East has made the Internet a popular means of communication as well as opening new opportunities for online business. The potential for abuse is even greater. Due to the lack of security awareness programs, many online users are becoming victims of cybercrime attacks and the incidence of successful attacks is increasing.

Information infrastructure

The investment in IT infrastructure in the Middle East is extensive, especially in Gulf; but there is more to network infrastructure security than the initial implementation of the system – upgrades and ongoing maintenance must be taken into account. Meanwhile financial institutions and corporations in the Middle East say they have the best and most expensive security systems that no hacker can beat. But financial experts[3] in Middle East have disclosed that over the past few years banks in the region lost approximately one billion dollars to organized cybercrime on online transactions. Additionally most banks[4] in the region are vulnerable to phishing attacks, which should be strong warning to allocate more investments in IT security systems and awareness.

Investments in information infrastructure have increased the value of e-commerce and e-governments and have created great opportunities for small businesses in the region, helping with the unemployment problem. However, not all investments are directed toward including and implementing security solutions while developing the infrastructure – business first, security later. Also ISPs in the region have been rapidly deploying broadband Internet connections without implementing security solutions – a major problem in the region – business first, security later. Without sufficient security policy to protect their businesses against spammers, most ISPs in the region are blacklisted and marked as sources of spam. A culture of information security must be foremost. Even the richest countries in Middle East are not immune to cybercrime: the UAE's e-government sites have been attacked by hackers, causing financial loss and availability of confi-

[1] http://conventions.coe.int.

[2] Internet World Stats: http://www.internetworldstats.com/stats5.htm.

[3] Saudi Chamber of Commerce: http://www.chamber.org.sa/allnews/all_newsDetail.asp?id=502.

[4] http://www.infosecnews.org/pipermail/isn/2008-February/015963.html.

dential information to the public; the Al-Jazeera[5] website is another example of hacking big names inside the region.

Poor security awareness programs

Information security awareness is crucial for combating cybercrime. In the Middle East there is a significant lack of security awareness among users, whether the general public or organizations and enterprises. Comparing security awareness in the Middle East to Europe or the U.S., we would see far less effort being made to raise awareness among users. One of the major factors that makes information security awareness programs ineffective in the region is that most IT security awareness programs available are in English, making them difficult to implement in the region. This lack of security awareness is also a big problem inside IT companies in the region as most IT decision makers in Middle East are not aware of the cybercrime problem, thinking the Middle East is still immune. Also they do not have good security policies and do not divulge any information security incidents – business first, security…. For example a former employee email which is still active can lead to a big security hole inside the enterprise and could allow an employee to steal or hack into the network. Poor security awareness means that investments to fight cybercrime are minimal, leaving businesses across the Middle East vulnerable to cybercrime or online attacks. This region needs strong security awareness training, targeting native speakers to educate users, employees and law enforcers to understand the risks and thwart the attacks.

A target for cybercriminals

Many international sources[6] are warning that the Middle East is becoming a major source of cybercrime; for example, Saudi Arabia is ranked as the leading country in the region as the target *and* source of malicious activities online and ranked number 38 worldwide; also Saudi Arabia is the number one source of malicious attack in the Gulf Cooperation Council (GCC).[7] Egypt also is one of the *most phished*[8] countries in the world with about 1763 phishing incidents, followed closely by other countries in the region such as Saudi Arabia, the UAE and Qatar. It is not hard to see that cybercrimes are increasing in the region due to growth of user base with poor security awareness and the lack of regulations. But even normal cybercrime such as phishing has its unique characteristics in Middle East. Due to religious motives and political issues in the region, hackers are successfully sending political or religious scams[9] urging users to open an email attachment, infecting the computer with malware in order to attack infrastructure targets in Middle East such as e-commerce websites, banks, telecommunications and government services.

Another important factor making the Middle East, and especially the GCC, a source and target of much cybercriminal activity is the growth of international banking and money laundering. The unique opportunities of a quickly developed financial infrastructure allowing anyone to transfer monetary funds to any country, anonymously and through tangled routes caught the attention of cybercriminals. Electronic transfer is an efficient tool for concealing sources of money intakes and laundering illegally earned money. There are many well-known online money laundering cases involving victims in Middle East who were tricked in order to steal their identity or transfer money from their real accounts using phishing and scams. For example, the attacker will send a well-crafted link to users in the Middle East with an email saying "there is a bulk money someone wants to transfer to UAE bank account." Too often users will reply to this scam, start to interact, and in the end be victimized.

