International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 01, January - March, 2021, pp 75-80

IT SECURITY AND MALWARE THREATS: AN ANALYSIS OF UNIVERSITY STAFF AND STUDENTS APPROACH

Dr. Kapil Kumar[*]

ABSTRACT

This research presents results related to the capacity of students and staff members to detect malware threats. Eight malware groups were defined by researchers as the most common threats to higher education systems such as virus, Ransomware, worm, Trojan, browser hijacker, spyware root kit malware, and adware. To highlight the importance of identifying security risks, the effect of malware intrusions on higher education systems has to be understood. This research studies the approach and awareness level of University staff and students worldwide to identify and tackle problems related to malware threats. A model recommendation will be proposed for educating faculty and staff members so as to identify malware threats in less identified categories to help alleviate future malware intrusions.

Keywords: *Ransomware, Cryptocurrency, Antivirus, Security Threats, Risk Factors.*

Introduction

In 2014, several universities that were targets of malware attacks, including phishing scams to steal credentials, were documented by REN-ISAC. The University of Western Michigan, the University of Boston, Texas A&M, the University of Iowa and the University of Michigan have been identified as allegedly attacking universities (REN-ISAC, 2014).Future guidelines include exploring new forms of malware hazards, identification of malware risks by staff and students, and ways to minimize these hazards. Can malware threats be detected by universities? Malware attacks cost time, resources and the loss of confidential data. The possibility of malware invasions is higher in higher education institutions. Exploring the areas at stake highlights the importance of why it is important to resolve malware risks as the stakes are very high. Studies have shown that security knowledge effectively decreases malware infections and calls to technical assistance desks (Wombat Security Technologies, 2014). Users that are unable to detect malware threats are more likely to become victims of malware invasions. Malware attacks cost time, resources and the loss of confidential data for organizations. For malware remediation, a medium-sized university will spend $30,000 per year on average (Lehrfeld, 2013).This expense often entails loss of working time and infringement of confidential data. Symantec’s cybercrime study reported that attacks cost $575 billion per year (Symantec, 2016). Several anti-malware systems can assist with cleanup after infections. Anti-malware technologies, however are limited to stopping intrusions from malware. It is more likely that end-users who bypass anti-malware settings would fall prey to malware intrusions. Compromised safety due to computer system malware intrusions can lead to work disturbances and ultimately loss of valuable data and revenue.

The possibility of malware invasions is higher in higher education institutions. Many kinds of sensitive data are handled by higher education institutions, especially for students, which makes them a target for malicious hackers. A BitSight Technologies study reports that higher education institutions are more at risk of breaches of security than the retail and healthcare industries (BitSight Technologies, 2014).Higher education institutions have become more mindful of these rising threats and are worried with keeping their data secure. Higher education systems such as the University of North Alabama aim to

[*] Assistant Professor, Department of Management Studies, BPS Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana, India.

add and implement information technology security awareness training programs while companies use various data security approaches (University of North Alabama, 2016). Information security awareness programs are also mandated by the University of Arizona, the University of Cincinnati and Villanova University (Cincinnati University Information Security Office, 2016); (University of Arizona Office of Information Security, 2016).

Objectives

- To identified the various categories of malware threats as faced by the students and staff of universities worldwide.
- To find out the factors that affected university students and staff member's ability to identify malware threats.
- To suggest methods to prevent malware threats faced by the university students and staff members.

Research Methodology

This study uses all systematic reviews of evidence on malware threats in higher education sector.

Literature Review

The key objective of the "Ongoing Malware Threat" study was the recognition of web browser vulnerabilities as GeoTrust, an Internet security firm, manufactures anti-malware scanning technologies to secure websites. While the main emphasis was on website attacks, GeoTrust recommends a security strategy that covers all device platforms and multiple types of malware.

Malware Terms and Definitions

Adware is software used to view ads that contains code to monitor user data and provide it to the developer of adware. Without the awareness of the user, this monitoring is achieved. Adware creates issues if the adware has bugs in its code and by installing multiple advertisements when it slows down the device (Sophos, 2016).

