Internet Worms and the Weakest Link: Human Error

Group 12: Avery Speller, Katie Myers, Andy Burke, Matt Blatz

Introduction

For several years now, the internet has been the primary form of contact between people and businesses. However, even with the ever expanding uses for our computer networks, the general population is still overwhelmingly undereducated about malware. While people are usually aware that computer viruses exist, they often do not know that there are various types of malware, or what these different types are capable of doing. Many people are terrified of getting a virus on their computer, even though they often are unsure as to what a specific virus is capable of doing, or how it managed to infiltrate their computer. Even when people are aware of a virus on their computer, and they know how they acquired it, they often refuse to tell others how it happened.

Our goal is to improve malware awareness in computer users. In specific, we wish to bring awareness to the dangers posed by computer worms.

While most people have heard of the Morris Worm, many have not experienced or witnessed the development of worms as they have been programmed to be more adaptable and more destructive than ever before. For instance, several members of our group, all upper-year computer science majors, were unaware of the existence of the Stuxnet worm before this project. However, the Stuxnet worm is possibly one of the most weaponized uses of the worm virus seen to date [10]. Having a unique spreading mechanism and a highly malicious payload, the Stuxnet worm may very well be classified as one of the first weaponized viruses [10].

Even within the category of viruses classified as worms, there are still several distinctions between the different types of worms. There are approximately five types of defined worms, all of which are classified based on how they spread [3]. By definition, worms are spread over a network, and run independently with the priority of multiplying and releasing the payload [3]. The five types of worms are defined as follows:

- Network Worms: Use the internet or local network to spread via TCP
- Email Worms: Spread through emails and their attachments
- IRC Worms: Spread by internet relay channels
- P2P Worms: Spread through peer to peer networks
- IM Worms: Spread through instant messaging applications

[3]

Regardless of the type of worm, there are five stages to a computer worm life cycle [3].

- Penetration into computer
- Activation
- “Victims” search
- Duplicate preparation
- Duplicate distribution

[3]

Most users are unable to catch a worm virus before it reaches the distribution

of it's duplicates, and as such many networks are flooded by worms. Our goal is to improve computer users awareness of worms, and how to stop the worms before they are even able to penetrate the computer.

Findings

There are no specific studies on the education of computer worms, however this is not surprising considering a very small percentage of worms actually affect our daily lives, such as slowing our computers or reducing our bandwidth [5]. Approximately 2% of all malware strains that actually affect the end user are Worms, with 57% being virus's [5]. This explains why when most people are referring to malware they use the term virus, because it is more commonly a problem for us compared to the various other types of malware [5]. However, if one of those worms is malicious, it could cause a company to lose up to 70% of productivity, and 40% of company data in the aftermath [5].

More so than the computer software or protocols, humans are highly susceptible to malware attacks. There are works that claim that as long as we have access to emails, we will be subjected to phishing emails [2]. Phishing emails are a for of phishing done through professional looking emails that often seek to gain the receivers sensitive personal data [4]. Of the 156 million phishing emails that are sent out daily, approximately 800,000 links are clicked on, and 80,000 people every day are scammed of their personal information [7]. Phishing emails have been around for years, and yet we still keep falling for them, allowing them to gain access to our computers and our networks. Email worms are only capable of propagating through emails, and therefore are forced to use user involvement to achieve their end goal, and yet they are still so popular to date [11]. Software and hardware have been updated again and again, however a system can only do so much on account for user error. It is time that we "upgrade" people as well [6]. When it comes to worms, a system is only as strong as its weakest link, and right now that is the user [6].

However, "it is both impractical and unwise to expect every individual with a computer connected to the Internet to be a security expert" [8]. While we can spend the time training as many computer users as possible on the subject, it only takes one computer on the network to have caught a virus in order to infiltrate an entire network. However, as we educate more people, there are less potential sources on the network.

The complication with relying solely on your own security is that "the current mechanism for dealing with security holes expects an end user to constantly monitor security alert websites to learn about security flaws and then to immediately download and install patches. The installation of patches is often difficult, involving a series of complex steps that must be applied in precise order" [8]. It is a very heavy burden to place upon an end user, and even with these measures, it is still completely possible for their computer to become infected.

This is possibly the biggest problem with worms, as they are autonomous, they continue to generate and spread through vulnerabilities that many users are not even aware they possess [9]. This is the problem our group is set out to solve. We desire to reduce the number of weak links on the

network, so that there are fewer vulnerabilities to a system.

