Marshall Eddy

CS331-001

Vincent Skimmer

19 September 2016

Affective Cyber Attacks

There are a lot of different types of attacks; and in that, there are several different levels of effectiveness for all the different types of attacks. We are going to talk about some of the more common ones and ones that are more effective for a business. Here are some of the more commonly used attacks that are quite effective: Socially engineered Trojans, Unpatched software, Phishing attacks, Network-traveling worms, and Advanced persistent threats.

Socially engineered Trojans are the number one method of attack. An end-user browses to a website usually trusted which prompts him or her to run a Trojan. Most of the time the website is a legitimate, innocent victim that has been temporarily compromised by hackers. Usually, the website tells users hey are infected by viruses and need to run fake antivirus software. Also, they’re nearly out of free disk space and need a fake disk defragger. Finally, they must install an otherwise unnecessary program, often a fake Adobe Reader or an equally well-known program. The user executes the malware, clicking past browser warnings that the program could possibly be harmful, and it is done. Socially engineered Trojans are responsible for hundreds of millions of successful hacks each year. There are ways you can prevent these attacks.

Socially engineered Trojans are best handled through end-user education that’s informed by today’s threats, such as trusted websites prompting users to run Trojans). Organizations can further protect themselves by not allowing elevated users to surf the Web or answer email.

The next most common attack is software with known, but unpatched exploits. The most common unpatched and exploited programs are Java, Adobe Reader, and Adobe Flash. It’s been this way for a while. “Not a single company I’ve ever audited has ever had these three programs perfectly patched. I just don’t get it” (infoworld). The best way to prevent this is by simply patching, patching, and more patching.

Then there are Phishing attacks. Approximately 70 percent of email is spam. However, anti-spam vendors have made great strides, so must of us have reasonably clean inboxes. Regardless, everyone gets spam every day and some of them are most likely to be some pretty crafty phishing replicas of legitimist emails. Everything looks great; it even warns the reader not to fall for fraudulent emails. The only thing that gives them away is the rouge link asking for confidential information. The best way to decrease the risk from phishing attacks is mostly accomplished through better end-user education, and with better anti-phishing tools. Making sure ones’ browser has anti-phishing capabilities (like google chrome).

Network-traveling worms are the new viruses. Most organizations have had to fight worms such as Conflicker and Zeus. The network-traveling worms are much better at hiding in comparison to the email counterpart. Network-traveling worms can be defeated by blocking executables in email, better patching, disabling auto-run capabilities, and strong password policies. Many network worms, like Conflicker, will try to exploit network shares by logging on using a list of built-in, bad passwords like: 12345, password2, qwerty, and so on. So, having a solid password that is not something someone could guess.

Finally, there is an APT (advanced persistent threat) which steals intellectual property, and almost every major organization has been hit with this type of attack. APTs usually gain a foothold using socially engineering Trojans or phishing attacks. A very popular method is for APT attackers to send a very specific phishing scam, known as spear-phishing, to multiple employee email addresses. The phishing email contains a Trojan attachment, which at least one employee will usually be tricked into running. After the initial execution and first computer takeover, APT attackers can compromise an entire enterprise in a matter of hours. It’s easy to accomplish, but extremely difficult to clean up.

The countermeasure for APT, detecting and preventing, can be difficult, especially in the face of a determined adversary. All the previous advice applies, but you must also learn to understand the legitimate network traffic patterns in your network and alert on unexpected flows. An APT doesn’t understand which computers normally talk to which other computers, but you do. Take the time now to start tracking your network flows and get a good handle of what traffic should be going from where to where. An APT will mess up and attempt to copy large amounts of data from a server to some other computer where that server does not normally communicate. When they do, you can catch them.