AN INTRODUCTION TO EMERGING THREATS AND VULNERABILITIES TO CREATE USER AWARENESS

N Veerasamy & B Taute

Council for Scientific and Industrial Research (CSIR)

nveerasamy@csir.co.za

+27 841 2893

PO Box 395

Pretoria 0002

ABSTRACT

With technological change and advancement, attackers are increasingly becoming more sophisticated in their attack strategies and techniques. Other global factors and developments also impact the line of attack. This paper provides an introduction to the most current, pertinent attack strategies and trends. It aims to create an awareness of emerging areas that should be better studied and understood. The paper addresses the blurring lines of cyber crime, information warfare and cyber terror to indicate the key concerns at a national, commercial, governmental and individual level. Thus, the paper proposes and discusses topical security threats to elucidate their methodology and gauge their impact such that further strategic, operational and technical measures can be taken

KEY WORDS

Cyber crime, cyberterror, Information Warfare, security, threats

AN INTRODUCTION TO EMERGING THREATS AND VULNERABILITIES TO CREATE USER AWARENESS

1 INTRODUCTION

ICT networks are regularly the target of various exploits. However, due to poor user awareness the ease and impact of attacks is missed. This paper attempts to clarify the current perspectives of information security exploitation by providing an introduction to emerging threats.

Enormous investment is put into tools, personnel and procedures to better protect systems. Technical evaluations and analysis can identify security threats, but by instilling good security awareness many mistakes can be prevented upfront.

In addition, by looking at threats from a higher-level perspective, understanding can be gained into the underlying motives and areas of impact. This view is given in the framework proposed in Section 2. It is also important to take note of the influence of global trends and issues that impact the development of new attack techniques. Thus, by studying attack trends, knowledge can be gained into more effective protective techniques and emerging areas that should not be overlooked. This will be addressed in the discussion of top exploits in Section 3.

2 FRAMEWORK

As a preliminary introduction to information security threats and vulnerabilities a framework is presented that depicts the current state of the various perspectives of technological information exploitation. The framework (Figure 1) commences with the different perspectives of perpetrators, then their underlying motives which is enabled by information security exploits through the portals of Information Communication and Technology (ICT) networks and leaves on impact of different domains. A brief discussion of the framework follows.

2.1 Perspectives of Perpetrators

When an attack takes place on a network or computer, the media often labels it as an act of cyber terror or a hacking incident. However, much misconception exists over whether an attack on the network is information

warfare, cybercrime, or cyberterror. A brief discussion follows to place these concepts into perspective (Figure 1).

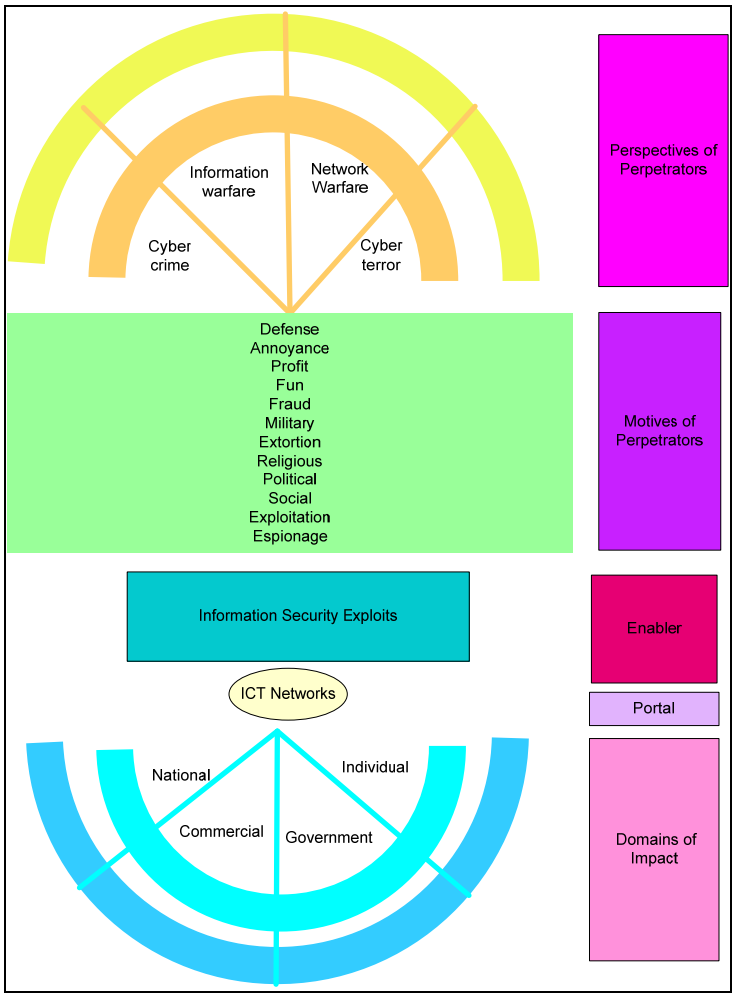

Figure 1: High-level Framework of Current State of Information Security

Symantec defines cybercrime as criminal activities using a computer, network or hardware device where the computer or device may be the agent, facilitator or target of the crime [9]. Information warfare implies a range of measures intending to protect, exploit, deny or destroy information and resources to gain a significant advantage over the adversary (Alger in [5]). Thus information warfare addresses both

