Web Apps Security 2019: *Analysis of Malware Samples and Code Injections Vulnerabilities in Tanzania Cyber Space*

Geofrey Kilimba

General Introduction

Malware is one of the most serious security threats on mobile devices [1], electronic medical devices [2], and the Internet [3] as a whole. Spam e-mails, phishing SMS, malicious internet links and denial of service attacks have malware as their underlying cause. Criminals are using malware as their financial gain by circulating Ransomware – a malicious software designed to block access to a computer system until a sum of money is paid. State sponsored hackers are using malware in the form of spyware – a software that enables a user to obtain secret information about another's computer activities by transmitting data secretly from their computer systems. In order for a malware to successfully infect an electronic device or a particular web application, there must exist some kind of security vulnerabilities in them; the most common vulnerability exploited by hackers to inject malware is code injections [4] exploitation. Code injection is a result of poor programming in computer (or mobile phone) application hence making it send untrusted data to an interpreter.

Malware are spread in many ways, the most common method that makes them spread worldwide is drive-by downloads – these are downloads that occur without a user's consent while visiting infected websites, opening malicious email attachments or clicking phishing links on the internet or on social media[5]. Malware can be designed to target certain computer, application service (like control systems, nuclear plants [6], power grids, financial services) or a particular cyber space [7] (example *xxx.tz* space). When malware samples are spotted, it is important to analyze them and uncover their origin and modus operand. The analysis should be extended to how did the malware land in our cyber space; are our web applications not secure enough? What kind of vulnerabilities do exist in them? This research is all about analyzing malware samples existing in Tanzania. In the course of study, the state of web application security will be examined to see how likely they support for malware hosting and spread. While malware samples will be examined using reverse engineering software packages, Web Applications will be tested using Penetration Testing Methodologies.

B. Statement of the Problem

B.1. General Overview

Ransomware – malware that cyber criminals use to lock computers and then ask for money before they reopen them, has been found to circulate in Tanzania cyber space for the past few years. Although institutions are reluctant in declaring publicly that they have been cyber attacked, cases of ransomware which have been found in Tanzania includes WannaCry (was observed in one major Hospital, some local banks and academic institutions) and SAMSAM ransomware which was observed in some institutions (public and private). The TZ-CERT has been issuing notices and alerts on these kinds of malware. According to one of the TZ-CERT [8] notice, SAMSAM exploits web-based JBoss Applications; this is to say the success of SAMSAM depends on security weaknesses in web applications. This is indeed the case for all kinds of malware.

B.2. Problems Leading to Successful Injections of Malware.

The two most famous scripting languages used in programming websites are Hypertext Preprocessor (simply **PHP**) and Active Server Pages (ASP). If website programmers do not carefully sanitize input parameters that are inputted by users in a particular application, that will cause the application to process invalid data and may allow for code injections. Injection flaws can be found in SQL, LDAP, OS/Shell commands, XML, SMTP headers, etc. When a website (or web server) has code injections vulnerability it is possible to inject malware in that site. Unfortunately, preliminary observations shows that there exists cases of web applications allowing code injections.

B.3. Various Malware (Including Ransomware) cases in Tz

When visiting internet café it is common to get infected with computer viruses. Some of these viruses are actually Trojan horses or spyware. A Trojan horses are types of malware which hide their true intents; they can be used as backdoors (for stealing information) or as ransomware (for cybercrimes and money theft) or as computer worms (for gathering computer activities). Preliminary observations spotted the following types of Trojan horses; Trojan:BAT,

HackTools:/MSIL and MonitoringTools:Win32. Also, early this year, cases of SAMSAM and WannaCry ransomware were spotted in several public institution

B.4. Mobile Phone Malware

People using smartphones, especially those with android operating system are frequently complaining of their devices draining charge rapidly, being unusually slow, restarting unexpectedly and freezing. Some users even complained that once they buy air time bundles, the air time finishes "ünproportionally" to the time they bought. All these are symptoms of mobile phone malware.

B.5. Financial Malware

Tanzanian banks, financial institutions, the Tanzania Revenue Authority (TRA) and Municipals are using web based technologies in financial transactions. These technologies are prone to malware attacks if not properly configured. Cases of ATM malware[9] that targets banks has been on the rise worldwide and becoming sophisticated[10]. Also, attacks against fiscal devices like PoS are increasing as well.

