**#Malware Spread Tactics**

##How does most malware spread?

Most malware spreads because we choose to interact with it. Sometimes it’s on purpose, sometimes it’s an accident. The ultimate fact is that humans are one of the defining factors that propagate the spread of malware. Most instances of malware transmission occur through means like email, the use of unnecessary software, unchecked administration usage, and the use of removable media[^1].

One of the biggest ways to guard against this, as per the NIST is to follow several guidelines:[^2]

* Don’t open suspicious emails, and be sure to have images set to \*\*NOT\*\* automatically download.
  + Reason being, sometimes the malware can be scripted into an image and executes when the image loads, thus running the malware and compromising the computer
* Ensure that files that are downloaded from sites are scanned and that they are less likely to be associated with malware[^3]
* Don’t use administrator-level accounts for regular system operations.

They seem like simple steps, but the difficult part for most corporations is implementing policies that actively control these actions. If a person does something that breaks the policy established that safeguards against these actions, they can compromise the entirety of the company's assets.

Microsoft also provides advice on how to prevent malware spread. When it comes to email, their advice establishes a few key takeaways:

* If you aren’t sure who sent you the email, or something doesn’t look quite right, don’t open it.[^4]
* Don’t open attachments to an email that you weren’t expecting, even if it appears to come from somebody you trust.[^5]

They even elaborate further on some of the office macros that can be run, one example being a scammer asking you to open a file and disable harm-preventing settings that would allow a malicious program to run and infect your computer.[^6] The takeaway is, if you have an issue, and you reach out to a company whose service you are using, they should never ask you to run a program in order to cancel a service.

The other piece of advice is to run security scans on peripheral devices that you use such as USB sticks, or external hard drives.[^7] If you don’t want malicious programs running on your computer, then treat everything that you plug into it that isn’t yours as a dangerous or infected machine.

##How does malware spread quickly and quietly?

Think of the internet. It doesn’t operate on a single server. That server would be massive! Instead, the viruses operate on a nodal basis. Nodes are the individual computers that comprise the entirety of the internet. These nodes can also consist of servers that host the domains that we access when we reference a website’s domain name. These domain name servers are what comprise the whole of the internet, and they are also where viruses are more commonly found.[^8]

So you may ask, why is it that viruses spread through these servers and infect more computers? It’s because not everyone has the ability to use the methods that we’ve talked about to protect the visitors to their websites. Even if they do, it’s impossible to create a perfect protection against all viruses. Zhao states “Accurately analyze the dynamic behavior of malware propagation is significant for the real-world applications, such as defend against the wireless malware, safeguard network security, ensure system stability and so on.”[^9]

##So how do we prevent it?

The act of preventing malware is more often than not more difficult than simply installing malware and sanitizing your emails. A lot of mathematical research goes into finding out just how malware spreads on a mathematical and statistical level too. For instance, the Mirai virus was the subject of heavy research, with groups going as far as to calculate the querying, that is requesting, of domain names by botnets designed to spread malware.[^10]

This gives us insight into what we would normally need to do. The advice that this learning management system offers is this. If you’re going to analyze the spread of any kind of malware, put it on a sandboxed network. Ensure that it isn’t connected to an active network, and then purposely infect your host computer. This way you can get your hands on the malicious code, see how it is executed, develop countermeasures by examining the exploits that it uses, and then cover those exploits by using methods outlined by the MITRE organization, or by other reputable sources.

Once you have those solutions in place, using a programming language, you would then create a script based program that either isolates or corrects affected systems, notifies the user, and then attempts to patch the error. This method is what companies use to prevent malware, and it’s the method that you would be using when developing your own solutions for yourself or a company that you work for.

Another thing to keep in mind is that viruses can have variants. These are the versions of the virus that are tweaked in order to use new exploits and vulnerabilities. If you don’t create a program that can regularly update based off of these vulnerabilities, your antivirus software would quickly become obsolete. This means that you need to be aware of current exploits, and use that awareness to generate new solutions, keeping up with cybersecurity news.

#Works Cited

[^1]Mell, P., Kent, K., & Nusbaum, J. (2005). Guide to malware incident prevention and handling (pp. 800-83). Gaithersburg, Maryland: US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

[^]Windows. (2022). *Protect your devices and data from malware*. Microsoft Support. Retrieved April 15, 2022, from https://support.microsoft.com/en-us/windows/how-malware-can-infect-your-pc-872bf025-623d-735d-1033-ea4d456fb76b

[^]Comodo. (2021, July 20). *What is malware in computer?: How does malware spread on computer?* Comodo Enterprise. Retrieved April 15, 2022, from https://enterprise.comodo.com/what-is-malware-in-computer.php

[^]MITRE. (2022). *Mitre ATT&CK®*. MITRE ATT&CK®. Retrieved April 15, 2022, from https://attack.mitre.org/

[^8][^9]Zhu, L., Zhao, H., & Wang, X. (2015, March 7). *Stability and bifurcation analysis in a delayed reaction–diffusion malware propagation model*. Computers & Mathematics with Applications. Retrieved April 15, 2022, from https://www.sciencedirect.com/science/article/pii/S0898122115000504#br000055

[10]Hwang, S.-Y., & Kim, J.-N. (2021). A Malware Distribution Simulator for the Verification of Network Threat Prevention Tools. *Sensors (14248220)*, *21*(21), 6983. https://ucark.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=153593359&site=ehost-live&scope=site