offensive and defensive areas whereas cyber crime largely looks at attack activities. Network warfare can be seen as an enabling component of Information Warfare which sees conflict in the networked forms of communication. Thomas argues that the core of computer Network Warfare is to disrupt the layers in which information is processed with the objective of seizing and maintaining control of network space [17].

Cyberterror addresses unlawful attacks and threats against computers, networks, and information done to intimidate the government or its people to further certain political or social objectives and thus cause violence or enough harm to generate fear [10]. Cyberterror can thus form part of both information warfare, network warfare and cyber crime. Cyber terror largely operates from political, religious or social motives and thus when invasive illegal activities are committed, it can be considered as cybercrime. Furthermore, hacking describes activities to break into systems covertly and exploit vulnerabilities. Thus, hacking relates to techniques to carry out cyber crime, information warfare and cyberterror. Another aspect of cybercrime linked to cyberterror is that hackivists, who will engage in hacking activities from a political standpoint [19].

From the discussion, a key distinguishing factor will be the motive that will determine whether an attack is cyberterror, cybercrime, or information warfare and is discussed next.

2.2 Motives of Perpetrators

The outcome of security exploitation is to have a beneficial result for the perpetrator: be it financial reward or the satisfaction gained from causing inconvenience. Some typical motivating factors follow:

- Cyberterror: social, religious, political, philosophical [8][6][15][7]
- Cybercrime: fraud, espionage, sabotage, extortion [11]
- Information warfare and network warfare: exploitation, military, defense [3]
- Hackivists : hacking for political reasons [19]
- Hacking: fun, profit, cyberterror, cybercrime, information warfare, hackivism[14]

Some motivating factors cross categories. For example, exploitation is applicable to cybercrime, network warfare and information warfare. Thus, the lines are quite blurred and a closer inspection of the target can shed light on the intended impact. The discussion therefore moves to the domains of security exploitation which looks at the target areas.

2.3 Domains of Impact

Information security exploitation can have an impact at four typical levels. This includes National, Governmental, Commercial and Individual:

Denning states that serious attacks against critical infrastructures would be acts of cyberterrorism, depending on their impact [10]. If we were to look at cyberterrorism, cyberterrorists would typically launch attacks at targets of national and governmental importance as this would have the biggest impact. However, victims of cybercrime and actors of information warfare can be found across all four domains. Cybercriminals attack various individuals and companies and defensive strategies of information security are also applied across government, industry and personal systems.

2.4 Summary of Framework

ICT networks are the portals through which information security exploitation is taking place. Information security can be classified as cybercrime, information warfare or cyberterror depending on the underlying motive. However, in many instances activities are blurred and clear boundaries cannot be established. Nevertheless, the combination of various threats, vulnerabilities and risks enable information security exploitation. Thus the focus shifts to exploits to look at emerging trends and create user awareness.

3 TOP EXPLOITS TO ALL DOMAINS OF IMPACT

Currently the most common and critical threats facing users: Trojans, phishing with custom malware and web application vulnerabilities [13]. A discussion of each of these areas follows.

3.1 Trojans

A Trojan is code that hides insides a program and performs a disguised function [16]. Trojans provide the ability to control a machine and thus monitor activity and download information. In the Symantec Global

Internet Threat Report, Trojans made up 71% of the volume of the trop 50 malicious code samples [18]. The type of information that can be gained access to include: trade secrets (Commercial domain), classified data like strategy and policy documentation (National domain), identification or voting records (Governmental domain) and email or Internet banking records (Individual domain).

Thus, the impact of Trojans is felt across the board from national to individual level. Typical types of Trojans as listed by the IBM X-Force study include Infostealers (keyloggers, password stealers) and Clickers (provide revenue through malicious traffic generation) [1].

3.2 Phishing with Custom Malware

Users are often sent emails requesting an update of personal details by clicking on an embedded link. The spoofed sender is typically shown as banks and other reputable vendors. According to IBM, 82% of targets in 2008 were financial institutions [1]. Users are actually redirected to a malicious site where they are prompted to enter personnel information which is then harvested for other fraudulent activities. Users could also be installing rootkits and other malware when clicking on links, thus providing control of machines to the perpetrators.