Methodology

The approach we took to this problem follows standard educational methods while allowing for the expansion of this project. We developed a qualtrics quiz that covers the basics of how worms are transmitted between systems, the best ways to protect your system from an attack, examples of famous worms that have successfully taken down large scale systems, and scenario questions to put the users of the quiz into a position where they have to think critically about the information handed to them. Informing people of these types of threats is the only way to properly deal with them, each type of question was specifically chosen as it presents to the user the proper way to defend themselves and allows them to become informed on the current threats.

Definitions: This section allows someone who is completely new to the world of worms to get their grounding and begin their education on the subject matter. The questions from this topic cover things such as the different types of viruses and malware, to more specifically worms and the different ways they are transmitted including email worms, instant messaging worms, and worms that transfer over a file sharing network. To begin to protect oneself you must understand the threat so the focus of this section is to build a fundamental understanding of how malicious files function and spread throughout a network.

Five Components of a Worm: This series of questions breaks down worms even further allowing the taker of the quiz to get a closer look into the inner workings of these malicious software programs. The goal of this series was to explain the technical components of worms to even those without a heavily involved technological background. This is due to the average user being much more susceptible to an attack versus someone who has taken time to study computer security and this is a factor we are looking to address.

Examples: While this section is interlaced in other sections the examples of dangerous worms help to put into perspective who these pieces of malware are made by, who they affect, and the real world implications of having these pieces of software connecting to your home or professional environment.

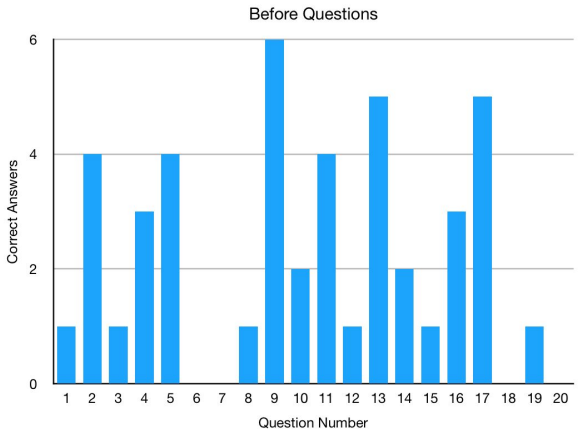
Detection & Protection: Questions about detection and further the protection of systems help the quiz taker understand why worms are so difficult to keep track of and slow down. By showing the quiz taker the various means that security teams take to protect their data and account for the threats worm pose to the systems we use every day we hope to instill a sense of responsibility in the quiz taker showing them they must do their part to protect the systems they use. This will not only make the jobs of security teams easier but hopefully build a more secure system.

Scenario Questions: Finally the scenario questions put the quiz taker in the shoes of someone having to deal with a worm or at a chance of encountering one. This will help make the information the quiz taker has encountered up until this point seem much more real and again instill a sense of responsibility in the user. The purpose of this entire quiz is to get users to understand exactly what their responsibilities are in protecting themselves

from outside threats and by putting them in hypothetical situations we allow them to train themselves how to react when presented with a threat and give them the tools to leave unscathed.

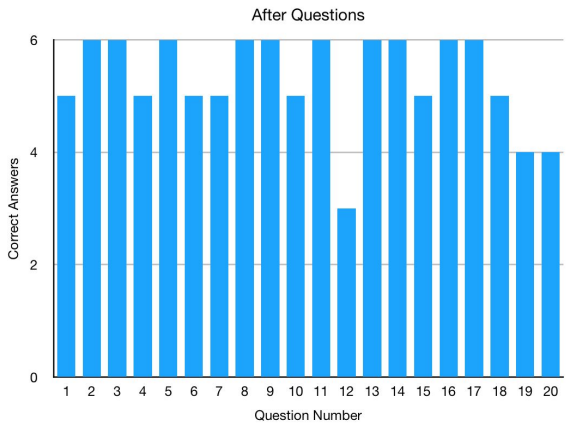
Discussion

In order to prove that the information we were providing to users was effective and useful, we had them complete the quiz first before they had read the information sheet, and once again afterwards. This allowed us to have a baseline to which we could compare the average person's knowledge to. When we ran these tests, we did not inform the participants of their scores on the first quiz before they took the second, nor did we display the notes we had provided them with. We enlisted six participants to be part of the trial group, all of which had very different backgrounds and experiences with viruses. We selected two participants who were relatively well versed in computer software, two that frequently used their computers for either school or work, and finally two users who used their computers primarily for email or instant messaging. The chart following displays the results of the first quiz, before the participants had read anything from our group. The maximum number of correct answers a question could get was 6, for the total number of participants, and there were 20 multiple choice questions available for this portion of the quiz.



