Information Security - Recent Attacks In Fiji

Shaneel Deo, Mohammed Farik

Abstract: Information technology (IT) plays a vital role in Fiji's economy as businesses strive for competitive advantage. However, IT has also become a tool for attackers. Hence, it is important that all IT users invest in better information security technologies and practices to safeguard against all possible attacks and threats that emerge in the horizon. In this paper, we review recent information security attacks that have taken place in Fiji and recommend countermeasures to safeguard against such attacks in the future.

Index Terms: Attacks, data, exploits, Fiji, information security, threats, vulnerabilities

1 Introduction

Information security ensures confidentiality, integrity and availability of information in information systems (IS). IS are made up of components such as data, hardware, software, procedures, networks, and people. The aforementioned must be protected at all times from both internal and external threats that include hackers and malware. According to Rouse (2016), information security is not a single technology, but a strategy comprised of the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Processes and policies typically involve both physical and digital security measures to protect data from unauthorized access, use, replication or destruction [1]. This paper reviews a few recent attacks on information security in Fiji. For each attack scenario, we recommend some solutions to prevent such attacks in the future. In the next Section, some recent cases of such attacks and their preventative measures are presented.

2 Cases of Information Security Attacks

According to Whitman and Mattord, to make sound decisions about information security, management must be informed about cyber threats to its people, applications, data, and systems [2]. This section explains some attacks that have happened in Fiji

2.1 Malware Infection

One of the most common information security attacks is malware. This is software that is mainly built to generate unauthorized entry point, or damage software or data without the knowledge of the person. There are many types of malware such as spyware, key loggers, viruses, worms or any type of malicious code that breaks into the computer. Last year, a company in Suva lost US$65,000 to cybercriminal in a single remittance transaction for purchase of soft goods from Taiwan [3]. Payment was diverted to UAE and then to India. What this exploit did was injecting random HTML code in the web page displayed by the browser and intercepting any payment data entered by the user in the original or inserted web forms. The situation arises because there was weak and loopholes in banking session between the victim's browser and the online banking web app, in other words, by using a Man-in-the-Browser (MITB) technique. Customer's bank account website was affected. This malicious program is spread via specially created emails with an attachment containing a document with the downloader. Three major ways in which we can protect IS from such attacks include – first, implementing best and applicable security software such as *Bitdefender 2016*. Second, use a security-mindful Internet service provider (ISP) and third, be careful when opening attachments.

2.2 Phishing Email

One of the common problematic attacks is the phishing email. Phishing is a type of fraud in which an attacker tries to find out information such as the users login credentials or account information by deception as a truth worthy entity or individual in email, instant messaging or other communication channels. In total 18 cases of cyber laundering through email spoofing were investigated by the Finance Intelligence Unit (FIU) between 2013 and 2015 [4]. List of offences include – four attempted cases amounting to FJ$300,000, one case of recovery of stolen funds: amounting to FJ$60,000 and thirteen cases of stolen funds amounting to FJ$724,000. One of the attackers used the malware *Dridex*. Dridex uses email attachment in Word or Excel, causing macros to activate and download Dridex, infecting the computer and opening the victim to banking theft. These types of attacks are increasing because users are either giving their personal email ID publicly, or registering for fake surveys or campaigns that says they would win if they send their email and details to them. Consequently, both the user email and computer get infected. This type of attacks works through most spam campaigns spreading Dridex using attached Word documents containing a malicious macro. Symantec detects these malicious attachments as *W97M.Downloader* [5]. W97M.Downloader specializes in stealing bank credentials via a system that utilizes macros from Microsoft Word [5].The targets of this malware are Windows users who open an email attachment in Word or Excel, causing macros to activate and download Dridex, infecting the computer and opening the victim to banking theft [5]. Ways to prevent such attacks are include – one, being cautious with email attachments and not opening an attachment if it is not from a known sender. Two, consider configuring an antivirus to scan all email attachments. Three, implement a good spam-filter to identify and isolate all spam emails. Four, apply caution in the use of digital signatures,

- *Shaneel Deo is currently pursuing master's degree program in Information Technology in University of Fiji. E-mail: shaneel.deo@fnu.ac.fj*
- *Mohammed Farik is a Lecturer in Information Technology at The University of Fiji. E-mail: mohammedf@unifiji.ac.fj*

instant messaging systems, and social network sites.

