View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2010 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2010

49P. Web Security: A Cross-Sectional View of Businesses Operating in Jamaica

Curtis Busby-Earle
University of the West Indies Centre, curtis.busbyearle@uwimona.edu.jm

Ezra K. Mugisa
University of the West Indies, ezra.mugisa@uwimona.edu.jm

Follow this and additional works at: http://aisel.aisnet.org/confirm2010

Recommended Citation

Busby-Earle, Curtis and Mugisa, Ezra K., "49P. Web Security: A Cross-Sectional View of Businesses Operating in Jamaica" (2010). *CONF-IRM 2010 Proceedings*. 19.
http://aisel.aisnet.org/confirm2010/19

This material is brought to you by the International Conference on Information Resources Management (CONF-IRM) at AIS Electronic Library (AISeL). It has been accepted for inclusion in CONF-IRM 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

49P. Web Security: A Cross-Sectional View of Businesses Operating in Jamaica

Curtis Busby-Earle
University of the West Indies
curtis.busbyearle@uwimona.edu.jm

Ezra K. Mugisa
University of the West Indies
ezra.mugisa@uwimona.edu.jm

Abstract

Companies and government ministries alike have been rapidly shifting from the brick-and-mortar to the brick-and-click business model following the tremendous improvements in telecommunications infrastructure, coupled with the ever increasing competitiveness and global influences in local industries. Security unquestionably plays a pivotal role in any online presence. Websites that are built and maintained with a greater awareness of security issues have become more difficult targets for those with malicious intentions. These individuals have begun to shift their focus to softer targets both as the primary goal and as launching pads for other attacks. The aim of this paper is to highlight the susceptibility of businesses in Jamaica to these types of attacks by presenting the results of tests conducted on a representational subset of well established businesses operating in Jamaica with an online presence. We also discuss how the tests were conducted and the nature and consequences of the security flaws discovered.

Keywords

e-Business, Security, Vulnerabilities, Exploits

1. Introduction

Jamaica has been striving to move forward in the development of its information and communication technology (ICT) environment: the enactment of the Electronic Transactions Act 2006, the Telecommunications Policy 2007, the five year national ICT strategy 2007-2012 and the request for Jamaica's inclusion in the annual e-Readiness survey (CITO 2009). This survey is a ranking of the world's largest economies and is conducted, compiled and published by the Economist Intelligence Unit. It is anticipated that these developments in conjunction with new legislation and strategies being formulated will lead to an acceleration in consumer and business adoption to drive the advancement in the local business environment (CITO 2009).

In respect to computer and network security, until December 2009 there was no legislation in Jamaica that addressed the issue of cybercrimes. The Cybercrimes Act 2009, passed in December 2009, was developed to provide criminal sanctions for the unauthorized access to and use of computer systems and data, and for crimes which are facilitated by the misuse of such systems and data (of special note, this study was conducted in March 2009).

Many businesses operating in Jamaica have already embraced and integrated the use of the Internet as a part of their core services. Banks and other financial enterprises offer online transaction services, periodicals cater to both local customers and the Jamaican diaspora and even the simplest websites offer the omnipresent email. Although these online services do enhance the experience and interaction opportunities for customers of these organizations, they do introduce unwanted avenues for potentially undesirable accessibility to their computer networks.

If these networks can be accessed, then the organization's assets are subject to a variety of threats.

Globally, software security has become an issue of the utmost importance and albeit both organizations and researchers have approached the issue of security in various ways, the number of malicious programs found has reached an unprecedented high (BBC 2008). Exploits such as distributed denial of service (DDoS), worms, spam and botnets all continue to disrupt or distract us from our daily activities and destroy our software and hardware assets. Bots for example are pieces of software that are typically planted on hundreds or thousands of computers belonging to unsuspecting third parties. Collections of bots (botnets) are capable of acting in a co-ordinated manner (Stallings and Brown 2008) and are utilized to launch attacks such as DDoS. The unsuspecting third party participants in these attacks are typically owners or users of machines that fail to provide or incorporate effective security measures. These include but are not limited to the incorporation of defensive programming techniques, regularly updating anti-malware applications and implementing operating system and application security patches.

Ineffective security measures coupled with broadband Internet access and a lack of awareness of the issues associated with securing computer and network systems makes any business or individual a desirable target for an attack. Jamaica in its development efforts has certainly realized improvements in its broadband services while the number of businesses with an online presence continues to grow, but how effective are the software security measures in these organizations? How easily can these firms be penetrated or used as unwitting participants in an attack?