The average number of correct answers per question was 2.2 on the first iteration. None of the user's answered questions 6, 7, 18, or 20 correctly, and the only questions with correct response rates above 4 out of 6 were questions 9, 13, and 17. Therefore we can assume that the users either knew the answers to these questions before the information provided by our group, or that they were able to infer this answer from the question or their previous experience. In the case of question 9, which asks if the user requires antivirus if they already have a firewall, it could be that the users understand the difference between antivirus software and firewalls. However given the much lower correct response rate to question 10, we can infer that is not the case. It is more likely that participants figured both were better than just one, or that they were lucky on the true/false question. Because of these discrepancies, we analyzed the questions in groups according to our goals outlined in the Methodology. Because of the vastly varying answers in the first iteration of this quiz, we decided that there was not a clear dominant goal that the participants understood well. Therefore, we hoped to improve the users understanding of worms overall. The following chart is the result of the second

iteration of the quiz, after the users had read the information sheet from our group.



This graph depicts the results of the second trial, where the participants did substantially better on the second quiz. There was only one question that fell below a 66.6% success rate, which was question 12. This question asked for the name of the computer worm that spread through e-mail messages, with the following options:

a) ILOVEYOU
b) Ramen
c) Morris
d) Blaster

Two users selected the Blaster worm, and one selected the Morris worm, when the correct answer was the ILOVEYOU worm. We believe that it might have been difficult for participants to remember the exact name of each worm attack, as well as their method of spreading. For the two that selected the Blaster worm, it would have been contradicted by their next answer, a true/false asking “The blaster worm spread through the Windows OS by identifying a vulnerability?”. However, because it was a true/false question, we are again taking into consideration that the participant may have been unsure and guessed the correct answer.

With regards to the sections mentioned in our methodology above, we believe that we managed to successfully educate the participants on definitions, worm components, examples, detection, and prevention. The questions that participants struggled the most on were not only the most difficult but the most specific of the recall multiple choice questions. Overall, there was a vast improvement in the scores from the first iteration of the quiz to the second.

The final component of our methodology that is not displayed in the graphs above is the scenario questions. We posed a scenario where an imaginary employee Bob received an ILOVEYOU email and proceeded to open the attachment against the advice of the firewall. Bob then proceeded to open his shared network folder, and the ILOVEYOU worm started to generate files in the folder, infecting the network. Upon learning that the infiltration started with Bob, he was unceremoniously fired.

4 of 6 participants were able to identify the worm name and the actions Bob should have taken to prevent this from happening. However, on the first iteration none of the participants were able to identify the type of worm that the ILOVEYOU worm is. On the second iteration, almost every participant was able to identify that the ILOVEYOU worm was neither an email worm, a file-sharing worm, nor an IM worm.

The question that was more interesting to our research was about whether or not Bob should have been fired. On the first iteration, only one participant agreed that Bob should have been fired, and this was a participant that was older and had worked in the software development industry several years ago.

Most of the participants were strongly against it, believing that it was a simple error. As a point of reference, many of the participants of this quiz were university students, who had not worked in a corporate situation, and therefore had a different view on the value of the items in a shared file system.

Following the information from our team, 3 of the 6 participants agreed that Bob should have been fired, as he compromised company files and possibly secure data on another person's computer. Of the three who disagreed, one stated that the company should have better antivirus software if the user can simply turn it off, or should have better screening of their emails. Another user was confused as to why Bob was allowed his personal email on his work computer, and claimed that if they were worried about security in the first place, that was more of a concern to them than the infiltration of the worm. One participant still believed it to be too harsh of a repercussion for a simple mistake, and that they should have been given another chance to prove themselves, or that Bob and all other employees should have been trained for such situations.

Future Works

The future goal with this quiz and its successors is to expand this type of education and knowledge to not only worms but to all types of malware to take some of the pressure off of network security teams and allow the users of a system to protect themselves. Given more time and resources we would have liked to develop a series of quizzes each focused around a different kind of network threat. These quizzes would have been more intensive and interactive allowing for the inclusion of custom made videos and other multimedia including infographics. These types of media would aid in the learning progress and help the quiz taker to retain the information they are learning to a greater extent.

Eventually we would like to have these quizzes be backed by either a technological organization or an educational institution as to give out a certificate upon completion. This would give our quizzes more weight in a professional work environment and allow the takers of the quiz to add it to their resume as a certification giving another incentive for their completion and therefore increasing the likelihood of mass adoption of these kinds of quizzes and practices.

The final goal of this quiz would be to get these kinds of practices implemented in any workplace where the employees have access to important systems and given the rate at which technologies have been implemented into the workplace this will soon become every workplace. These kind of training practices could go hand in hand with training protocols, such as the Workplace Hazardous Material Information Systems (WHMIS), to allow for a much safer workplace not only for the company's information but for the information of the employees as well.