2.3 Unethical Hacking

Hacking is a top threat that can crack information system securities. According to Emberton (2016), an unethical hack is one that is done without the target of the hack being aware [6]. It is often done to break into a network system to steal information or money, and sometimes to cause damage by inserting a virus or malware program. Unethical hacking is against the law, and those who engage in the act are considered cyber criminals. Fiji Police Force's Cybercrime Unit (FPFCU) warns of an increase in cybercrimes, in particular hacking by locals [7]. In 2015, a man was able to graduate with a degree within his first year of tertiary education and became a teacher after hacking into a prominent university's database [7]. While the man became an assistant head teacher within his first year of teaching, he continued hacking as a business allowing a number of other students to graduate without completing the prescribed years of study [7]. According to FPFCU, the man hacked into the university's system from his home using a laptop [7]. FPFCU described similar cases of hacking in Fiji where student records and intellectual property were compromised [7]. Countermeasures to detect and prevent such attacks include – one, investing in best and latest generation agile firewalls that can detect, prevent, and report intrusion attempts in real-time. Capabilities such as virus checking at the firewall, implementing both software and hardware firewall in layers of defense, and enforcing physical authentications like biometrics will also help. Two, implementing best encryption for all connections and data transfers, authentication by synchronized, timed passwords or security certificates. Three, no one except for the network administrator should be granted system permission to install and execute software tools such as port scanners and other network monitoring tools on the network computers.

2.4 Social engineering attacks through Facebook

Social engineering attack or persons hacking is a term used to explain the act of deceiving a user by an act of deceptiveness. For example someone could call up an organization and cheat an employee into thinking they are from IT department and will ask them to verify their username and password so that they can gain access to the network or take a look at a web page so they can rob information. In another case, a 27 year old resident of Nadi was charged for creating a fake Facebook account by using the profile information and picture of a well-known radio personality [8]. According to Fiji Police, attacker then went on to allegedly displaying electronic items for sale, and exchanging information such as contacts from the group whereby sale proposals took place. It is also alleged that victims of this case deposited money into the attacker's bank account but never received anything. The attacker then deactivated the account after customers had made payments. The same attacker has been charged for similar cases in Namaka and Raiwaqa. Social networking site users are hereby advised to be careful about aforementioned transactions. One can prevent such attacks by keeping personal information such as their birth date, location, and other information that can be used in creation of unauthorized or fake IDs and accounts private. There has been numerous instances in Fiji where identify thieves steal photos and create fake profiles to either engage in sales or make contact with your loved ones in disguise. Attackers use blackmail, information disclosure and identity theft techniques. It is important that people log out of social networking sites after use, especially in Internet cafes. Users should not reveal or share too much personal information on the internet, especially photos which can be publically shared by friends to unknowns. Personal information can also be manipulated without user's consent. Other measures that can help include not revealing location information of a photo and avoiding geo-tagging of photos that show exact locations. Also avoid posting photos that reveal where you keep valuables in your home. The more you publicly reveal your identity and social status, not only identity thieves, but also robbers will surely take notice. So, delete photos and posts on your timeline that show personally identifiable information. Finally keep changing account password with stronger ones.

2.5 Denial of Service

Distributed denial-of-service (DDoS) attack disrupted to government website services this year [9]. According to Newswire, official websites of the Fiji Police Force, Royal Fiji Military Force and the Department of Immigration was hacked by unknown hackers [9]. The attack comprised confidentiality and integrity and posed a threat to the Fiji government. Unlike a denial-of-service (DoS) attack, which uses one computer and its own Web connection to flood a targeted system with packets, a DDoS attack uses a botnet of hundreds or thousands of computers to make exponentially greater quantity of service requests. Attackers can use DoS or DDoS attacks to gain control of the target system, vandalize software and data, to finally sabotage business operations. DDoS or DoS attacks can be classified as sabotage or vandalism. It appears that in many such attacks, threat agents were Kurdish hackers. They mostly use SQL injection exploit – an open source CMS script called "*Drupal*" [10]. Website vulnerability includes using an old version of the script as well as use of unsafe passwords. Suggested remedial approaches to fight denial of service attacks are the use of "SYN cookies" either in the server OS or, better yet for network efficiency, in a network security device at the network edge such as the Cisco Guard. Routers can be configured to stop simple ping attacks by filtering nonessential protocols and can also stop invalid IP addresses and have more secure firewalls. Cisco (2016) recommends Anti-spoofing measures such as limiting connections and enforcing timeouts in a network environment seek to ensure that DDoS attacks are not launched or spread from inside the network either intentionally or unintentionally [11]. Finally, it is wise to be ready, using the Cisco six-phase DDoS mitigation model is a good start, and may also be continuously revisited when creating a sound DDoS policy. Preparation is a key part of any DDoS strategy. Ensure that the tools to be used for DDoS identification are tested, functioning, and in the proper locations and that networking staff is trained and capable of operating the necessary tools for DDoS identification.