- **Hijacker Browser:** A browser hijacker alters your web browser's default homepage and search engine without your permission (Sophos, 2016). A browser hijacker influences the perception of surfing.
- **Ransomware**: Ransomware is a malicious software that attackers use to steal information from the owner and keep it locked until a ransom is paid (Invincea, Inc., 2014). The most popular one is requiring users to pay a ransom for a decryption key for the stolen and encrypted encrypted data (Invincea, Inc., 2014).
- **Rootkit**: A rootkit is a software program used to mask malicious activities so that they can not be detected by antivirus programs. Rootkits modify the operating system to hide the infected machine itself and its behavior (Kaspersky, 2016). Since the majority of malware infects apps, this is different.
- **Spyware**: Spyware is malware that allows advertisers or hackers to obtain confidential data without permission from you (Sophos, 2016).
- **Trojan**: A Trojan, like a worm, does not clone itself. A Trojan executes by user interaction on compromised computers and does not execute by itself (Kaspersky, 2016). A Trojan may create an opening which gives the computer system access to malware hackers.
- **Virus**: A virus is malware that by inserting a virus code, infects other programs and begins to spread when an infected file starts (Sophos, 2016). A virus is host program based and typically attached to an executable file. So even if a virus is on a computer, someone has to run the executable file to trigger it.
- **Worm**: To spread to other machines, a worm makes a copy of itself. A worm does not rely on a host program such as a virus and uses vulnerabilities such as the auto-run function when a USB drive is connected to a computer to access and propagate via network resources such as email (Sophos, 2016)

Result of Malware Attacks

The different threats to malware are generated as a way for malicious users to either interrupt a system's workflow or steal data. If a device is contaminated, the list below briefly describes the things compromised by the specific threat.

- **Adware:** Through uploading many commercials, Adware slows down machines. If the coding for an advertising has flaws, device instability may occur (Sophos, 2016).
- **Hijacker of the Browser**: A browser hijacker disrupts legitimate browsing practices and redirects users to either sites that help the hacker increase the operation of specific sites or may redirect them to inappropriate sites or malicious sites that could cause further harm (Sophos, 2016).
- **Around Ransomware**: If they want to pay a ransom to recover data from the attackers, ransomware will steal data, lose data and cause uses to lose money (Invincea, Inc., 2014).
- **Rootkit**: A rootkit can steal and then send passwords or other sensitive data to hackers (Sophos, 2016). Various things may be at risk if hackers gain access, depending on the degree of access a person has to a device, databases, or network.
- **Spyware**: Without authorization, spyware records user behavior and data. By depleting memory and computing power, spyware can also slow down or crash a computer (Sophos, 2016).
- **Trojans**: Trojans can remove data, steal information and freeze computer systems (Kaspersky, 2016).
- **Viruses**: Viruses can steal information, give hackers computer control and show annoying messages (Sophos, 2016).
- **Worms**: Worms are used to steal information, send spam and can infect several computers (Kaspersky, 2016).

In July 2013, one case study reported an incident in which a business became contaminated with a Worm malware. The cause has been traced to an infected program administrator on a USB the computer that uploads the infection unknowingly. Many of the server systems have not been upgraded to Installed anti-virus signatures or some servers have been entirely missing anti-virus applications. Since infections continued for an additional three months after the first diagnosis, the cost incurred equivalent of $109,000,000 for damages, prosecution, and cleanup (NTT Group, 2014). The research It also concluded that user education and training would help to avoid infections with malware, as this case revealed the outcome of user behaviour.

For all malware risks, malware signatures used to recognize particular forms of malware are not usable. A Zero Day attack is a common threat to prevent detection by anti-malware software, as this form of attack consists of a newly created malware threat that has not yet had an identifiable signature threat (Faust, 2011).

Three billion malware attacks on users in 2010 and high costs due to stolen credit card information and costs for remediation of the attacks were documented in a Symantec White Paper on The Ongoing Malware Threat (Reavis, n.d.). The study revealed that many instruments are developed by design to focus on certain areas of technology systems, reinforcing the notion of weaknesses in anti-malware tools.