C. Research Objectives

C.1. Main Objective

The main objective of this research is to propose a solution that will mitigate security weaknesses that course malware spread in Web Applications.

C.2. Specific Objectives

1. To examine the security of Web Applications for websites in the Tanzania cyber space
2. To study the presence of mobile phone malware in Tanzania's cyber space
3. To study the presence of malware in websites that provides services for Tanzanians
4. To reverse engineer malware samples for the purpose of uncovering their modus operand
5.

D. Significance of the Research

In this research, a solution to detect code injections will be laid down. The results of the research will be helpful to the following:

1. Agencies that deals with Combating cyber criminals, cyber spies and cyber terrorists.
2. Internet Service Providers will add knowledge in dealing with malware in their systems.
3. Findings will add knowledge to the Bank regulatory authority in studying financial losses which are a result of security weaknesses in websites and web applications servers.
4. Academic institutions will find out which areas to concentrate in teaching programming and cyber security related topics
5. Policy makers will be in a position to establish relevant and exact security awareness training among Tanzanians in the best and secure use of electronic devices to avoid leakages of sensitive information, privacy intrusion and money (mobile / online banking) theft.

E. Research Scope

The research will be based on websites that offers services to Tanzanians. Also, selected mobile devices will scanned for malware samples.

F. Literature Review

F.1. Malware and Malware Analysis

As researchers, we perform malware analysis in order to understand how malware behaves and the latest techniques used in its construction. According to the definition provided by Wikipedia (https://en.wikipedia.org/wiki/Malware_analysis) malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor.

The process of analyzing malware follows steps used in reverse engineering software applications in which two approaches are usually deployed: Static and Dynamic analysis.

- S**tatic analysis.** This is the process of analyzing malware or binaries without actually running them. It involves the disassembly or DE compilation of malware code to symbolic execution, which is something like virtual execution of a binary without actually executing it in a real environment.
- In **dynamic analysis** we analyze a piece of malware while running it in a real time. The behavior of the malware and its side effects are carefully observed in the course of this action.

F.2. Web Apps Security Overview

Web App security involves the process of examining whether it is free against all sorts of attacks that may result in the disclosure of users' Confidentiality, Integrity of information being exchanged and systems Availability. For a website (or web App) to be secure it has to be configured that it does not allow code injections and unintended scripting (like Cross Site – XSS) and also has to have properly installed cryptographic cyphers to minimize the risk of man in the middle attacks.

Improperly defining character sets an "unsanitizing" inputs while designing web pages are the main course denial of service (DoS) attacks and SQL injections. Systems downtime (unavailability) is the best example of DoS attacks. Unfortunately, we have many cases of service downtimes especially in banks operating in Tanzania.

G. Related Works

This work is similar to a pierce of research work done by Clemens Kolbitsch et al [11] when they investigated a number of compromised drive-by download exploits web sites in order to develop a novel malware detection approach that is both effective and efficient, and thus, can be used to replace or complement traditional anti-virus software at the end host.

Also, in year 2017, David Korczynski and Heng Yin [4] presented a unified approach to tracing malware propagations inside the host in the context of code injections and code-reuse attacks. Their paper titled Capturing Malware Propagations with Code Injections and Code-Reuse Attacks demonstrated the first approach to identifying dynamically generated code based on information-flow analysis. It implemented techniques in a system called Tartarus and match Tartarus with both synthetic applications and real-world malware.

H. Research Design

H.1. Methodology

This is an *applied research* [12] which aims at finding a cyber-security solution for web applications that exchanges sensitive information and financial related data in Tanzanian. The research will be *Descriptive* whereby surveys and fact-finding enquiries utilizing penetration testing techniques will be deployed. As such, this study will be a laboratory based research work.

A survey of selected websites will done and observed if they host malware applications. Two approaches will be used in the detection of malware in such websites; One is scanning with open source tools and online website that offer malware scanning. Two is configuring our laptops and make them detect drive-by downloads and later scan them for malware. The detected malware will then be:

- Statically analyzed using Ghidra Reverse Engineering tool
- Dynamically analyzed using sniffing tools like Wiresharks
- Malware detection sensors will be deployed to networks that we'll agree with.
- Selected websites will be checked for code injections. The process of checking for code injection will be non-intrusive and will abide to ethical hacking methodologies.