2.6 Ransomware

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. TrendMicro (2016) explains that more modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to

get a decrypt key [12]. On 25th August, this year a new ransomware was found called fantom which uses a feature to display fake windows update screen that acts as windows OS is installing windows update. But what actually fantom is doing is encrypting victim's files [12]. Fantom attack firstly generates random AES-128 key, encrypts it using RSA and then loads to the server. Then it creates a ransom note by changing fantom extension to the encrypted file. Then two batch files are executed and encrypted. The batch file purpose is to delete the shadow copies with its own fake executable windows update. Vulnerability are that users try to access explicit sites such by illegal download torrent to a software package. Just lately there have even been records of text file documents spreading Ransomware. However, what your location is probably to find this malware in a contaminated email (such a note might be found both in your spam folder and in your Email Inbox). User also opens emails attachments. Typically via the letters in your email from suspicious senders. Regardless of how they have travelled, this virus has found ways to penetrate computers. It also works with the Trojan horse virus. The attack brings alarming notification and sometimes the encryption process makes the whole system sluggish. First solution to protect from such attacks is by using Spy Hunter – a professional Fantom Ransomware scanner – to make sure you find all files related to the infection. Second, backup is the best option to fight ransomware. Third, make sure the software is up-to-date (Microsoft, Java). Fourth, avoid opening attachments or emails from people who you do not know and install and use an up-to-date antivirus solution. Finally, use modern browser such as Internet Explorer 11 which includes better Smart Screen Filter.

3 Conclusion

It can be concluded that more awareness on information security has to be created in both general public level and organizational levels. Such awareness should be able to identify threats, threat agents, exploits, vulnerabilities and attacks on information systems, and finally prevent attacks.

REFERENCES

[1] M. Rouse, "http://www.techtarget.com/network," TechTarget, January 2016. [Online]. Available: http://searchsecurity.techtarget.com/definition/information-security-infosec. [Accessed 3 October 2016].

[2] M. Whitman and H. Mattord, Principles of Information Security, Boston: Cengage, Boston: Cengage, 2014. .

[3] n. delaibatiki, "http://fijisun.com.fj/," Fijisun, 15 December 2015. [Online]. Available: http://fijisun.com.fj/2015/12/13/fijian-firms-lose-thousands-of-dollars-through-cyber-crime/. [Accessed 7 October 2016].

[4] S. Pandey, N. Shah, A. Sharma and M. Farik, "Cybersecurity Situation In Fiji," International Journal of Scientific & Technology Research, vol. V, no. 7, pp. 215-219, 2016.

[5] D. O'Brien, "www.symantec.com," 16 feb 2016. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf. [Accessed 7 october 2016].

[6] Emberton, "computerhope.com," [Online]. Available: http://www.computerhope.com/jargon/u/unethical-hack.htm. [Accessed 15 October 2016].

[7] N. Swami, "Fijitimes.com," Fiji Times, 26 May 2015. [Online]. Available: http://www.fijitimes.com/story.aspx?id=307220. [Accessed 15 October 2016].

[8] E. Turagaiviu, "www.fbc.com.fj/," Fiji broadcasting company, 19 september 2013. [Online]. Available: http://www.fbc.com.fj/fiji/13807/man-wanted-for-identity-theft. [Accessed 15 October 2016].

[9] Newswire, "5 government websites attacked by Kurdish hacker," Newswire, 11 March 2016. [Online]. Available: https://www.newswire.com.fj/national/government-websites-attacked-by-kurdish-hacker-restored/. [Accessed 16 October 2016].

[10] Ekurd, "http://ekurd.net/," ekurd, october 2015. [Online]. Available: http://ekurd.net/kurdish-hacker-targets-dell-2016-06-14. [Accessed 2 october 2016].

[11] Cisco, "A Cisco Guide to Defending Aganist Distributed Denial of Service Attacks," Cisco, [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html#_Toc374453078. [Accessed 2 October 2016].

[12] Trend Micro, "Ransomware," Trend Micro, [Online]. Available: http://www.trendmicro.com/vinfo/us/security/definition/ransomware. [Accessed 13 September 2016].