Methods/ Strategies to Tackle Threats

In February 2015, Wombat Protection Technologies gave a presentation listing five reasons why a safety education program did not succeed, ten concepts of learning science, a framework for continuous training and case studies. They found that the explanation for 95 percent of security incidents in 2013 was human error (Wombat Security Technologies, 2015). The 5 reasons for inadequate safety education initiatives were;

- Training happens only once a year.
- Training via videos or slides not hands on.
- Training teaches the end user what to do but not why.
- Training sessions are over 15 minutes long.
- Training focuses on threat perception, but not change in actions.

The solution included the development of training programs that were not only informative, but educational. The solutions proposed included clarifying why something is a threat and then providing what security measures were needed. It was proposed that lessons should be kept for ten minutes or less and topics should be condensed to allow the audience to absorb the knowledge in the lesson.

DanchoDanchev (2012), an author of Webroot, addressed the shortcomings of anti-malware software focused on a reactive approach rather than using a proactive approach. The current approach of recognizing and preventing threats was identified by Danchev (2012).

The latest methodology utilizes out-of-date methods for anti-malware tools and signature-based threat identification (Danchev, 2012). Signature-based threat identification requires the discovery of a new malware variant, then an anti-malware tool provider develops a new signature to defend against the new threat, then it is passed on to consumers as an upgrade to the anti-malware tool after the vendor confirms the security works.

The key findings described end users as the greatest security threat, with faculty and staff users posing more danger than students (Gordon, 2015). In the interviews, the main ideas on where and how to focus their future efforts to reduce safety risks were addressed.

Among these were the development of security awareness programs, regular contact by higher education institutions and IT departments of security initiatives, shifting emphasis on protecting the data at the source rather than protecting the computer accessing it, and the need to maintain a balance between user access and security so that the higher education mission is still accomplished (Gordon, 2015). Institutions also need to enable end users, through recognizing its value, to remain vigilant about security.

Findings and Conclusion

Faculty and staff had difficulty identifying malware in the spyware, rootkit and worm categories. Overall, the capacity to detect malware threats is not impaired by the number of years of computer use. Results showed a pattern where spyware identification grew from 11-15 years to 20 years to 21-25 years and then over 25 years of grouping.

There is no connection between the number of hours of regular use and the capacity of faculty and staff members to recognise threats from malware.

There is no connection between victims of past malware attacks and the improved ability to recognise threats from malware.

Malware infection prevention keeps confidential data secure, decreases worker downtime, and reduces technical support hours for men.

The definition of the malware word should be included in a proposal for training to help faculty and staff identify threats.

Additional safe practice guidelines include reinforcing users not to click on suspicious Internet links or unexpected email links and updating anti-virus and anti-malware applications with the new concepts and signature files that help the tool detect threats. Only reputable websites can be accessed by users. When downloading applications, users should be vigilant to make sure they are only downloading what they have requested.

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-researchreveals-nations-top-colleges-and-universities-are-at-high-risk-for-security-breaches

✓ CDW Government Inc. (2009). CDW-G Federal Cyber security Report: Danger on the FrontLines. 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-antivirussignatures-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/readingroom/whitepapers/malicious/mitigating-browser-based-exploits-behavior-based-defenseshardware-virtualization-33804

✓ Gordon, C. J. (2015, December). Addressing Security Risks for Mobile Devices: What HigherEducation 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 andDebunking the Myths. Retrieved January 29, 2016, from Trend Micro:http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wpanalyzing-breaches-by-industry.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-combundling-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 MerriamWebster: 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

✓ Open DNS. (2013, October 16). Press Releases: OpenDNS Reports that Higher EducationNetworks are 300 Percent More Likely to Contain Malware. Retrieved February 6, 2016, from CISCO OpenDNS: https://www.opendns.com/about/press-releases/opendns-reportshigher-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/RENISAC_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-ofthreats.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-awarenessrequest-formUniversity of Cincinnati Office of Information Security. (2016, January). Awareness: Office ofInformation 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/formslinks/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 highered 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-infectionsattributed-to-lashback/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-enabledglobal-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/fissea2015-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