Other emerging scams include scareware and ransomeware. With scareware, false security warnings are displayed encouraging users to download a named security tool [4]. The user's clicks are redirected to a malicious site whereby malware is downloaded. Thus, users are tricked into installing harmful software.

Ransomeware occurs when data is kidnapped and encrypted. The attackers demand payment in return for the decryption key. This form of extortion originated in Russia but has since surfaced around the world [4].

3.3 Web Application Vulnerabilities

SQL injection takes place when there is improper validation of user input. According to IBM, SQL injection vulnerabilities increased a staggering 134% from 2007 [1]. This indicates that even though this vulnerability is not a new exploit, its application is still wide-spread. With SQL injection, access to sensitive information in databases can be gained and thus the integrity of information on web sites and in transactions could be in

jeopardy if data is deleted or modified. New attacks could also be embedded in the database and thus be used against other visitors to the site. Examples would be to redirect visitors to a vulnerable web site or manipulate a feedback form by generating a query to select and modify supplier details through cleverly crafted SQL statements.

Cross-site scripting also takes advantage of improper validation of user input and can utilise cookie theft to hijack sessions, gain access to sensitive information, manipulate fields and commit fraudulent transactions [18]. Another manipulation technique is to embed vulnerabilities or scripts to steal information

Thus, various techniques exist to trick users into downloading malicious software and these types of attack will continue to fool users unless some awareness is created on the topic. In addition, other trends stemming from global issues also emerge and are discussed next.

4 THE NEW FACE OF THREATS

Whilst not new, spam continues to be a thorn in the side of many network administrators. The economic crisis could also see new avenues of exploitation as people try to make the quick buck. However, a crucial area of exploitation will be sites like Facebook and Myspace. Another area that is often overlooked is the spreading of infections on storage devices like USB and flash drives. In addition, the underground server economy provides an extensive black market for malicious exploits and other resources. A brief discussion on each of these issues follows.

4.1 Spam

In previous years, spam made up 71% of monitored email traffic [18]. Phishing scams can also be distributed using spam. As a consequence, with poor user awareness, an ignorant or ill-informed used could be enticed or manipulated into believing that a received link is a genuine message from a bank or vendor.

Spam trends are changing in terms of delivery methods like pdf, random text and image spam (complex images, random pixels and borders to disguise intention) [1]. Users are attracted to a range of services being offered from handbags to watches. The implications include the storage resources, engagement in unnecessary services and resource wastage. The

impact of bringing down one of the key spamming role-players was felt when the spam host McColo Corporation had the plug pulled out on them in November 2008. McColo is believed to have been responsible for up to 60% of worldwide spam [12].

4.2 Economic Crisis

With the current downturn in the economy and unemployment at such a high rate, the negative situation could be further exploited through the exploitation of people's fears and quest for financial stability. McAffee predicts that 2009 will see many fake web sites and services being hosted [12]. Examples include transactional services, investment firms and legal services. Phishing scams could also utilise these tactics.

4.3 Social Networks Exploits

Social networks like Facebook, Hi5, Friendster and MySpace are becoming targets of spam, adware, malware and other social engineering scams. At the end of 2008, the Koobface exploit surfaced. According to the Computer Emergency Response Team (CERT) advisory, it is spread through an invitation which provides a link to a video in which users are prompted to update Adobe Flash Player [2]. When users agree to the download, it is actually malicious code being installed. These social networks provide a wealth of information in terms of personal details, tracking activities and interests. They can also be used to profile users and commit acts of identity theft, fraud, spoofing and various other exploits.

4.4 Storage Devices

The unregulated use of USB and flash memory discs can see the widespread leakage, theft, loss or infection of data across enterprises, governments, commercial companies and individual users' systems.

4.5 Underground Economy Servers

The criminal black market is a hub to advertise and trade in stolen information and services, as well as required tools and data. Typically the type of goods available on these servers includes [9]:

- Information : Government issued identification numbers, credit card numbers, credit card verification numbers, debit card numbers, PINs, user accounts, email address lists, bank accounts

- Services: Scam page hosting, job adverts to be scam developers or phishing partners
- Applications: Malware, Zero-day exploits

From a security point of view at a national level, the ability to track and shut down these sites has become an issue. However, due to the nature of these servers, they can shut down quickly and move to a new site. From an individual level, users need to be made aware of the ease and frequency of exploitation and be aware that personal information can be sold off.

4.6 Defensive Strategies

A few defensive techniques are listed to help protect against some of the described information security exploits (whilst remembering that many threats have no identified solutions as yet).