Courses like this will keep people informed as to the nature of malicious software and allow stigmas to be destroyed. Many people believe that malware originates from viruses originate from sources such as illegally downloaded files or pornographic materials but in reality they normally originate from small business sites. By destroying these myths and stigmas we will help the average user to become more aware of the situations they face and help

them proactively avoid situations that put them in danger.

By working in combination with the advancing detection methods, such as the on-line monitoring systems that have been proposed to search for behavioural patterns in worms and allow for early detection, we may be able to slow the quel of these treacherous pieces of malware and reduce the stress on the security teams of large corporations especially those that hold very personal information [1].

Conclusion

In conclusion, we believe that there is a major lack of public understanding when it comes to cyber security and more specifically pieces of malware such as worms. Our study showed that people do not fully understand the seriousness of these attacks as in the scenario questions many believed Bob was unjustly fired. This shows that, despite his mistake costing the company potentially millions in damages depending on the size of the network, the quiz takers saw this as a mistake they could easily have committed themselves. This lack of understanding and ignorance to the dangers we impose on the systems we use needs to be fixed if we are to keep introducing these technologies to the workplace. Training systems must be put in place to make users aware of the consequences of these breaches and how they impact the company allowing the employees to take on some responsibility for their online actions and hopefully become more aware in their practices. In turn this education will also make the quiz takers practices at home become more secure and keep their own information safe not just with worms but other forms of malware as well. As long as there is people making malware we have to keep our employees and even our family members up to date to protect our information [9]. We must work together to understand the threats and keep one another accountable when it comes to online security and our privacy [9].

References

1. Chiarella, Davide. “WORM DETECTION: a Monitoring Behaviour Based System.” *DISI*, www.disi.unige.it/person/ChiarellaD/ChiarellaD-06-proposta.pdf.

2. Collins, Keith. “As Long as Humans Have Access to Email, Phishing Will Work.” *Quartz*, Quartz, 7 May 2017, qz.com/977085/as-long-as-humans-have-access-to-email-phishing-will-work/.

3. Gharibi, Wajeb. “Studying and Classification of the Most Significant Malicious Software .” *Jazan College*, arxiv.org/pdf/1106.0853.pdf.

4. “How to Avoid Virus, Phishing, Worm and Internet Scams?” *COMBOFIX*, 18 Mar. 2015, combofix.org/how-to-avoid-virus-phishing-worm-and-internet-scams.php.

5. Mackey, Niall. “Surprising Statistics About Computer Viruses.” *Topsec Cloud Solutions*, 3 Dec. 2014, 2:19:00 PM, www.topsec.com/it-security-news-and-info/surprising-statistics-about-computer-viruses.

6. Nazario, J. (2003). *Defence and Detection Strategies against Internet Worms*. Retrieved from

http://web.a.ebscohost.com.subzero.lib.uoguelph.ca/ehost/detail/detail?vid=0&sid=7d276990-d420-47a2-8ec9-7ad1732544fc%40sessionmgr4007&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=nlebk&AN=104653

7. “Phishing: How Many Take the Bait?” Get Cyber Safe / Pensez Cybersécurité, 4 Mar. 2015, www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx.

8. Shannon, Colleen. “The Spread of the Witty Worm.” CAIDA, 11 Apr. 2018, 16:00:55 PDT, www.caida.org/research/security/witty.

9. Weaver, Nicholas, et al. “A Taxonomy of Computer Worms.” Operating Systems: Security and Protection, 27 Oct. 2003, www1.icsi.berkeley.edu/~nweaver/papers/2003-taxonomy.pdf.

10. Weinberger, S. (2011). IS THIS THE START OF CYBERWARFARE. Nature; London, 474(7350), 142-145. Retrieved from https://search-proquest-com.subzero.lib.uoguelph.ca/docview/872363390/abstract/233D2F8AF7E24E06PQ/1?accountid=11233

11. Zou, Cliff, et al. “Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm.” Semantic Scholar, pdfs.semanticscholar.org/d149/2558458fab214d7825fe422f065dd1bf3734.pdf.

Quiz References

Danooct1,Email-Worm.Win32.Loveletter (ILOVEYOU Worm), 4 May. 2012, https://youtu.be/ZqkFfF5kAvw

Mithril Tortoise, The Morris Worm – 5 Minute Internet, 30 Sep. 2013, https://youtu.be/3x94Y787zfM

danooct1, Net-Worm.Win32.Blaster (thanks for 75k subs!), 17 Mar. 2016 https://youtu.be/ogyc6A9N3k0