The remainder of the paper is as follows. In section two we discuss the tests that were conducted, how they were performed and the types of businesses that were investigated. In section three we discuss the results, nature and potential consequences of the flaws that were discovered and present our conclusions in section four.

2. The Tests

Knowingly having your company probed goes by many names such as ethical hacking, penetration (pen) testing, tiger teaming, intrusion testing, vulnerability analysis, and security assessment (Tiller 2005). Regardless of the preferred term the process can be divided into four phases; reconaissance, scanning, enumeration and penetration. Broadly speaking these phases involve gathering information about a target system, determining what services, operating systems and ports are being used, gathering user information such as account names and passwords and finally infiltrating the system.

We were not commissioned by any of the selected companies to perform any security tests and therefore maintained a passive, non-invasive approach to our analysis. As the line between passive and active tasks begins to blur the deeper the tester delves into the phases of a pen test, we restricted our procedures to the first two phases of reconaissance and scanning. Using a number of different techniques and tools we knocked on some “doors” and allowed our actions to be dictated by the responses.

All information was remotely gathered using social engineering, tools such as Google, Nmap and Maltego, and other publicly available sources from the mass media. Our primary goals were to identify operating platforms, operating systems and services, IP addresses and any easily detected vulnerabilities. “Easily detected” requires a bit of clarification. Open ports, SQL injection and SMTP vulnerabilities are all easily identified if they exist. Discovering the UNICODE flaw in Microsoft's IIS or buffer overflow vulnerabilities in operating systems and other services are not.

Being easily detected however does not diminish the severity of a vulnerability. A website that is susceptible to SQL injection can be easily discovered yet the potential gains are extremely rewarding to the attacker.

A typical test would involve obtaining information using periodicals, Google and Maltego. This provided two key bits of data; how aware the company appeared to be of the security implications of divulging unnecessary information (e.g. what operating systems they use) and the IP addresses of key servers such as SMTP, DNS and HTTP. This was the most time consuming phase of each test. We would then visit the company's web site(s). The information gathered from the site in conjunction with that from the following stage provided us with all the data we wished to use. Next we would use a network scanning and security tool such as Nmap to discover the status of any well-known ports. This provided us with the information we needed to complete the test. At this point, there was no further investigation of any company. The results were then collated and presented.

We utilized the most abundant resource at our disposal, students. All had little to no prior knowledge or experience with pen testing, their only advantage was a familiarity with a personal computer and the Internet. This description fits the generally accepted profile of the majority of attackers worldwide who are young adults and others who seek a challenge, and disgruntled or overly inquisitive employees. Prior to commencing the exercise, all members of the project were instructed on local and international laws and regulations on cybercrime and related offenses, and were given strict guidelines on what tools could be used and what techniques would be permitted in their analysis. They arranged themselves into teams of no less than two and no greater than four. No team member should have had any prior direct association (current or previous employment, nor any family member) with the group's chosen target and no two groups could have the same target

Organizations were randomly selected by each team but were required to be (a) generally accepted leaders in their respective industries (b) generally accepted leaders in the Jamaican business environment or (c) a government ministry. These criteria are what we used to establish whether a business is “well established”. However, these criteria in conjunction with the business environment made the selection of targets a challenging process due to the numbers that could potentially fit the description. For example, in the Jamaican business environment there are three cellular providers, two companies that provide reputable dailies and many of the ministries' web sites are still rudimentary in that they offer email contact and corporate information and little more.

Firms were eventually selected from from the following sectors; banking and finance (3); cellular telephone services (1); government(1); the press(1); and trading(1). Considering the aforementioned criteria, the state of the web presence of many companies, and with the exception of a couple of industries, the small number of entities, we thought the numbers adequate for the purposes of this work. Upon completion of their analysis, all teams then wrote and submitted their findings which were then subjected to our verification.

3. The Results

Our teams successfully discovered weaknesses in every organization investigated. We present the results by broadly grouping the potential exploits discovered and highlighting their nature and the potential dangers the underlying weaknesses pose.

3.1 Email

Email is ubiquitous. It predates the Internet and is ingrained in both our private and corporate relationships. Because of its simplicity, importance and universal use, it is the source of many security problems.

Spoofing, spamming, virus propagation, spear phishing, buffer overflow and denial-of-service exploits can all be achieved using the underlying simple mail transfer protocol (SMTP). We were able to verify that *all* of the aforementioned attacks are possible from *every* firm investigated based on the responses we received from their corporate mail servers. This makes it a simple matter for an attacker (internal or external) to use these servers for a plethora of exploits. The SMTP servers can also be used to verify user accounts. Having verified the accounts, an attacker can then proceed to crack the associated password and infiltrate the network.

