8-2016

An Analysis of Faculty and Staff's Identification of Malware Threats

Malora Quesinberry
East Tennessee State University

An Analysis of Faculty and Staff's Identification of Malware Threats

A thesis

presented to

the faculty of the Department of Technology

East Tennessee State University

In partial fulfillment

of the requirements for the degree

Master of Science in Technology,

concentration in Engineering Technology

by

Malora Quesinberry

August 2016

Dr. Todd Emma, Chair

Dr. Brian Bennett

Dr. Megan Quinn

Keywords: Malware, Information Technology, Information Security, Security Awareness

ABSTRACT

An Analysis of Faculty and Staff's Identification of Malware Threats

by

Malora Quesinberry

This document presents findings related to faculty and staff member's ability to identify malware threats. Research identified eight malware categories to be the most common threats to higher education systems. The impact of malware intrusions on higher education systems was provided to emphasize the importance of recognizing malware threats. The study presented faculty and staff members at a midsize southeastern university with realistic scenarios of malware threats. Results indicate malware categories such as virus, Trojan, browser hijacker, adware, and ransomware were identifiable by faculty and staff. Additionally, findings demonstrate worm, spyware, and rootkit malware categories were difficult for faculty and staff members to identify. A recommendation for educating faculty and staff members to better identify malware threats in the less identified categories was proposed to help mitigate future malware intrusions. Future recommendations include investigating new types of malware risks, student recognition of malware threats, and solutions for mitigating these risks.

ACKNOWLEDGEMENTS

I would like to thank all of my graduate committee members; Dr. Todd Emma, Dr. Brian Bennett, and Dr. Megan Quinn. I appreciate all of the assistance and guidance during the process of completing my thesis.

I also would like to thank my family for their support and patience during the time I spent on my studies and research.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION AND OVERVIEW

Can people identify malware threats? Malware attacks cost organizations time, money, and loss of sensitive data. Higher education institutions are at a greater risk for malware invasions. Exploring the areas at stake shows the importance of why there is a need to be concerned with malware threats, what is at risk, and who is at risk.

Studies have demonstrated security awareness successfully reduces malware infections and calls to technical help desks (Wombat Security Technologies, 2014). Users who cannot recognize malware threats are more susceptible of becoming victims of malware invasions. Identifying the most common incidences of user malware infections can lead to the creation of a training program to combat these occurrences. Identification of malware threats before they invade computing systems provides a more secure and productive work environment when using technology.

Malware attacks cost organizations time, money and loss of sensitive data. A medium size university can average a cost of $30,000 per year for malware remediation (Lehrfeld, 2013). This cost also includes loss of worktime and breach of sensitive data. A cybercrime report by Symantec showed attacks cost $575 billion each year (Symantec, 2016). Many anti-malware tools can aid with cleanup after infections. However, anti-malware technologies are limited to preventing malware intrusions. End-users who override anti-malware settings are more likely to fall victim to malware intrusions. Compromised security due to malware intrusions of computing systems can lead to work disruption and downtime, susceptibility of data, and in extreme cases, impact revenue.

Higher education institutions are at a greater risk for malware invasions. Higher education institutions handle several types of sensitive data, especially for students, which makes them a target for malicious hackers. A report from BitSight Technologies states that higher education institutions are at a higher risk for security breaches than the retail and healthcare industries (BitSight Technologies, 2014). With these increasing risks, higher education institutions have become more aware and concerned for keeping their data secure. While organizations use different data security methods, higher education systems such as the University of North Alabama look to add and enforce information technology security awareness training programs (Unversity of North Alabama, 2016). The University of Cincinnati, the University of Arizona, and Villanova University also require information security awareness programs (University of Cincinnati Office of Information Security, 2016); (University of Arizona Information Security Office, 2016); (Villanova UNIT, 2015).

Statement of Problems

Technological advancements make information widely and easily available over the Internet. This easy access also causes the software to be vulnerable to malware attacks. Higher education institutions are responsible for insuring sensitive organizational and member data remains secure. Higher education institutions use several technological utilities and anti-malware tools to keep their sensitive data safe on their systems and network, but case studies show that anti-malware tools by themselves are not completely effective (NTT Group, 2014). This puts data at risk and threatens to result in lost work time. Lost work time results when institutions perform damage control following a malware attack. This occurs because most institutions take a reactive approach.

Research Questions

To help determine any relationship between security awareness benefits and identifying malware threats, the following questions were used during the study:

- Can faculty and staff members identify malware threats?
- Does the amount of years of computer use affect the ability to identify malware threats?
- Does the amount of hours of daily computer use affect the ability to identify malware threats?
- Does the experience of previously being attacked by malware increase the ability to identify malware threats?

Significance of the Study

This study looks into malware identification. As higher education institutions look to reduce their security risks associated with sensitive data or malware infections, many institutions are implementing general security awareness programs to combat these risks. Cleaning infected machines requires a substantial amount of time by IT resources and impedes the effective work time of faculty and staff members. This study is significant because it uses scenarios related to the top threats in a midsize southeastern university's environment and common threats national security firms have identified.

Limitations and Delimitations

This study was limited to faculty and staff computers at a midsize southeastern university. Research was not extended to students or to other universities. The study was also limited to Windows and Macintosh operating systems, while excluding mobile or personal devices. These limitations were guided by the higher level of network access permitted to faculty or staff members when compared to student access, which is restricted from network resources with sensitive data. The university provides a separate help desk for students which could be used for future studies involving students and their technology use. Although this study was limited to one university, this research could help guide other institutions to develop their own training programs to combat stolen or lost data and worker downtime.

Malware

To gain a better understanding of the background and malicious capabilities of hackers who utilize malware, this section describes malware threat categories. Additional sections show compromised areas from the different malware categories, various infection vectors of malware, and how to detect malware infections. The final section will describe the remediation process performed at a midsize southeastern university for malware intrusions on systems.

Malware is malicious software created and used to interrupt a computer's normal operations per Merriam-Webster.com (Merriam-Webster, 2016). Malware includes different categories of threats ranging from small and less invasive threats to more disruptive threats. Less invasive threats, such as adware, can slow down a system by providing nuisance advertisements repeatedly. More disruptive threats, such as CryptoLocker, falls under the ransomware category

and can prevent a person from working. Other general categories of malware are known as worms, viruses, rootkits, Trojans, and browser modifiers (also known as browser hijackers), and spyware. The malware's design determines how it impacts or threatens a computer system and the user. To understand what can be compromised, the categories of adware, browser hijackers, ransomware, rootkits, spyware, Trojans, viruses, and worms will be described in more detail. An analysis on data breaches from 2005-2015 performed by Trend Micro shows malware as the top method of breaches in the education field (Huq, 2015).

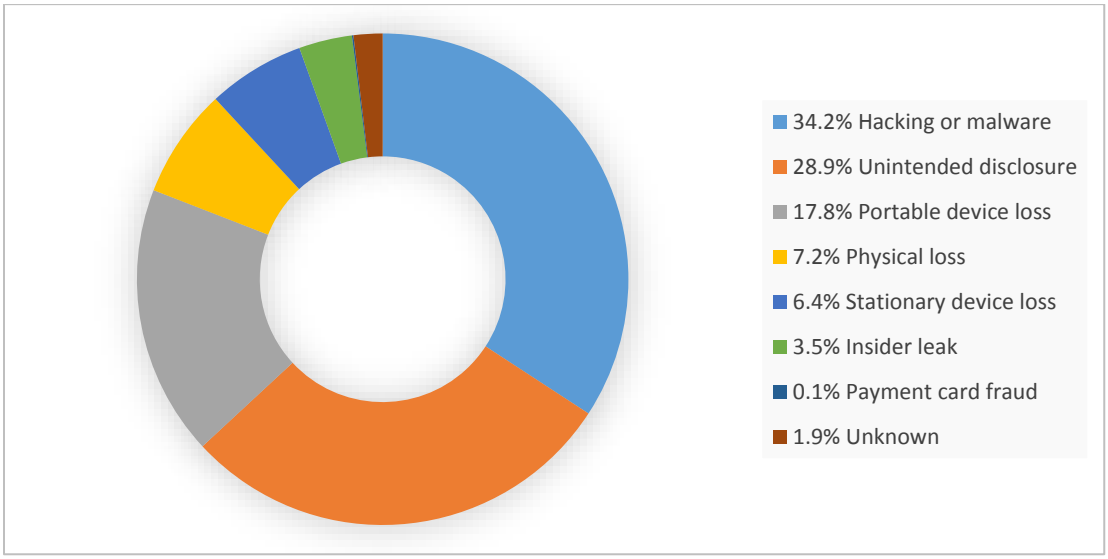

Figure 1. Adapted from Trend Micro chart of breach methods observed in education sector from 2005-2015 (Huq, 2015).