Social networking

Cybercriminals also attack popular sites in the region like many social networking websites. Most employees and online home users are using social networks. Many studies[10] have revealed that social networking can open a backdoor into corporate IT platforms, putting businesses and individuals at risk of information compromise, identity theft and other malicious attacks. Cybercriminals are looking for sites that have many users with poor security awareness to infect, and social networking sites are an excellent place to hunt. The Middle East at present has over 27 local[11] social networking sites which can be used by hackers to infect users with malware or redirect them to phishing websites, stealing passwords, accounts and opening security holes in the victim's machine. Local social networks in the Middle East are not secured enough to protect user's or member's privacy and sensitive information; we hear about new cybercrime daily in the Middle East that happened to someone using social networking. Users in the Middle East also utilize international social networks[12] such as Facebook and Myspace for communications, friendships, blogging and other activities that if not taken with much care, can lead to ID theft and malicious activities against home users and employees in both private and public sectors as long as there is no policy. The risk is very high not only in social networks but also in peer-to-peer networks, Web 2.0, chatting and popular applications that can be exploited. Again, the need for security awareness training in the Middle East is great.

Unemployment

Most Middle East countries are facing unemployment problems; the numbers are increasing daily and will affect the growth of cybercrime in the region if not taken into con-

[5] http://www.wired.com/politics/law/news/2003/03/58200.

[6] Symantec *EMEA Internet Security Threat Report*, April, 2008.

[7] Gulf Cooperation Council : http://www.gcc-sg.org/eng/index.php.

[8] Source: http://toolbar.netcraft.com/stats/countries.

[9] http://www.informationweek.com/news/showArticle.jhtml?articleID=198900155.

[10] NCSA : http://staysafeonline.org/features/ncsalibrary.html.

[11] An De Jonghe, *Social Networks Around The World*, BookSurge Publishing (February 15, 2008).

[12] Map of Social Networking: http://valleywag.com/tech/data-junkie/the-world-map-of-social-networks-273201.php.

sideration. According to World Bank, "The Middle East and North African States are to face great challenges; they have to work by themselves to generate 100 million new job opportunity by 2020 or the region's instability will increase."[13] Statistics reveal that the unemployment rate is very high among youth in the region, most of whom are university graduates with computer and Internet competency. Even if they do not have access to Internet at home, cybercafes are readily available throughout the region at lowest rates for Internet access.[14] All these factors combine to create a new generation of local hackers and cybercriminals. Most are script kiddies working for financial motives, though others have terrorist motives. They do not have deep programming knowledge like experienced hackers who can create their own malware or viruses, but they take advantage of many Arabic websites available for free that help them understand the basics behind hacking techniques with links to underground hacking sites in foreign languages and even free tools to use. Script kiddies represent the biggest risk in Middle East; they have time on their hands, low cost Internet access and cybercafes that can be infected to launch their attacks easily.

Regulations: poor or none

Most of the countries in the region do not have Internet-specific laws, though some are beginning to adopt these laws. A few countries in the region are trying to shape new legislations and legal definitions for cybercrime, such as the UAE[15] and Saudi Arabia, but there still need to be more specific laws for cybercrime activities. Due to political issues in the Middle East, many countries in the region are using emergency laws instead of regular cybercrime laws against citizens as a form of combating cybercrime such arresting a blogger for insult.[16] Other countries in the region are trying to prevent such activities by blocking access to certain websites. But both actions are not effective. Regular laws and emergency laws in the Middle East are not designed specifically to deal with cybercrime, and there is no definition for such activity inside the law. Also that sort of action will put normal citizens in jail with cybercriminals.[17] Lack of regulation by default equals lack of law enforcement training, tools and techniques used to investigate the cybercrime. Middle East countries also do not have specific laws for intellectual property violation through cyberspace. According to the *Symantec Threat Report*,[18] Egypt is ranked number two across the EMEA in virus infection. We all know that viruses spread in executable files which can be downloaded through peer-to-peer networks or through pirated software, and this mean that Egypt also ranks high in intellectual property violation and software piracy[19] through cyberspace.

Motivations for cybercrime

Cybercrime in the Middle East has two main motivations: financial gain and terrorist communication and attack.

