Watering Hole Attacks

By:

Raymond Fradella
Abstract

The problem with watering hole attacks is that it gets past your security by attacking through a weaker security that you have no control over.

It is an interesting problem because you have to find a way to secure your system assuming an attack will already bypass your restrictions.

My solution will prevent watering hole attacks from working by preventing their access to the network that has the company property.

Using my solution I found that the watering hole attacks were not successful.
1. Introduction
2. Preliminaries
3. Problem Description
   a. Drawbacks of the previous approaches
   b. Cyber Threat(s) to Resolve
4. My Approach to Cyber Defense
5. Implementation/Proof
6. Conclusion
7. References
I. Introduction

Cyber attacks are becoming a common occurrence in this technological age. Attacks that seek to steal your identity and information, to sell to the highest bidder. Watering hole attacks can be disastrous for an organization. A watering hole attack lets the attacker bypass most of the security that would normally be put in place. Things like cameras, guards, passwords, and security doors can all be avoided by using a watering hole attack.

A watering hole attack is a type of phishing attack in which the attacker would first gather intelligence on the victim. The attacker would be looking for what websites the victim frequents and if and where the victim uses unsecure wifi on a constant bases. With this information gathered the attacker now knows his best attack vector, and will proceed to inject his malicious code onto the site. The next time the victim or anyone else visits the site they will have the malicious code dropped on there device. The attacker can now do two things, he can attack using the victims device or he can wait and see if the victim connects to a business network and attack the business. If he attacks the business he will have avoided every security door, guard, camera, and password that would normally be required.

II. Preliminaries

"Jia Xu and Danping Zhou proposed an early APT attack stage model in 2014. They divided APT attacks into six stages. First stage is intelligence gathering, the attackers spend a lot of time and resources collecting the target information, relying on the internet, active scan, and social engineering methods, and so on; Second stage is directional invasion, attackers break into the target network through phishing emails, SQL injection, mobile storage devices and any other methods to carry out directional zero-day attacks; Third stage is remote control, by installing back door programs or Trojan programs, attackers control the users’ computers and keep communication with the control servers via the network communication protocols; Next stage is lateral movement, attackers will use vulnerability scanning, listen to network traffic for password, embedded remote control tool (RAT) and other
methods continue to search important computers which store sensitive information; And the following stage is data mining, APT lurks for a long time quietly, manual data analysis for valuable data; The final stage is data theft or system destruction, attackers send sensitive data back to the specified servers, or do damage to critical systems quietly. "[2]

"For an APT actor attempting to infiltrate an organizational network, one effective approach is to compromise the site frequently visited by the employees and use it as an infection vector to disseminate malware."[3]

III Problem description
To launch a watering hole attack the attacker puts malicious code on a site, with the intent of infecting computer systems. Once infected and connected to a network the malicious code could transfer to other systems. There are proposed solutions to these attacks but they rely on solving the problem when it happens, instead of preventing it.

Using the six stage attack model which details the steps of the attacks is great for knowing which part of the process you are affected by and having an idea of how to prevent it at that stage. The other option of compromising the site frequently to learn the holes that need to be patched is also good with the exception of the fact that there will always be more holes than you can fix, and the attacker will find them before you do.

The problem with these approaches in my mind is that they look to solve the problem after the fact, which in my opinion is too late. You would want to prevent the problem from happening, not just recover from it. The other problem is that you have to prevent the problem in a cost effective manor.

My approach will prevent the problem from occurring and thus make it not a problem.

IV My Approach
My approach required two separate internet sources and a white list. The white list would have only a few acceptable sites available to the company computers. Even if the attack got past the white list it would still need to pass the firewall and anti-virus programs.
V. Implementation

I used Wireshark to trace the attack I launched using Kali linux penetration tools. I monitored as the packets traversed the system and breaked at the whitelist, for most sites. The test was run using one network at a time to ensure there was no interference in the results. One network has a hard line connection to an intranet, which would require a LAN connection. This connection would also be restricted in the sites that could be visited by using a white list. The white list would contain the only sites that would be permitted to be visited on the network. Past the white list and the intranet would be a firewall and anti-virus and anti-malware programs.

The other connection would be wireless and using a different network that was completely separate from the first. This ensures that there is no chance that information can be stolen over the network from an external weaker network. Any external device that was used like a phone, tablet, or computer, would have to use the wireless connection.
By setting up the networks this way it prevents even infected devices from accessing the network with all of the company information. Also since the hard line connections would be connected to an intranet it would be another level of separation the attacker would have to get through. Even past the intranet the attacker would have to get past even more security in the firewall and as a last resort the anti-malware programs.

VI. Conclusion

Watering hole attacks are one type of cyber-attack that every organization should be prepared for. They are extremely easy for the attacker to use and hard to defend against. My approach will help to defend against these types of attacks. Multiple approaches should be utilized when it comes to securing your systems from attacks for best results.
References