Malware Terms and Definitions

Adware. Adware is software used to show advertising that includes code to track user information and give it to the adware creator. This tracking is done without the user's knowledge. Adware causes problems if the adware has flaws in its code and when it slows down the computer by downloading several advertisements (Sophos, 2016).

Browser hijacker. A browser hijacker changes the default homepage and search engine in your web browser without your permission (Sophos, 2016). A browser hijacker affects browsing experience.

Ransomware. Ransomware is a malicious program used by attackers to steal data and keep it locked from the owner until a ransom is paid (Invincea, Inc., 2014). The most successful per Invincea, Inc (2014) is forcing users to pay a ransom for a decryption key for the encrypted data that has been stolen and encrypted (Invincea, Inc., 2014).

Rootkit. A rootkit is a software program used to hide malicious activity so antivirus programs cannot detect them. Rootkits change the operating system to disguise itself and its actions it takes on the infected computer (Kaspersky, 2016). This is different since most malware infects applications.

Spyware. Spyware is software that permits advertisers or hackers to gather sensitive information without your permission (Sophos, 2016).

Trojan. A Trojan does not copy itself like a worm. A Trojan executes on infected computers by user interaction and cannot execute by itself (Kaspersky, 2016). A Trojan can create an opening that gives malware hackers access to the computer system.

Virus. A virus is malware that infects other programs by adding a virus code and continues to spread when an infected file starts up (Sophos, 2016). A virus is dependent on a host program and usually attached to an executable file. So even if a virus is on a machine, it needs to have the executable file run by someone to activate.

Worm. A worm makes a copy of itself to spread to other computers. A worm is not dependent on a host program like a virus and uses vulnerabilities such as the auto-run feature when connecting a USB drive on a computer to access and spreads via network resources including email (Sophos,

2016).

Definitions of Additional Terms

Firewall: A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on a set of security rules (Tech Target Search Security firewall, 2016). A firewall typically establishes a barrier between a trusted secure internal network and a less secure outside network, such as the Internet (Tech Target Search Security firewall, 2016)

Domain: A group of computers on a network accessed or administered with a common set of rules (TechTerms, 2016).

Signatures: Unique identifying number for a file to serve as verification the file is what it says it is and not modified (Wise Geek, 2016).

Phishing: The act of deceiving victims into sharing sensitive information to criminals which comes in the form of an email (Sophos, 2016).

Results of Malware Infections

The various malware threats are created as a means for malicious users to either disrupt the workflow of a system or steal data. The list below briefly describes the items compromised by the particular threat if a system is infected.

Adware. Adware slows down computers by downloading several advertisements. System instability can occur if the coding for an advertisement has flaws (Sophos, 2016).

Browser Hijacker. A browser hijacker interrupts legitimate browsing activity and redirects user to either sites that benefits the hacker to increase specific site activity or can redirect to inappropriate sites or malicious sites that could cause more harm (Sophos, 2016).

Ransomware. Ransomware can steal data, lose data, and causes uses to lose money if they choose to pay a ransom to retrieve data from the attackers (Invincea, Inc., 2014).

Rootkit. A rootkit can steal passwords or other sensitive data and then send it to the hackers (Sophos, 2016). Depending on the level of access a person has to a system, databases, or network, various items can be at risk if hackers gain access.

Spyware. Spyware tracks user activity and data without permission. Spyware can also slow down or crash a computer by depleting memory and processing resources (Sophos, 2016).

Trojans. Trojans can delete information, steal data, and freeze computer systems (Kaspersky, 2016).

Viruses. Viruses can steal data, give computer control to hackers and display irritating messages (Sophos, 2016).

Worms. Worms are used to steal data, send spam, and can infect multiple machines (Kaspersky, 2016).

Infection Vectors

Malicious users or hackers normally intrude machines by finding vulnerabilities or flaws in computer software. Non-reputable websites also attempt to install malware when you visit their website. Another avenue of attack malicious hackers use when operating systems or network systems are secure, is by sending their malware in ways that users will install it by deceptive tactics. Below is the listing of how machines can become infected with each malware threat.

Adware. Adware can be installed from websites or applications that rely on ads to help fund their sites or apps. These can be legitimate or reliable sites but may have an advertisement that has been infected (Kaspersky, 2016).

Browser Hijacker. Browser hijackers are hidden in coding on a webpage or link. They are also bundled into an installer like from Download.com. Malicious software such as Search Protect by Conduit is bundled and installed with free software downloads from Download.com (Krebs, 2016).

Ransomware. Ransomware infects computers of individuals who visit suspicious or compromised websites, click on malicious links in emails, or click on an infected advertisement (Symantec, 2016).This type of malware can also spread through network shares.

Rootkits. Rootkits infect through system vulnerabilities or retrieved login information from a successful phishing attempt (Symantec, 2016).

Spyware. Spyware is often installed by prompting the user to download a falsely needed utility and then hides itself in that download (Sophos, 2016). Spyware also finds a way into machines via email messages or spam, instant messages, and direct file-sharing connections (Symantec, 2016).

Trojan. Trojans can be found in video codecs to view online videos, fake game downloads, or pirated software (Sophos, 2016).

Viruses. A virus can attack through users opening infected email attachments, USB drives, or from the Internet when downloading music files and the virus is attached (Sophos, 2016).

Worms. A worm attacks through emails, email attachments, files shared from peer to peer networks, instant messages, and phishing exploits (Kaspersky, 2016).

Detection of Infections

These infectious items are found by the abnormalities seen in a computer system for each type of malware threat category. Additional detection methods include the use of anti-malware tools alerting of the infection and user suspicion towards an action being requested of them.

Through investigation using an incident reporting database used by a technology Help Desk, users reported several examples of detection of malware on their computer system.

One user noticed the proxy settings for the Local Area Network connection continued changing and set to use a proxy server. A proxy server is not needed or used for this organization to access the Internet and this displayed an example of a rootkit intrusion. Another user detected her computer infection after receiving a message that her data would not be accessible until receiving payment and then an encryption key would be sent. It was determined the infection was an example of a ransomware infection named Cryptowall and arrived through a fake update for Adobe Flash Player. Symantec, a technology security company, notes that this specific malware can also invade through deceptive emails with attachments that appear to be for an invoice or a packaging company (Symantec, 2016).

Detection of a malware infection has also been discovered while a user attempting to use a web browser notices his homepage has changed and is unable to change it back to his preferred default page. In addition to being unable to change the web browser homepage, the user was able to identify that a new shield in the bottom right corner of the computer screen appeared to look like an anti-virus program but not the usual anti-virus program. This particular instance was an example of a browser hijacker variant named Conduit Search Protect.

Another similar detection involved a program that occurred after a user attempted to download a video file converter from what he thought was a reputable site. Instead of receiving a legitimate video file converter, he began to see a program covering his screen named PC Optimizer Pro download and state it found over 1500 serious infections after analyzing his computer. The user was certain that many infections did not exist and reported the incident to the technical Help Desk to be removed. Each of these incidents were experienced by faculty and

staff members that could not proactively identify the malware threat. Each infected computer system required remediation to remove the threat.

Cleaning/Remediation Process

This next section is a brief overview of the process involved when a malware incident is reported to an organization's technical Help Desk.

An incident or issue is first reported to the technical Help Desk. If the issue is not resolved by the initial Help Desk technician contacted due to time constraints or difficulty of issue, the issue is escalated to the next level of technicians. The next level of technicians may require a site visit to access the computer. Some access to a computer system can be performed remotely over a network connection, but if that network connection is disabled for the infected system, a remote remediation is not possible. Once the system is accessible by the technician, removal of the infection can be accomplished by manually removing the infected files or programs, removing malicious coding, or removing registry entries if the area of corruption can be easily identified. A repair to a program that has been infected may also be necessary. Depending on the severity of the infection, some anti-malware tools can be utilized to remove the infections automatically after scanning a system instead of needing to manually clean the infection. Even when anti-malware tools are used to remove an infection, a technician must still manually reset the infected program back to its default working condition. Different issues warrant different remediation methods. In a situation where data is encrypted, a restoration of the data can be processed if the original data was backed up to a separate storage location. In some cases, a computer system rebuild may be necessary. A computer system rebuild requires data backup, reinstallation of software for the operating system, programs such as Microsoft Office, proprietary applications, and restoring or transferring the user's data files. Some systems, like

mobile laptop devices, include encrypting hard drives as part of the rebuild process. This type of encryption is performed for security purposes and stores an encryption key. The number of hours a midsize university spends remediating a malware infection is close to 571 hours a year (Lehrfeld, 2013).

As mentioned previously, anti-malware tools are used to clean infections and some can be used as a preventive measure, but anti-malware tools are not a catchall. Technology is ever changing to increase user enhancements, causing new vulnerabilities. There are also several scenarios where users inflict their own damage because they are unable to identify malware threats.