- It is advised to rather use reputable vendors instead of following the prompts from displayed warning messages.
- Be aware of suspicious sites or emails (many anti-virus software have automatic scanning of potential vulnerabilities)
- Refrain from clicking on sent URL's in emails but rather navigate to the site itself and try and find listed location
- Users need to be made aware of regularly backing up data to prevent becoming a victim to ransomware attacks
- Defensive tool like anti-virus, anti-malware and firewalls have to be regularly updated
- Remain current with patch updates (web application fixes)
- Spam filters, use of alternate email address when browsing to prevent spam being sent to main email address
- Be very cautious when disclosing personal information on social networks
- Using an assigned memory stick for external connections and routine scanning/formatting when using it on sensitive systems
- Regulation is needed to control portable drives and users need to be better educated on the sensible use of these portable devices.

5 CONCLUSION

A worldwide battle has emerged in the form of hacking, cybercrime, information warfare, network warfare and cyber terrorism. At the heart of these areas is information security. Threats like phishing, Trojans, and web vulnerabilities still exist but are finding new avenues of exploitation like preying on people's insecurities during the economic crisis and kidnapping data. Thus, users need to be made aware of these techniques and remain vigilant for scams and other deceptive techniques. Users should not fall into a false sense of security but be knowledgeable of the potential traps of social exploits and that disclosed personal information is not necessarily secure and private. Defensive mechanisms need to be instituted across the domains. This translates to: the establishment of a Computer Security Incident Response Team (CSIRT), in-house security awareness and maintenance programs (typically ISS at a commercial and governmental level) and personal security awareness like getting alerts from security web sites and organisations.

This paper presents a structured overview of the underlying perspectives, motivation, application areas and techniques of information security exploits so as to create an awareness of the current face of threats in the global networked space.

6 REFERENCES

[1] Anonymous, "IBM Internet Security Systems X-Force 2008 Trend and Risk Report," IBM Global Technology Services, 2009.

[2] Anonymous, "Malicious code targeting social networking site user," US Computer Emergency Readiness Team (CERT), Accessed 7 April 2009, Available online at http://www.us-cert.gov/current/archive/2009/03/04/archive.html.

[3] N. Bhalla, "Is the mouse click mighty enough to bring society to its knees?" Computer Security, vol. 22, pp. 322-336, 2003.

[4] G. Cluley, "Viruses and Spam 2008: A look at the current security landscape and future trends," 19 August 2008.

[5] B. Cronin and H. Crawford, "Information warfare: Its application in military and civilian contexts," The Information Society, vol. 15, pp. 257-263, 1999.

[6] K.C. Desouza and T. Hensgen, "Semiotic emergent framework to address the reality of Cyberterrorism," Technological Forecasting and Social Change, vol. 70, pp. 385-396, 2003.

[7] A. Embar-Seddon, "Cyberterrorism: Are we under siege?" Am.Behav.Sci, vol. 45, pp. 1033, 2002.

[8] C. Foltz Bryan, "Cyberterrorism, computer crime, and reality," Information Management & Computer Security, vol. 12, pp. 154-166, 2004.

[9] M. Fossi, E. Johson, M. Turner, J. Blackbird, D. McKinney, M.K. Low, T. Adams, M.P. Laucht and J. Gough, "Symantec Report on the underground economy," Symantec, 2008.

[10] S. Gordon and R. Ford, "Cyberterrorism?" Computer Security, vol. 21, pp. 636-647, 2002.

[11] I. Lachow, "Cyber security: A few observations," National Defense University, 2008.

[12] McAffee Avert Labs, " 2009 Threat predictions," McAffee, 2009.

[13] H. Meer and C. van der Walt, "Cyberterrorism threats," Sensepost, Personal communications on 11 March 2009.

[14] Nortel Networks and Aspen Institute, "The promise of global networks (Annual Review of the Institute for Information Studies)," Institute for Information Studies, 1999.

[15] M.M. Pollitt, "Cyberterrorism - fact or fancy?" Computer Fraud & Security, vol. 1998, pp. 8-10, 1998.

[16] D. Russell and G.T. Gangemi, “Computer security basics,” O'Reilly Media Incorporated, 1991.

[17] T.L. Thomas, "Chinese and American network warfare," Joint Force Quarterly, vol. 38, pp. 76, 2005.

[18] D. Turner, M. Fossi, E. Johson, T. Mack, J. Blackbird, S. Entwisie, M.K. Low, D. McKinney and C. Wueest, "Symantec Global Internet Security Threat Report," Symantec, Tech. Rep. Volume XIII, 2008.

[19] G. Weimann, "Cyberterrorism: How real is the threat?" United States Institute of Peace, Tech. Rep. 119, pp. 1-12, 2004.