Marshall Eddy

CS332-002

Vincent Skimmer

25 January 2017

Penetration Attacks

Some of the more common attacks on companies’ infrastructures are phishing, RATs, and ransomware attacks. These are all fairly easy ways to steal information from a company and to jeopardize their servers as a whole. However, there are certainly ways to prevent such attacks, but you need to know what to do and how the attacks themselves work.

**Phishing**

“Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reason, by masquerading as a trustworthy entity in an electronic communication” according to Wikipedia. Essentially, Phishing is any way someone obtains data from an unsuspecting user via any sort of “bait”, such as links to a clone of a common website, that is then used obtain login information and then from there all sorts of other information. There are several different types of phishing, such as clone phishing, spear phishing and whaling.

Clone phishing is done by taking any sort of commonly used website or email with an attachment and slightly changing the website’s URL or email attachment to be a malicious link. Spear phishing is when the phishing attack is directed at specific individuals to obtain their information and credentials to then obtain potentially more important/useful information. Whaling is where the phishing attack is specifically directed at senior executives and other high profile people within a business to be able to obtain their credentials, which would allow them to gain information simply by asking one of their “employees” or if the attacker is lucky, the executive will have Dom-Admin. Whaling is effective since most of the time, executives are not very knowledgeable about cyber attacks/scams or how to prevent them.

There are ways to prevent these phishing attacks, and protect the information within a business, one of the more effective strategies is to teach employees within a company on how to spot phishing attacks, especially if their credentials would allow the hacker access to a lot more information (Dom-Admin/executives). Web filters also help prevent phishing websites from being utilized, and the most effective way to use a web filter for this purpose would be a white list. Two-factor authentication is another great way to prevent phishing attacks from gaining access to accounts since there would be no way for them to access the code from your phone, and it would be different every time you would login. There are many more ways to prevent phishing, such as spam filters and utilizing browsers that alert users to fraudulent website; however, these are some of the more common/best solutions out there.

**RATs**

“RATs, or Remote Access Trojan, are very common and designed to provide the attacker with complete control over the victim’s system”, according to darkreading.com. They are used to steal information, spy on victims and remotely control infected computers to use them in other malicious attacks, such as DDOS attacks. RATs are hard to detect since they open legitimate network ports on the infected machines, and since this is a very common operation then it is essentially obsolete when attempting to find the RAT. They resemble legitimate commercial remote admin tools, as well as perform operations that do not resemble common malware techniques.

Darkreading.com has a list of the seven most common RATS in use today, here are a few of them:

*“Sakula* is believed to be associated with the recent OPM attack. It is signed, looks like benign software, and provides the attacker with remote administration capabilities over the victim machine. Sakula initiates simple HTTP requests when communicating with its command and control (C&C) server. The RAT uses a tool called “mimkatz” to perform “pass the hash” authentication, which sends the hash to the remote server instead of the associated plaintext password.”

*“KjW0rm* is believed to be associated with the recent breach of TV stations in France. KjW0rm was written in VBS, which makes it even harder to detect. The Trojan creates a backdoor that allows the attacker to take control of the machine, extract information, and send it back to the C&C server.”

“*Havex* targets industrial control systems (ICS). It is very sophisticated and provides the attacker with full control over the infected machine. Havex uses different variants (mutations) and is very stealthy. The communication with its C&C server is established over HTTP and HTTPS. Its footprint inside the victim machine is minimal.”

Unfortunately, these newer RATs are quite difficult to detect since they resemble commercial remote administration software. Traditional protection mechanisms that rely on static signatures are typically unable to detect the execution of malicious activity has proven to be an effective approach for sniffing out a rat.

**Ransomware**

“Ransomware is computer malware that installs covertly on a victim’s computer, executes a crypto-virology attack that adversely affects it, and demands a ransom payment to restore it” (Wikipedia). Some simple ransomware will lock the system, which would not be difficult for someone to reverse is they knew what they were doing, and then display a message saying that it is required to make a payment to restore their computer. These attacks can get more advanced by actually encrypting all the files on the system, thus making it harder for them to reverse the attack and feel more like they have to pay to decrypt their files. Depending on the level of encryption it might be impossible to decrypt without a decryption key, making it a much more effective attack.

It is difficult to detect these types of attacks before they happen, making them quite a nuisance. The best defense for these attacks is to always have a backup of all your files on an external storage device that could not be remotely accessed.

References

<https://en.wikipedia.org/wiki/Phishing>

<http://www.darkreading.com/perimeter/the-7-most-common-rats-in-use-today-/a/d-id/1321965>

<https://en.wikipedia.org/wiki/Ransomware>

References

[SOURCES]