Recognizing and understanding what types of information hackers or thieves target and how they threaten these items should encourage people to be more cautious and protect sensitive data. If people can identify the ways thieves or hackers might try to retrieve sensitive information, it could reduce the risk of infections and data loss. If users can understand how the problem occurred, they may be able to prevent the problem in the future. Identification can also help with the cleaning process of the infection if one does happen. Work time that is normally lost during the infection and remediation process could be saved.

CHAPTER 2

LITERATURE REVIEW

The literature summaries below discuss a combination of limitations, risks, and scenarios demonstrating why the higher education sector is a huge target, how end users have been identified as a root cause of infections, and why assessing multiple factors of risks and combining them is needed to create a successful awareness program. The first section reviews limitations of only using anti-malware technologies to mitigating malware intrusions. The second section provides examples of institutions of higher education with recorded information technology security risks. The third section shows how end users have attributed to causes of malware intrusions in regards to their actions with information technology in the higher education environment. The final review covers key items needed for an effective security awareness program and how to measure the effectiveness.

Limitations of Only Using Anti-Malware Technologies

The literature provides reports where anti-malware technologies have failed to capture all instances of malware. These reports describe the characteristics how malware is capable of eluding anti-malware protection tools. Reports provided by technology companies, SANS, Symantec, Webroot, and the NTT Group, will reflect on their research regarding anti-malware technologies and cyber security threats.

SANS, a technology company that handles information security training, certification, and research, pointed to anti-malware technology tools' deficiencies due to the quick advancement and modification of new malware threats. Firewalls are using blacklists and known

malicious domains or sites based off community forums, but since malware changes domains quickly, it is impossible to block everything (Faust, 2011). SANS reported a major exploit is through browsers and identifies why this is a popular method of attack for hackers.

Malware signatures used to identify specific types of malware are not available for all malware threats. A common threat able to avoid detection by anti-malware tools is a Zero Day attack, since this type of attack consists of a newly developed malware threat that has not yet had an identifiable signature (Faust, 2011). Many anti-virus programs are limited because they rely on known malicious signatures databases and, if the malware does not match a known signature, it bypasses the anti-virus program. SANS also concentrated on web browser attacks identified as a popular avenue of attack since there is a large frequency of use of web browsers. The exchange of information online is more valuable and the attack can be automated without any interaction from the client it is attacking (Faust, 2011). SANS also noted that technology users are a concern and can enable threats. The use of social engineering such as phishing, has become a large threat and deceives technology users into releasing important credentials and other information. SANS also reported technology users will often click past a warning message that might be legitimately provided by the IT department because of inconvenience to the user (Faust, 2011).

NTT Group researchers reported anti-malware technologies failed to detect 54% of new malware that takes control of systems and 71% of malware intended to make money for hackers (NTT Group, 2014). Part of NTT's 2013 research identified the education industry as a prime target for malware infections and relates this to educational environments need to make information easily available and the large amount of users connected to the Internet (NTT Group, 2014). The research group also analyzed several anti-malware tools manufactured by different companies and discovered multiple malware threats were not detected by these tools (NTT

Group, 2014). The case studies compiled by NTT Group demonstrated the vulnerabilities organizations have even if they utilize anti-malware tools and discuss the need for user education and training involving technology.

One case study revealed an event in July 2013 where a company became infected with a malware worm. The cause was attributed to an administrator with infected software on a USB device unknowingly uploading the infection. Many of the server systems did not have updated anti-virus signatures installed or some servers were missing anti-virus software completely. Since infections continued for three additional months after the first detection, the cost accrued for damages, investigation, and clean up equaled to $109,000 (NTT Group, 2014). The study also concluded that educating and training users can help to prevent malware infections as this case demonstrated the result of user action.

Another case study expanded on the attack from a Zero Day infection and the anti-malware tools that failed to prevent it. Since the infection was caused by a Zero Day infection, malware signatures or footprints were not available for anti-malware tools to detect it. The cause of infection was traced back to a phishing scam against multiple employees to browse infected websites controlled by hackers. The reported cost of this event was $9,717. This study showed an additional reason to educate users for safe technology use to prevent future malware attacks (NTT Group, 2014).

A report gathered from a Symantec White Paper on “The Ongoing Malware Threat” documented three billion malware attacks on users in 2010 and incurring high costs due to stolen credit card information and costs for remediation of the attacks (Reavis, n.d.). The report revealed that by design many tools are developed to concentrate on certain areas of technology systems reinforcing the idea of limitations in anti-malware tools. The whitepaper noted single

computing systems, servers, or websites are separate entities of risk and that a single anti-malware tool is not designed to eliminate threats across all of these. Another comparison is an anti-virus tool versus an anti-spyware tool. A couple of examples provided were anti-virus software not capable of detecting spyware and the second example being computer protection tools are not the same as website protection tools. A solution to use GeoTrust's anti-malware scanning tool was recommended.

"The Ongoing Malware Threat" report's main focus was the recognition of vulnerabilities in web browsers as GeoTrust, an Internet security company, does manufacturing for anti-malware scanning technology to protect websites. Although website threats were a main focus, GeoTrust does recommend a security approach that encompasses all platforms of devices and different malware categories.

Dancho Danchev (2012), an author for Internet security organization Webroot, discussed limitations of anti-malware tools based on a reactive approach instead of using a proactive approach. Danchev (2012) described the current approach of identifying and preventing threats. The current technique uses anti-malware tools utilization of out-of-date tools and signature-based threat detection (Danchev, 2012). Signature-based threat detection involves discovery of a new malware variant, then a vendor of an anti-malware tool creates a new signature to protect against the new threat, then after the vendor confirms the protection works, it is passed along to customers as an update to the anti-malware tool. The storing and updating of malware signatures also causes computer slowness and involvement of users to update their anti-malware program. Needing users to interact and be responsible to update their anti-malware programs increases risk. Webroot's solution is the creation of a new proactive approach. The proactive approach

uses a method of detecting malware threats based on behavior and analyzing files to identify what they are attempting to do (Danchev, 2012).

Higher Education Information Technology Security Risks

Existing literature also discusses security risks in the higher education sector. The first two are related to the information technology risks for higher education systems.

In 2014, REN-ISAC reported several universities that were targets of malware attacks including phishing scams to steal credentials. Western Michigan University, Boston University, Texas A&M, University of Iowa, and the University of Michigan were listed as universities with documented attacks (REN-ISAC, 2014). This particular report provided by REN-ISAC covered phishing campaigns to target faculty and administrators at universities and colleges. It also focused on tactics using the term salary to entice users to click malicious links. The report described the appeal of attacking a university or college. The documentation included the appeal of attack to the institutions due to ease of accessibility of finding contact information for targets and the vast information available online related to the institutions' technology (REN-ISAC, 2014). REN-ISAC is an organization made up of members in research and higher education communities and recommended educating end users by providing real world techniques used such as a phishing email for prevention.

Higher Education institutions are noted to be large targets of malware attacks because of open access and lower security limitations for research purposes. Findings by the NTT Group reported higher education systems have been impacted by 42% of malware attacks compared to other industries which account for the other 58% of malware attacks (NTT Group, 2014). Higher education institutions have also been attributed to higher malware attacks since they have a large

number of people connecting with personal, possibly unsecure devices to a network (NTT Group, 2014).

Actions of Information Technology in Higher Education Environment

Other studies show the additional challenge higher education sectors have with combatting malware threats. A University of Nebraska study presents how higher education institutions have responded to campus data security threats by mobile devices. This study addresses policies and procedures, balancing security and accessibility, and ways leaders can proactively handle security challenges of mobile devices. Four higher education institutions interviews with IT professionals and faculty were performed to show what institutions were doing currently for security measures, which policies and procedures are in place, and what higher education should do in the future.

The examples presented demonstrated the careless actions of professors while using technology. These actions also show different strategies hackers use to target their unaware victims. One example described a professor using an unsecure network at a coffee shop and not realizing the professor was on a hacker's network. The professor accessed university information such as email, grades, and even checking her personal bank account information. Because she was not on a secure network provided by the coffee shop, university data was compromised. Another scenario described a staff member saving all of his passwords on a tablet instead of remembering them because of the difficulty of the different password complexities for various applications. His daughter then used the tablet to access the Internet and the next day, he noticed his email with confidential information was accessed and files moved. A third situation involved downloading an application on a smartphone that claimed the ability to access university

resources. The application was not from a respectable source and a hacker was able to use a malware program to capture her username and password. This story relates malware installation. Additional stories were provided in the study and demonstrated users of technology with convenient access to the Internet through mobile devices assuming they were as secure as using a stationary device or were not aware of safe Internet browsing techniques.

The key findings identified end users as the highest security threat with faculty and staff users presenting more risk than students (Gordon, 2015). The interviews discussed the key concepts for where and how to concentrate their future efforts to mitigate the security risks. Among these were creating security awareness programs, frequent communication of security initiatives by the higher education institutions and IT department, shifting concentration on protecting the data at the source instead of protecting the device accessing it, and the need to maintain balance of user access with security so the mission of higher education is still accomplished (Gordon, 2015). Institutions also need to encourage end users to remain vigilant about security by understanding its importance. The study also provided research by CDW-G determined user education was the number one defense against security breaches (CDW Government Inc., 2009; Gordon, 2015). Justifications for preventative measures were also shown by the high cost of remediation when a breach does occur.