Financial

Due to increased unemployment problem and lack of security awareness among users, cybercriminals in the region are continually looking for new ways to steal. As most of the local hackers are script kiddies, they use Arabic hacking websites to organize the cybercrime and spread their activities. Spam and phishing have become the biggest problem in the region. Local cybercriminals are targeting home users, e-commerce websites, financial institutions websites and small business companies. Cybercrime for financial gain in the Middle East also includes violation of intellectual property by selling pirated software. Cybercriminals also use spam to sell certain products that might be prohibited in the region such as drugs and pornography. Spam can be used also by cybercriminals to generate fake traffic and steal money from advertising networks that begin to realize the problem and block Internet traffic from certain Middle East providers. The Middle East also is known for credit card fraud which causes e-payment processors to block Middle East countries.

Terrorist

Terrorist motivation plays a dramatic role in cybercrime in the Middle East as a communication tool and a weapon against an enemy. Cyber terror is growing in the region due to religious motives, Israeli-Palestinian issues, political issues and unemployment problems. "Jihad Online"[20] claims to use hacking technique to make jihad[21] against their enemies. Cyber terrorists use their websites in many activities such as psychological warfare, propaganda, recruitment, fund raising, coordination of actions and data mining. One jihad website captures information about users who browse their websites. Those who seem most interested in the group's cause or well-suited to carrying out its work are then contacted. Recruiters may also use more interactive Internet technology such as online chat rooms and cybercafes, looking for receptive members of the public, particularly young people who have the religious motive that later can be converted to terrorist motive! They also look for IT professionals who can be influenced to help with the technology. Using electronic bulletin boards and forums as vehicles, they reach out to potential recruits.

Terrorists use the Internet not only to learn how to build bombs, weapons information and raising their funds but also to plan and coordinate specific attacks. For example Al Qaeda relied heavily on the Internet in planning and coordinating many attacks. Jihadists are utilizing advanced techniques to attack online targets and also are using advanced encryp-

[13] World Bank report, 2007 http://www.worldbank.org.

[14] http://www.sdnp.undp.org/it4dev/stories/egypt.html.

[15] http://archive.gulfnews.com/articles/06/02/13/10018507.html.

[16] http://news.bbc.co.uk/2/hi/middle_east/6385849.stm.

[17] http://www.openarab.net/en/reports/net2006/jordan.shtml.

[18] Symantec *EMEA Internet Security Threat Report*, July – December, 07.

[19] http://w3.bsa.org/globalstudy//upload/2007-Global-Piracy-Study-EN.pdf.

[20] http://www.adl.org/internet/jihad.asp.

[21] http://en.wikipedia.org/wiki/Jihad.

tions to communicate[22] online to coordinate attacks. They are working hard to develop their encryption tools as they do not trust other software out there.[23] Jihadists are always targeting military networks, government systems and websites, e-commerce and financial institutions and many other websites that side against their positions.[24] It is important to understand that not all cybercriminals involved in cyber terrorism are script kiddies; they are always looking for professionals and potential members. Propaganda is also one of the biggest activities for jihadists online. They use their websites to advertise their activities in real life,[25] encourage others to join, and warn others that they are coming!

Conclusion

Cybercrime in Middle East has its global impact especially with cyber terrorism. Despite the progress being made, most countries in the Middle East still rely on standard laws to combat cybercrimes. Strong and specific regulations should be a concern to all Middle East governments. Our countries should learn from others; we have to prepare ourselves for the changing and increasing phenomenon of cybercrime in the region as it is not only affecting our region but also affecting our relations with others around the world. We must develop security awareness training and education programs to help minimize the risk. Governments and private sectors should invest more in information infrastructure security, employees' awareness and compliance. Government authorities should understand the real risk of cybercrime and they should train their law enforcement. Our region is full of problems varying from political to financial, and all those issues will increase the number of cybercriminals. For those who think that our region is still immune from cybercrime, they should understand that we are living in connected world. It does not matter where you live and what you are doing, you will be affected sooner or later. So let's not just watch what is happening around us without taking an action.

Security first.

About the Author

Mohamed N. El-Guindy, PhD, MBCS CITP, is an IT specialist working in the field of information technology for over a decade. He is the president and founder of ASK PC, LLC and current president of ISSA-Egypt chapter. He is author of the first IT security course in Arabic, a Microsoft technology speaker, a member of IEEE, BCS and WAOE, and is well-known in the Middle East with his online Arabic technical support community. He can be reached at admin@ask-pc.com.

[22] http://www.international.ucla.edu/cms/files/FTPV_A_175157_P.pdf.

[23] http://memriiwmp.org/content/en/blog_personal.htm?id=342.

[24] Arab Hacker: http://www.foxnews.com/story/0,2933,201684,00.html.

[25] http://60minutes.yahoo.com/segment/47/jihad_online.