3.2 FTP

A couple of firms had standard file transfer protocol (FTP) services open on their enterprise servers. There are dozens of FTP exploits and vulnerabilities. Standard FTP for example, transmits its information (usernames, passwords and the data itself) in the clear. It becomes effortless for an attacker to obtain either unauthorized access to the network or the transmitted data itself.

3.3 Injection Attacks

One major firm's website was vulnerable to structured query language (SQL) and command injection attacks. Utilizing the SQL injection vulnerability, we were able to ascertain table and field names in the database and execute queries.

We were able to do this entirely using their website and without any request or requirement for authorization. Based on the type of service the website offered , customer's credit card numbers could be a primary target and could be retrieved using a SQL injection attack. The nature of this flaw is the improper validation of data supplied to fields on the website. The same holds true for the other type of vulnerability this website contained. We were able to craft simple HTML commands that were executed through the website.

This affords a potential attacker the ability to deface the firm's website, or inject malicious code that could be executed when the site is visited by an unsuspecting user.

3.4 Phishing

Phishing is a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity (Jagatic et al 2007). It is a form of social engineering. One company's site was of great concern to us as the company is in the financial sector, it provides its core services online and markets that its services are secure. However its site is exceedingly vulnerable to a web phishing attack. The source of our concern lies in the fact that the registered URL for the organization and an unregistered URL in the *same* domain differ by a single, easily excluded or forgotten character.

A possible attack would be simple. Using a freely available tool an attacker could completely replicate the organization's website and store it in a local directory (which we successfully did), register the available URL, post the replicated site to the newly registered URL and direct all traffic (including login information) from the newly published version to the attacker's machine. An unsuspecting user will be completely unaware of the fact that he no longer has exclusive use of his account unless some form of suspicious activity is noticed.

4. Conclusion

Our goal was to highlight the susceptibility of firms operating in Jamaica to computer based attacks. We have demonstrated that they are vulnerable to a wide range of possible exploits. Businesses operating in Jamaica can be both primary, relatively lucrative targets and unwitting participants in larger, more structured attacks.

It could be argued that some of these successes were due to the infiltration of corporate honeypots which by nature are designed to give their owners the opportunity to observe and learn about those trying to penetrate their systems. A honeypot can be a single computer with IP addresses or an entire network designed to attract hackers (Stallings and Brown 2008). But as we narrowed our investigation to particular types of weaknesses (for example web phishing) to restrict how invasive our tests would be, the possibility of the discovered flaws being false positives was reduced.

One could also suggest that these concerns are not pertinent to the Jamaican environment. The Jamaican ICT landscape is changing and the telecommunications industry is a driver of that change. Broadband access to the Internet via computers and cellular phones alike puts information and access to tools of the hacking trade at the fingertips of even the mildly inquisitive.

Video podcasts like Hak5 provide hands on instructions on a wide range of topics, from network security to hacking digital cameras (Hak5 2009). Further, uninformed individuals and enterprise end-users can unknowingly cause damage through their careless propagation of malware.

With twenty-four hour broadband Internet access and improvements in electricity supplies to both homes and businesses, the number of idle, improperly secured computers will rise. These are exactly the types of machines that are sought after by experienced hackers and those trying to develop and hone their skills.

We suggest that these factors, in conjunction with the ingenuity and increasing comfort in the use of computer systems and their availability, will foster an increase in the skill and numbers of the home-grown Jamaican hacker. It is an issue that deserves greater attention.

Corporations, government agencies and end-users must all be aware of the potential to be targeted. Security must be elevated to the importance it now demands when developing, purchasing, distributing, publishing and using software systems.

References

BBC 2008. Malicious Programs Hit New High .Available from http://news.bbc.co.uk/2/hi/technology/7232752.stm

CITO 2009. National e-Readiness Status. Available from http://www.cito.gov.jm/content/national-e-readiness-status

Hak5 2009. Available from http://www.hak5.org/about

Jagatic, Tom N., Johnson, Nathaniel A., Jakobsson, Markus, and Menezer, Filippo, 2007. "Social Phishing", *Communications of the ACM* (50:10), October, pp. 94-100.

Stallings, W. and Brown, L. 2008. *Computer Security:Principles and Practice,* Upper Saddle River, NJ: Pearson Prentice Hall.

Tiller, James S. 2005. *The Ethical Hack:A framework for business value penetration testing,* Boca Raton, FL: Auerbach Publications.