As a guidance for the type of training, the research showed the most popular form of training is digital, such as online training, website educational materials, and emails. Training should be presented in a positive manner. McElroy and Weakland (2013) and Gordon (2015) recommended that institutions should measure their success of security training to determine if their methods of training are working. Another tip presented that training should include how to detect a breach and then the how to handle it (Gordon, 2015; McElroy and Weakland, 2013). The

study also mentions future research to examine actual security breaches to focus on the highest security risks and addressing those since it is overwhelming to address all risks (Gordon, 2015). Policies should not simply limit a person's use of technology but should be created to guide safe use and demonstrate the balance between security and accessibility.

The study performed by Chiwaraidzo Judith Nyabando involved assessing behaviors of faculty and staff's understanding of potential risks to information security. This study included faculty and staff from two institutions, East Tennessee State University and Milligan College. The study's key findings demonstrated that users of computers for more than 20 years appeared to have safer habits than less than those with less than 20 years of user experience (Nyabando, 2008). Some of the behaviors attributed to users becoming victims of phishing emails and poor password management. Results from the study's awareness and practice scores discovered faculty and staff members are aware of information security issues and safe computing practices but did not always practice safe computing behaviors (Nyabando, 2008). The study summarized that awareness and training programs at both institutions were optional.

A case study by Wombat Security Technologies showed that employee education at a global manufacturing company reduced malware infections by 46% (Wombat Security Technologies, 2014).This education involved training employees to recognize malware attacks. The study emphasized the savings from the education program which included saving money by reducing malware infections, help desk calls, and costs associated with remediation of malware (Wombat Security Technologies, 2014). The next section provides more details of the Wombat Security Technologies' case study and its findings.

Measuring the Effectiveness of a Security Awareness Program

Wombat Security Technologies provided a presentation in February 2015 listing five reasons a security education program was not working, ten learning science principles, a continuous training methodology and case studies. They found human error was the reason for 95% of security incidents in 2013 (Wombat Security Technologies, 2015). The 5 reasons listed for failed security education programs were;

- Training occurs only once per year
- Training relies on video or slides
- Training tells the end user what to do but not why
- Training sessions are longer than 15 minutes
- Training focuses on awareness of threats, but not behavior change.

The solution involved creating training programs that were educational not just informational. The solutions offered involved explaining why something is a threat and then provided what actions were needed for protection. It was recommended to keep lessons to ten minutes or less and simplify topics so the audience can absorb the information in the lesson. The next recommendation covered reinforcing lessons with repetition and practice throughout the year instead of just a once. Wombat Security Technologies (2015) stated training should involve simulations to provide teaching opportunities or creating relatable scenarios such as threats when receiving emails. The report by Wombat (2015) also noted the training program should provide feedback after the practice sessions. Allow users to complete the training at their own pace such as with web-based training and repeat the training if the user wishes. Another tip is to teach through a story. To measure the effectiveness of the training, Wombat suggested assessing

knowledge gained after each training starting with a baseline of the initial training and then continue to assess annually (Wombat Security Technologies, 2015).

Wombat's case study of a manufacturing company consisted of using phishing emails. Starting with a baseline showing 32 calls a month related to malware with 70 infections per day worldwide, the company wanted to reach the goals of reducing malware infections, increase awareness of phishing attacks, and prove to the board this could be accomplished through security awareness and training (Wombat Security Technologies, 2015). In the case study, the manufacturing company reported their education program involved voluntary training at random scheduling to 5000 employees worldwide with mock phishing attempts. The company stated they were getting the support from their board because they could show results of the training. The results proved a reduction in malware infections and calls to their help desk. Due to their successful training program, they also reached results that were not listed in their original set of goals with positive user feedback on their training and showed a 700% return on investment based on remediation costs (Wombat Security Technologies, 2015). The company planned to improve their training program by migrating to mandatory training and additional training modules.

CHAPTER 3

METHODOLOGY

The objective of this study was to establish whether faculty and staff could identify malware threats that cause disruption in computer use or loss of sensitive data. The study included participants of faculty and staff members employed at a midsize southeastern university. Using the most frequent types of infections encountered by faculty and staff would help determine the categories of malware threats required in a training program. As stated in the University of Nebraska Lincoln study by Gordon, research should look at actual breaches (Gordon, 2015). The methodology listed below indicates where investigation of real malware breaches was used to identify the most common malware threats.

Research Design

The study evaluated staff and faculty members and their ability to recognize malware threats. A questionnaire involving various real-life scenarios for eight different categories of malware threats was used to find out whether the employees could identify the various malware threats. These eight categories of malware; adware, browser hijacker, ransomware, rootkit, spyware, Trojan, virus, and worm were based on research regarding the most common threats reported by multiple cybersecurity and endpoint security companies such as Sophos, Kaspersky, and Invincea. An incident reporting database maintained by the university was also used to confirm the most common malware threats. A quantitative methods research approach was used for this study. The quantitative research method was used to support the measurement in determining staff and faculty members' identification of malware threats.

Quantitative Methods

Population

The population of this study targeted faculty and staff members at a midsize southeastern university that included an estimated 2,296 employees made up of full-time faculty, adjunct faculty, full-time staff, and part-time staff members. Employees with a valid employee email address were invited to participate in the study. Approval to deliver the survey to faculty and staff members was granted by the university's Institutional Review Board.

Data Collection Procedures

Data collection was accomplished via a questionnaire to faculty and staff members. Survey Monkey, an online platform, collected all responses. The questionnaire was available for three weeks. The table in Appendix A, contains the various scenario questions and the corresponding malware category. The data retrieved from the questionnaire was then analyzed for this study.

Research Questions and Data Analysis

Quantitative data was analyzed to form an answer to the following questions.

Can faculty and staff members identify malware threats?

To evaluate this question, the percentage of correctly identified malware per number of respondents was calculated for each category of malware.

The following research questions attempted to show any additional factors that affected faculty and staff members' ability to identify malware threats.

Does the amount of years of computer use effect the ability to identify malware threats?

The comparison between the reported years of use by a person and successfully identified malware was calculated by using the percentage of correct responses per malware category and the number of years of used to find a relationship, if any.

Does the amount of hours of daily use of a computer affect the ability to identify malware threats?

The reported hourly daily use by a person and the comparison of successfully identified malware was calculated by using the percentage of correct responses per malware category and reported hours of daily use to find a relationship, if any.

Does the experience of previously being attacked by malware increase the ability to identify malware threats?

The assessment to find whether a relationship existed between faculty and staff members who have been victims of malware attacks and the ability to identify malware threats was calculated by the percentage of the respondents who correctly identified each malware category.

CHAPTER 4

DATA ANALYSIS

The study involved 98 participants that responded to the questionnaire. 48% of participants have used a computer for over 25 years. Over 69% of participants have been a victim of a malware attack. Five to six hours is the highest number of hours reported for daily computer use. The Years of Computer Use table below depicts characteristics regarding the faculty and staff population and shows the number of years participants have used a computer and how many hours of average daily computer use. The table also lists the percentage of victims of malware attacks compared to the number of survey respondents.

Table 1:
Years of Computer Use

	Participants	**%**	**N**
Years of Computer Use:	1-5 Years	1.0%	1
	6-10 Years	1.0%	1
	11-15 Years	6.1%	6
	16-20 Years	20.4%	20
	21-25 Years	23.5%	23
	Over 25 Years	48.0%	47
Average Daily Computer Use:	Less than 1 hour	0.0%	0
	1-2 hours	3.1%	3
	3-4 hours	13.3%	13
	5-6 hours	30.6%	30
	7-8 hours	25.5%	25
	8 or more hours	27.6%	27
Victims of Malware Attack:	Yes	69.8%	67
	No	30.2%	29

Note: Two participants did not respond to the survey question asking if he/she was a victim of a malware attack.

Figure 2 shows each category of malware and the percentage of participants who correctly identified the malware threat.

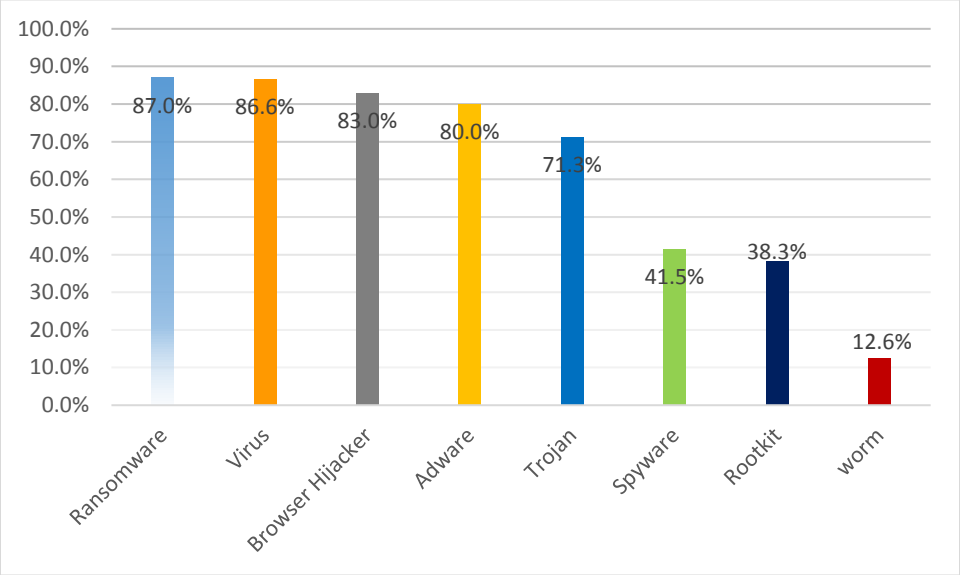

Figure 2: Amount of Correctly Identified Malware by Faculty and Staff

The number of years a person used a computer was compared to the percentage of malware they could identify. Figure 3 shows the percentage of identified malware per malware type and each grouping represents the number of years of use. The results from 1-5 Years and 6-10 Years were removed since there were not enough respondents to provide meaningful data.

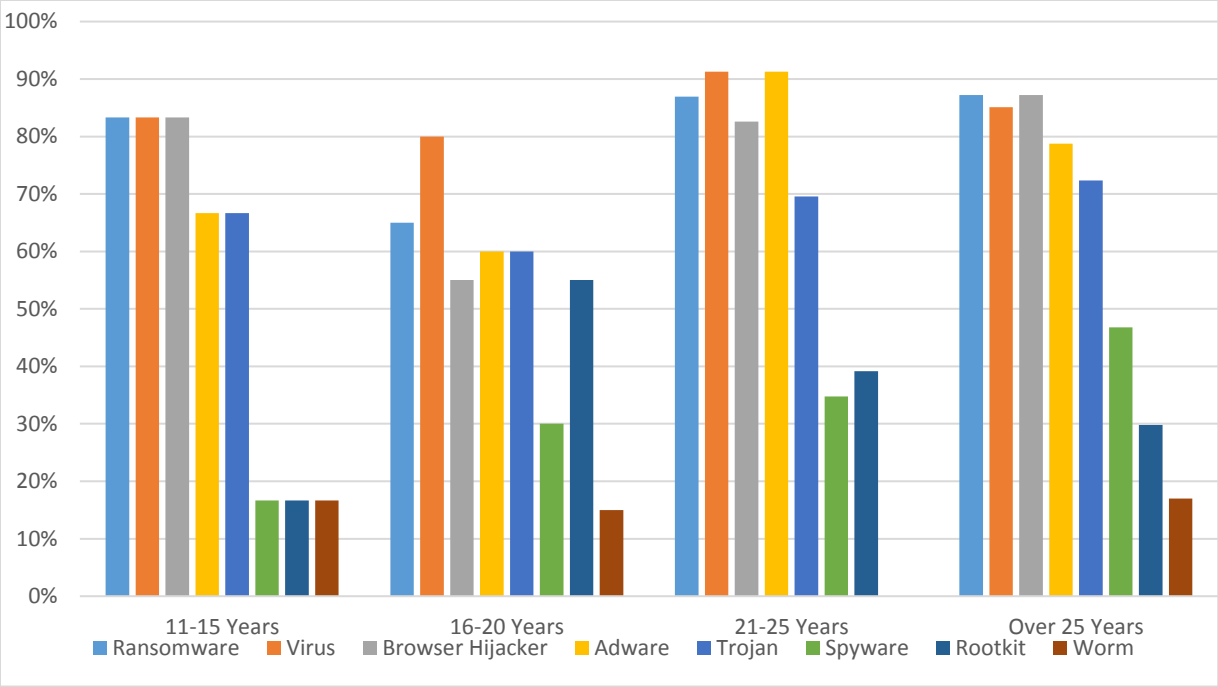

Figure 3: Percentage of Identified Malware per Number of Years of Computer Use

The hourly daily use by a person was compared to the percentage of malware they could identify. Figure 4 shows the percentage of identified malware per number of hours of use and each column represents a malware category. The results from "Less than 1 hour" were removed since there were not enough respondents to provide meaningful data.

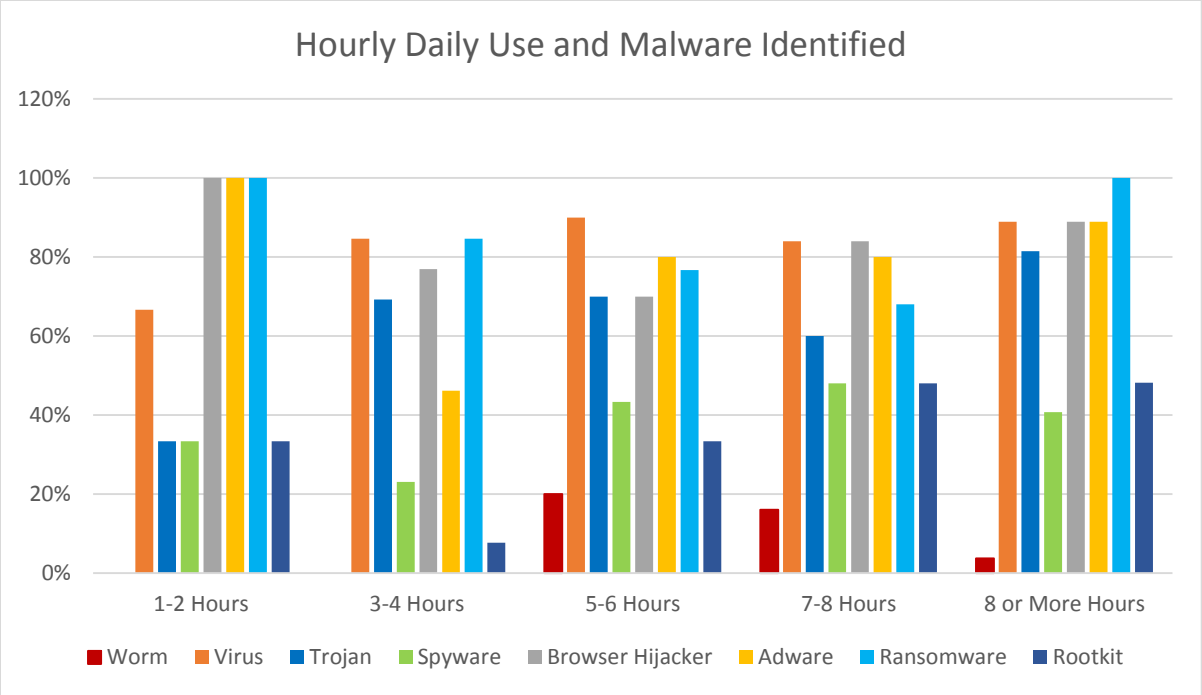

Figure 4: Hourly Daily Use

The number of respondents who reported they were victims of a malware attack was compared to the number of malware categories they could identify. Figure 5 shows the percentage of victims that could identify each malware category.

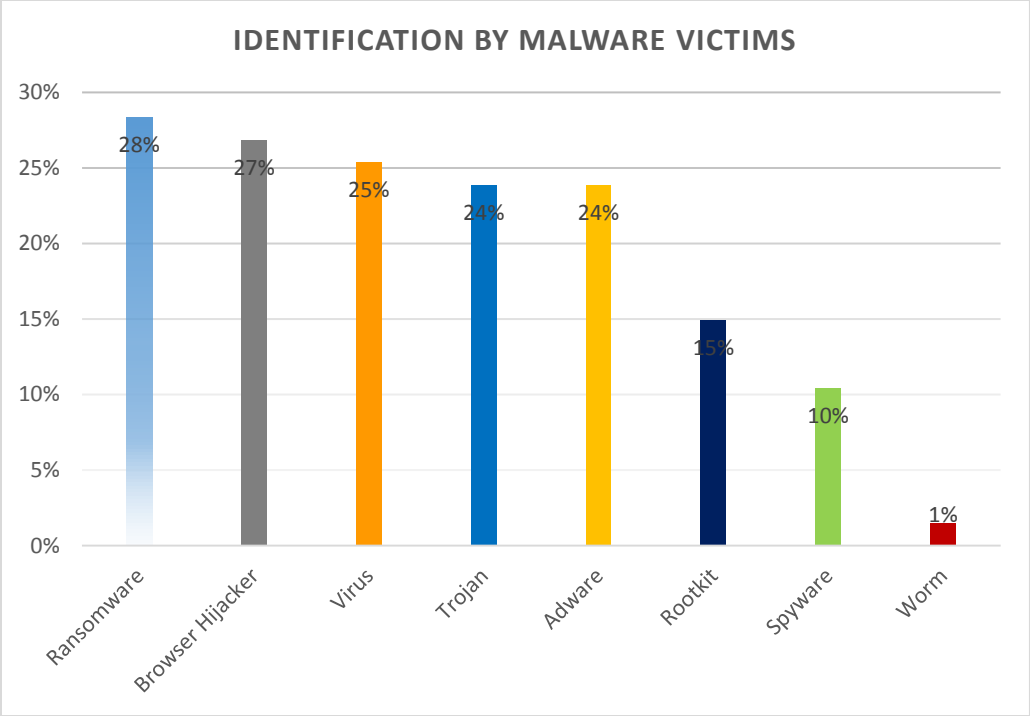

Figure 5: Percent of Malware Identified by Malware Victims

This section reviewed the quantitative methods used to evaluate the research questions. The research design, population characteristics, and data collection procedures were also provided. All of these items added to the data analysis process used for the study.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Findings Related to the Study

Can people identify malware? Faculty and staff can identify most malware threats depending on the category of malware. An average of 62.5% respondents were able to correctly identify different malware threats. Correctly identified malware based on a threshold of greater than 70% correct included ransomware, virus, browser hijacker, adware, and Trojan. 87% successfully identified ransomware, 86.6% identified a virus, 83% identified a browser hijacker, 80% identified adware and 71.3% identified a Trojan.

Faculty and staff had difficulty identifying malware in the spyware, rootkit and worm categories. Only 41.5% of participants identified spyware. Only 38.3% of participants could identify a rootkit and only 12.6% could identify a worm. Table 3 in the appendix shows the distribution of responses for each malware category.

Does the amount of years of computer use affect the ability to identify malware threats? Overall the amount of years of computer use does not affect the ability to identify malware threats. Results showed a trend where recognition of spyware increased from 11-15 years to 16-20 years to 21-25 years and then in the over 25 years grouping.

Does the amount of hours of daily use of a computer affect the ability to identify malware threats? There is not a relationship between the number of hours of daily use and faculty and staff members' ability to identify malware threats. The results showed in the daily use of eight hours or more, the ability to identify a worm and spyware lowered while these two categories were recognized with less hourly use. Results in the Hourly Daily Use chart show adware,

ransomware, and browser hijackers were identified better than members who used a computer longer than two hours.

Does the experience of previously being attacked by malware increase the ability to identify malware threats? There is not a relationship between victims of previous malware attacks and the increased ability to identify malware threats. Only19.25% of previous malware victims could identify malware threats.

Findings Related to Literature Review

A study conducted by Theodoros Nikolakopoulos included a hypothesis to evaluate whether people who have been attacked by malware previously are more aware of security (Nikolakopoulos, 2009). This hypothesis is similar to the research question "Does the experience of previously being attacked by malware effect the ability to identify malware threats?" in this study. Theodoros's study results show people who have been previously attacked are less aware (Nikolakopoulos, 2009). This is similar to the current study results reflecting only 19.25% of those previously attacked by malware can identify malware threats. The study by Nikolakopoulos also included real life scenarios to evaluate if users would click on harmful links or open harmful attachments but his results were aimed to generalize these as user traits and that fall under security awareness but not a measurement of how aware.

Conclusions

Based on the findings of this study, faculty and staff can identify the majority of malware threats. The type of identifiable malware threats does not show a dependency from people who have been a victim of a malware attack, the number of years of computer use, or the daily hours using

a computer by a faculty or staff member. Since the majority of faculty and staff had difficulty identifying worm, spyware, and rootkit malware categories, this shows the need for education to better prepare people on identifying these malware threats. The anticipated outcome will be to develop a proper training program to reduce or even prevent these common malware intrusions. Training concepts should include: who is targeting potential victims, how are potential victims being targeted, and what should be done for protection against malware threats (SANS, 2016). Prevention of malware infections keeps sensitive data secure, reduces worker downtime, and reduces man hours of technical support.

Recommendations for Practice

A recommendation for training to help faculty and staff recognize threats should include a definition of the malware term, items the malware compromises, and infection vectors. Examples of real life scenarios should be included. This training should be set up in a testing environment so not to infect the institutions production environment. The topics in the training should primarily focus on rootkit, spyware, and worm categories since the study results found these as the least identified threats. The other five topics; virus, Trojan, adware, ransomware, and browser hijacker still need to be included as an awareness of all the different threats. Training should occur at least twice per year. Wombat reported training fails if it only occurs once (Wombat Security Technologies, 2015). One training session would serve as a refresher on previously trained topics and another training session would include both previous topics and any newly identified threats. The training should be generalized for all faculty and staff users. Training should be measured to confirm its effectiveness or to determine if training should be modified. The effectiveness of the training can be measured in the training environment, noting

which malware is being installed by users in the training. Effectiveness of the training can also be measured by comparing the number of incidents reported to the technical help desk and if the amount of malware incidents has increased or decreased since the time training was implemented. Additional recommendations for safe practices include reinforcing users not to click on suspicious links on the Internet or unexpected links via email and updating anti-virus and anti-malware tools with the latest definitions and signature files that help the tool recognize threats. Users should visit only reputable websites. Users should be cautious when downloading programs to ensure they are only downloading what they requested.

Recommendations for Future Research

Future research should be conducted to include a study involving students. The study with students can include their personal devices as this study included standardized organizational owned devices. Future research should include investigation into newly created malware threats and the primary infection vectors for these new threats. As malicious hackers look for more ways to steal or generate money, malware threats involving this tactic should be studied closely. In order to better investigate hackers' strategies, research may include working with programmers to find vulnerabilities and the avenues of infection for malware. Research should also be expanded to all devices that includes mobile devices and Apple devices. Looking at future anti-malware tools is also beneficial to determine the tools' limitations and factoring which tool works best in an educational environment. The research on the limitations of anti-malware tools will also help to decide what additional topics need to be presented in the training program. Future research that expands this study which includes a training program then repeats the questionnaire to see if recommendations were effective.

REFERENCES

BitSight Technologies. (2014, August 21). *Press Releases: New Research Reveals Nation's Top Colleges and Universities Are At High Risk for Security Breaches*. Retrieved January 26, 2016, from BitSight: https://www.bitsighttech.com/press-releases/news/new-research-reveals-nations-top-colleges-and-universities-are-at-high-risk-for-security-breaches

CDW Government Inc. (2009). CDW-G Federal Cybersecurity Report: Danger on the Front Lines. 1-27.

Danchev, D. (2012, February 23). *Threat Research: Threat Blog*. Retrieved January 30, 2016, from WEBROOT: http://www.webroot.com/blog/2012/02/23/why-relying-on-antivirus-signatures-is-simply-not-enough-anymore/

Faust, J. (2011, July 23). *SANS Institute InfoSec Reading Room.* Retrieved January 29, 2016, from SANS Institute: https://www.sans.org/reading-room/whitepapers/malicious/mitigating-browser-based-exploits-behavior-based-defenses-hardware-virtualization-33804

Gordon, C. J. (2015, December). *Addressing Security Risks for Mobile Devices: What Higher Education Leaders Should Know.* Retrieved from May 13, 2016, DigitalCommons@University of Nebraska-Lincoln: http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1254&context=cehsedaddiss

Huq, N. (2015). *Security Intelligence: Follow the Data: Dissecting Data Breaches and Debunking the Myths.* Retrieved January 29, 2016, from Trend Micro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf

Invincea, Inc. (2014, June). *White Papers and Product Information.* Retrieved from January 25, 2016, Invincea: http://www.invincea.com/wp-content/uploads/2014/06/Invincea_Ransomware_whitepaper_061614.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 973-993.

Kaspersky. (2016). *Internet Security Center*. Retrieved January 23, 2016, from Kaspersky Lab: https://usa.kaspersky.com/internet-security-center/threats/adware#.V0iFaPkrKUk

Kaspersky. (2016). *Types of threats*. Retrieved January 23, 2016, from Kaspersy Lab: http://support.kaspersky.com/us/viruses/general/614

Krebs, B. (2016, December 11). *Download.com Budling Toolbars, Trojans*. Retrieved January 30, 2016, from Krebs on Security: http://krebsonsecurity.com/2011/12/download-com-bundling-toolbars-trojans/

Lehrfeld, M. (2013). Development of a Security Awareness Program to Reduce Security. *Proceedings of the 2013 ASCUE Summer Conference* (p. 52). North Myrtle Beach: ASCUE.

McElroy, L., & Weakland, E. (2013). Measuring the Effectiveness of Security Awareness. *Educause Center for Analysis and Research: Research Bulletin*, 1-10.

Merriam-Webster. (2016, January). *Dictionary*. Retrieved January 13, 2016, from Merriam-Webster: http://www.merriam-webster.com/dictionary/malware

Nikolakopoulos, T. (2009). *Open Digital Archive: Evaluating the Human Factor in Information Security.* Retrieved May 10, 2016, from Oslo and Akershus University of Applied Sciences: https://oda.hio.no/jspui/bitstream/10642/444/2/Nikolakopoulos_Theodoros.pdf

NTT Group. (2014). *Global.* Retrieved January 22, 2016 from Dimension Data: https://www.dimensiondata.com/Global/Downloadable%20Documents/2014%20NTT%20Group%20Global%20Threat%20Intelligence%20Report.pdf

Nyabando, C. J. (2008, August). *ELECTRONIC THESES AND DISSERTATIONS.* Retrieved January 26, 2016, from Digital Commons @ East Tennessee State University: http://dc.etsu.edu/cgi/viewcontent.cgi?article=3324&context=etd

OpenDNS. (2013, October 16). *Press Releases: OpenDNS Reports that Higher Education Networks are 300 Percent More Likely to Contain Malware*. Retrieved February 6, 2016, from CISCO OpenDNS: https://www.opendns.com/about/press-releases/opendns-reports-higher-education-networks-300-percent-likely-contain-malware/

Reavis, J. (n.d.). *Anti-Malware Scan.* Retrieved January 29, 2016, from GeoTrust: https://www.geotrust.com/anti-malware-scan/malware-threat-white-paper.pdf

REN-ISAC. (2014, November 12). *Alerts.* Retrieved January 26, 2016, from REN-ISAC: Research and Education Networking Information Sharing and Analysis Center: http://www.ren-isac.net/alerts/REN-ISAC_ADVISORY_University_Payroll_Theft_20141112_TLPWHITE.pdf

SANS. (2016). *End User Security Awareness Training Program.* Retrieved January 26, 2016, from SANS Securing The Human: https://securingthehuman.sans.org/training

SecurityScorecard. (2015, September). *2015 Higher Education Security Report.* Retrieved February 6, 2016, from Hubspot: https://cdn2.hubspot.net/hubfs/533449/2015_Higher_Education_Security_Report.pdf

Sophos. (2016). *Spyware: A to Z of Threats*. Retrieved January 26, 2016, from Sophos: https://www.sophos.com/en-us/threat-center/threat-analyses/threatsaurus/a-to-z-of-threats.aspx

Symantec. (2016). *2016 Internet Security Threat Report*. Retrieved January 24, 2016, from Symantec: https://www.symantec.com/security-center/threat-report

Symantec. (2016). *Ransomware on the rise: Norton tips on how to prevent getting infected.* Retrieved January 24, 2016, from Norton by Symantec: http://us.norton.com/ransomware/article

Symantec. (2016). *Security Response*. Retrieved January 26, 2016, from Norton by Symantec: http://us.norton.com/security_response/glossary/define.jsp?letter=r&word=rootkit

Symantec. (2016). *Security Response*. Retrieved January 26, 2016, from Norton by Symantec: http://us.norton.com/security_response/spyware.jsp

Tech Target Search Security firewall. (2016). Retrieved February 21, 2016, from Tech Target: http://searchsecurity.techtarget.com/definition/firewall

TechTerms. (2016). *Technical Terms: Domain Definition*. Retrieved February 21, 2016, from Tech Terms: http://techterms.com/definition/domain#

University of Arizona Information Security Office. (2016, January). *All-Employee Security Awareness Request Form: Information Security*. Retrieved January 17, 2016, from The University of Arizona: http://security.arizona.edu/all-employee-security-awareness-request-form

University of Cincinnati Office of Information Security. (2016, January). *Awareness: Office of Information Security*. Retrieved January 17, 2016, from University of Cincinnati: https://www.uc.edu/infosec/info.html

Unversity of North Alabama. (2016, January). *Human Resources Forms and Links.* Retrieved January 17, 2016, from University of North Alabama: https://www.una.edu/humanresources/files/forms-links/Security%20Awareness%20Training%20Program%20Requirements%20and%20FAQs%20for%20the%20Web.pdf

Villanova UNIT. (2015). *Fall 2015 - UNIT Progress Report: Innovative Technology Solutions & Services Unit*. Retrieved January 26, 2016, from Villanova University: http://www1.villanova.edu/villanova/email/unitprogressreport/progress_report.html

Walker, D. (2014, August 21). *Study: Most higher ed malware infections attributed to 'Flashback'*. Retrieved January 26, 2016, from SC Magazine for IT Security Professionals: http://www.scmagazine.com/study-most-higher-ed-malware-infections-attributed-to-flashback/article/367513/

Wise Geek. (2016). *What Is a File Signature?* Retrieved January 26, 2016, from Wise Geek: http://www.wisegeek.com/what-is-a-file-signature.htm

Wombat Security Technologies. (2014, December 9). *TOP NEWS: Wombat Security Technologies Enabled a Global Manufacturing Company to Reduce Malware Infections by 46%*. Retrieved February 11, 2016, from Reuters: https://www.wombatsecurity.com/press-releases/wombat-security-technologies-enabled-global-manufacturing-company-reduce-malware

Wombat Security Technologies. (2015, March 24-24). *FISSEA.* Retrieved February 11, 2016, from National Institute of Standards and Technology: http://csrc.nist.gov/organizations/fissea/2015-conference/presentations/march-24/fissea-2015-massaro.pdf

Wombat Security Technologies. (2015, September 08). *Global Manufacturing Company Reduces Malware Infections.* Retrieved February 11, 2016, from Wambat Security: https://info.wombatsecurity.com/hs-fs/hub/372792/file-2557238064-pdf/WombatSecurity_CaseStudy_Manufacturing_46PercentMalwareReduction_090815.pdf?submissionGuid=ca3f1d6b-6ff5-4b1c-a5f0-29704db7524f

APPENDICES

APPENDIX A

Table 2.

Malware Category Table

Malware Category	**Corresponding Survey Question**
Worm	(Q9)You receive an email stating you must provide your username and password. Later, you begin to see a large number of emails in your Sent Items folder that you did not compose or send.
Virus	(Q10)You receive an email from a colleague. After opening the attachment, you begin to see several messages indicating your computer is comprised.
Trojan	(Q11)To view an online video, you execute a video codec and then notice data missing from your computer and the system freezes.
Spyware	(Q12)Your computer slows down after downloading free software containing installation of other programs as part of the free agreement.
Browser Hijacker	(Q13)Your web browser's default homepage and search engine have changed. When you perform a search, you continually see a page that is not related to your search entry.
Adware	(Q14)The local newspaper's webpage begins to download several advertisements and your system slows down considerably.
Ransomware	(Q15)After opening an email attachment titled "Invoice", you receive a note stating all of your files are encrypted and the only way to retrieve a decryption key is by following one of the private links listed.
Rootkit	(Q16)After clicking a link you received from your Instant Messaging client, your computer fails to respond to keyboard or mouse input.

APPENDIX B

Table 3.

Distribution of Malware Responses

Worm Category	Browser Hijacker		Worm		Phishing		Rootkit	
	N	%	N	%	N	%	N	%
	14	17.7	12	12.6	82	86.3	5	5.3
Virus Category	Adware		Email Error		Virus		Browser Hijacker	
	N	%	N	%	N	%	N	%
	7	7.2	0	0.0	84	86.6	6	6.2
Trojan Category	Codec Error		Operating System Error		Trojan		Browser Hijacker	
	N	%	N	%	N	%	N	%
	12	12.8	5	5.3	67	71.3	10	10.6
Spyware Category	Adware		Spyware		Browser Hijacker		Ransomware	
	N	%	N	%	N	%	N	%
	46	48.9	39	41.5	3	3.2	6	6.4
Browser Hijacker Category	Web Browser Toolbar		Search Engine Manager		Browser Hijacker		Worm	
	N	%	N	%	N	%	N	%
	2	2.1	2	2.1	78	83.0	12	12.8
Adware Category	Ransomware		Slug		Worm		Adware	
	N	%	N	%	N	%	N	%
	5	5.3	5	5.3	9	9.5	76	80
Ransomware Category	Virus		Worm		Ransomware		Adware	
	N	%	N	%	N	%	N	%
	6	6.5	5	5.4	80	87.0	1	1.1
Rootkit Category	Browser Hijacker		Rootkit		Virus		Trojan	
	N	%	N	%	N	%	N	%
	7	7.4	36	38.3	27	28.7	24	25.5

APPENDIX C

Table 4.

Distribution of Years of Use

Years	**Correct Answers Per Malware Category**		**Responded**	**Percentage**
	Worm			
1-5 Years		0	1	71%
6-10 Years		0	1	0%
11-15 Years		1	6	17%
16-20 Years		3	20	15%
21-25 Years		0	23	0%
Over 25 Years		8	47	17%
Years	Virus		**Responded**	
1-5 Years		1	1	100%
6-10 Years		1	1	100%
11-15 Years		5	6	83%
16-20 Years		16	20	80%
21-25 Years		21	23	91%
Over 25 Years		40	47	85%
Years	Trojan		**Responded**	
1-5 Years		1	1	100%
6-10 Years		0	1	0%
11-15 Years		4	6	67%
16-20 Years		12	20	60%
21-25 Years		16	23	70%
Over 25 Years		34	47	72%
Years	Spyware		**Responded**	
1-5 Years		1	1	100%
6-10 Years		1	1	100%
11-15 Years		1	6	17%
16-20 Years		6	20	30%
21-25 Years		8	23	35%
Over 25 Years		22	47	47%
Years	Browser Hijacker		**Responded**	
1-5 Years		1	1	100%
6-10 Years		1	1	100%
11-15 Years		5	6	83%

16-20 Years		11	20	55%
21-25 Years		19	23	83%
Table 4: Distribution of Years Continued				
Years	**Correct Answers Per Malware Category**		**Responded**	**Percentage**
Over 25 Years		41	47	87%
Years	Adware		**Responded**	
1-5 Years		1	1	100%
6-10 Years		1	1	100%
11-15 Years		4	6	67%
16-20 Years		12	20	60%
21-25 Years		21	23	91%
Over 25 Years		37	47	79%
Years	Ransomware		**Responded**	
1-5 Years		1	1	100%
6-10 Years		0	1	0%
11-15 Years		5	6	83%
16-20 Years		13	20	65%
21-25 Years		20	23	87%
Over 25 Years		41	47	87%
Years	Rootkit		**Responded**	
1-5 Years		0	1	0%
6-10 Years		1	1	100%
11-15 Years		1	6	17%
16-20 Years		11	20	55%
21-25 Years		9	23	39%
Over 25 Years		14	47	30%

APPENDIX D

Table 5.

Distribution of Daily Hourly Use Responses

Hours	Correct Responses Per Malware	Responded	%
	Worm		
Less than 1 Hour	**0**	**0**	
1-2 Hours	0	3	0
3-4 Hours	0	13	0
5-6 Hours	6	30	0.2
7-8 Hours	4	25	0.16
8 or More Hours	1	27	0.037037
	Virus	**Responded**	%
Less than 1 Hour	**0**	**0**	
1-2 Hours	2	3	67%
3-4 Hours	11	13	85%
5-6 Hours	27	30	90%
7-8 Hours	21	25	84%
8 or More Hours	24	27	89%
	Trojan	**Responded**	%
Less than 1 Hour	**0**	**0**	
1-2 Hours	1	3	33%
3-4 Hours	9	13	69%
5-6 Hours	21	30	70%
7-8 Hours	15	25	60%
8 or More Hours	22	27	81%

	Spyware	Responded	%
Less than 1 Hour	**0**	**0**	
1-2 Hours	1	3	33%

Table 5: Distribution of Daily Hourly Use Responses Continued

Hours	Correct Responses Per Malware	Responded	%
3-4 Hours	3	13	23%
5-6 Hours	13	30	43%
7-8 Hours	12	25	48%
8 or More Hours	11	27	41%
	Browser Hijacker	**Responded**	%
Less than 1 Hour	**0**	**0**	
1-2 Hours	3	3	100%
3-4 Hours	10	13	77%
5-6 Hours	21	30	70%
7-8 Hours	21	25	84%
8 or More Hours	24	27	89%
	Adware	**Responded**	%
Less than 1 Hour	**0**	**0**	
1-2 Hours	3	3	100%
3-4 Hours	6	13	46%
5-6 Hours	24	30	80%
7-8 Hours	20	25	80%
8 or More Hours	24	27	89%

	Ransomware	Responded	%
Less than 1 Hour	**0**	**0**	

Table 5: Distribution of Daily Hourly Use Responses Continued

Hours	Correct Responses Per Malware	Responded	%
1-2 Hours	3	3	100%
3-4 Hours	11	13	85%
5-6 Hours	23	30	77%
7-8 Hours	17	25	68%
8 or More Hours	27	27	100%

	Rootkit	Responded	%
Less than 1 Hour	**0**	**0**	
1-2 Hours	1	3	33%
3-4 Hours	1	13	8%
5-6 Hours	10	30	33%
7-8 Hours	12	25	48%
8 or More Hours	13	27	48%

APPENDIX E

Table 6.

Distribution of Malware Victims and Correct Answers

Attacked by Malware	Correctly Answered	Responded	Percent
	Worm		
Yes	1	67	1%
	Virus		
Yes	17	67	25%
	Trojan		
Yes	16	67	24%
	Spyware		
Yes	7	67	10%
	Browser Hijacker		
Yes	18	67	27%
	Adware		
Yes	16	67	24%
	Ransomware		
Yes	19	67	28%
	Rootkit		
Yes	10	67	15%

APPENDIX F

IRB Approval

IRB APPROVAL – Initial Exempt April 28, 2016

Malora Quesinberry

RE: Identification of Malware Threats

IRB#: c0416.20e

ORSPA#:

On April 28, 2016, an exempt approval was granted in accordance with 45 CFR 46. 101(b) (2). It is understood this project will be conducted in full accordance with all applicable sections of the IRB Policies. No continuing review is required. The exempt approval will be reported to the convened board on the next agenda.

- New protocol submission xForm, pertinent literature, PI resume, Email letter, Survey Consent, Malware Identification Survey

Projects involving Mountain States Health Alliance must also be approved by MSHA following IRB approval prior to initiating the study.

Unanticipated Problems Involving Risks to Subjects or Others must be reported to the IRB (and VA R&D if applicable) within 10 working days.

Proposed changes in approved research cannot be initiated without IRB review and approval. The only exception to this rule is that a change can be made prior to IRB approval when necessary to eliminate apparent immediate hazards to the research subjects [21 CFR 56.108 (a) (4)]. In such a case, the IRB must be promptly informed of the change following its implementation (within 10 working days) on Form 109 (www.etsu.edu/irb). The IRB will review the change to determine that it is consistent with ensuring the subject's continued welfare. Sincerely, Stacey Williams, Chair

ETSU Campus IRB

Cc: Todd Emma

APPENDIX G

Survey Consent

Dear Participant:

My name is Malora Quesinberry, and I am a graduate student at East Tennessee State University. I am working on a master's degree in Engineering Technology, In order to finish my studies, I need to complete a research project. The name of my research study is Identification of Malware Threats.

The purpose of this study is to determine if people can identify malware threats. I would like to a brief survey to faculty and staff using Survey Monkey. It should only take about 5-10 minutes to complete. You will be asked questions about technology and malware identification. There are no risks to completing this survey. This study has no direct benefits to participants.

Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties, as is the case with emails. In other words, we will make every effort to ensure that your name is not connected with your responses. Specifically, Survey Monkey has security features that will be enabled: SSL encryption software will be utilized and no IP addresses will be collected. Although your rights and privacy will be maintained, the ETSU IRB (for non-medical research) and personnel particular to this research (Malora Quesinberry and Todd Emma) have access to the study records,

If you do not want to fill out the survey, it will not affect you in any way. You may skip any questions you do not wish to answer or simply exit the online survey form if you wish to remove yourself entirely, Participation in this study is voluntary. You may refuse to participate. You can quit at any time. If you quit or refuse to participate, the benefits or treatment to which you are otherwise entitled will not be affected.

If you have any research-related questions or problems, you may contact me, Malora Quesinberry, at 423- 439-3614.1 am working on this project under the supervision of Todd Emma. You may reach him at 423-979-3157. Also, the chairperson of the Institutional Review Board at East Tennessee State University is available at (423) 439-6054 if you have questions about your rights as a research subject. If you have any questions or concerns about the research and want to talk to someone independent of the research team or you can't reach the study staff, you may call an IRB Coordinator at 423/439-6055 or 423/439/6002.

Sincerely, Malora Quesinberry APPROVED By the ETSUIRB

Clicking the AGREE button below indicates

- You have read the above information APR 2 8 2016
- You voluntarily agree to participate •
- You are at least 18 years of age or older

I AGREE

I DO NOT AGREE

VITA

MALORA QUESINBERRY

Education:

M.S. Technology, concentration in Engineering Technology,
East Tennessee State University, Johnson City, Tennessee, 2016

B.B.A. Information Systems, Radford University,
Radford, Virginia, 1999

Professional Experience:

Information Technology Services –Support Specialist, East Tennessee State University, Johnson City, Tennessee. November 2008 – Present

Eastman Global Help Desk - Help Desk Agent/E-Business Representative, Tele-Optics, Kingsport, Tennessee. June 2008 – November 2008

Engineering Technical Assistant, Tempur-Pedic Production, Duffield, Virginia. June 2007 – August 2007 and November 2007- End of May 2008 (Consultant)

Sr. Information Technology Representative, T. Rowe Price, Acuity/Metro, Owings Mills, Maryland. February 2001-July 2001 – Mid April 2006

Information Technology Help Desk Agent, Enterprise Rent-A-Car, St. Louis, Missouri. May 2000 - December 2000