H.2. Materials and Tools

The research will make use of open source software and hardware. Some of these tools will be purchased, for example Reverse Engineering Software packages.

Making use of Python language and other necessary Linux based scripting languages, a malware analyzer prototype will be built.

H.3. Research Costs **:** USD 10,000.00

H.4. Research Duration **:** Twelve Months

H.5. Proposed Start Month **:** October, 2019

H.6. Sampling

Website, Mobile phone handsets, and Internet café selection will be done at random. However, the selection of website will cover the following categories:

- ✓ Sites that offer financial services
- ✓ Academic institutions
- ✓ Media
- ✓ Blogs
- ✓ Government
- ✓ Telecoms
- ✓ Insurance firms
- ✓ Health and Medicare

Appendix: About the Researchers:

Full Name: Geofrey Appolinary Kilimba

Contacts:

Email: aarsc@aasecure.co.tz

gkilimba@gmail.com

Mobile: 0715 362 886 (WhatsApp only) 0652 587093 (normal calls)

A Masters Degree holder (MSc. Digital Electronic) offered jointly by the University of Sussex and the University of Brighton in the UK. He graduated his masters degree in year 2003. His master's project was based on the applications of Artificial Intelligence in Computer Vision.

In year 2001, Geofrey attended courses on computer security and awarded a Certificate in Ethical Hacking from South African based security Research Institute – **Sense Post.**

In 1995, he graduated a first degree – BSc. (Hons) In Electronic Science and Communications at the University of Dar es Salaam.

Since graduation, Mr. Kilimba spent much time researching on Information and Communications Security Technologies. His last research work is on The State of Website Security in Tanzania which was uncovering security vulnerabilities existing in Tanzania cyber space. The report can be accessed at the Commission for Science and Technology - COSTECH.

Currently, his research works are based on cryptographic systems, GSM vulnerability assessment and a continuation on the study on Website security in Tanzania – focusing on web based financial systems.

In year 2012, Geofrey founded a private firm that deals with research on ICT security. The company is called AA RESEARCH FOR SECURE COMPUTING LTD, abbreviated as AARSC LTD. The firm is on the process of establishing a cyber elite group of penetration testers that will be focusing on ethical hacking businesses.

References:

[1]: Raj Samani, Gary Davis, (APRIL 2019). McAfee Mobile Threat Report Q1, 2019: Mobile Malware Continues to Increase in Complexity and Scope.

[2]: Greer Brian, Capstone A, (2018). CYBERSECURITY FOR HEALTHCARE MEDICAL DEVICES.

[3]: Brigid O'Gorman, Candid Wueest, Dick O'Brien, Gillian Cleary, Hon Lau, John-Paul Power, Mayee Corpin, Orla Cox, Paul Wood, Scott Wallace. (FEBRUARY 2019). Internet Security Threat Report. A Report published by SYMANTEC.

[4]: David Korczynski, Heng Yin. (October 30-November 3, 2017). Capturing Malware Propagations with Code Injections and Code-Reuse Attacks. CCS Publications at the University of California, Riverside.

[5]: Wu He, (2012). A REVIEW OF SOCIAL MEDIA SECURITY RISKS AND MITIGATION TECHNIQUES. Journal of Systems and Information Technology. 14.

[6]: Hana Hamdouni, Fredrik Doeser. (2017). The digital destruction: A case study of Stuxnet within the theory of new and old wars. Publication at the Swedish Defense University - White Paper.

[7]: Kenneth Geers (Ed.). (2015). Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015

[8]: TZ-CERT. SAMSAM Ransomware Notice. https://www.tzcert.go.tz/wp-content/uploads/2018/12/SamSam-Ransomware-Security-Notice.pdf

[9]: Trend Labs. (2017). Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types. https://www.europol.europa.eu/sites/default/files/documents/public_-_cashing_in_on_atm_malware.pdf

[10]: United States Secret Service. (2018). ATM Jackpotting Attack. https://www.secretservice.gov/data/press/releases/2018/18-JAN/GPA_01-18_ATM_Jackpotting_Attack.pdf

[11]: Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, XiaoFeng Wang. Effective and Efficient Malware Detection at the End Host.

[12]: C. R Kothari. 2004. Research Methodology: Methods and Techniques. Second Edition. NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS