**Watering Hole Attacks**

**By *Tahshina Mohsin***

**What is a Watering Hole Attack?**

Now that phishing has become a widely understood and common phenomenon throughout the world, many users are getting smarter about responding to emails. As a result, cyber criminals are seeing fewer desired results with such techniques. In a phishing email, a cyber-criminal intends to trick the receiver into providing his/her sensitive information or clicking a malicious link. In a variation of phishing — watering hole attack — instead of attacking the prey, the cyber criminals set up a trap for the user and wait for the prey to come to them.

The term “watering hole attack” refers to predators in nature that lurk near watering holes in the hope of attacking a prey nearby. In the cyber world, these predators stay on the prowl near websites which are frequently visited by their prey. They wait for an opportunity to infect these websites with malware to make their target vulnerable.

It won’t be wrong to compare watering hole attacks with spear phishing attacks, as in both cases, the prey is normally a group of employees of a large setup or government offices – and the aim is to gather their sensitive information. Though not as common as spear phishing, they pose a high risk as they cannot be easily detected and usually target connected vendors, business partners, or employees with low security systems.

**How is a Watering Hole Attack Carried Out?**

To understand it better, let us look at the step breakdown carried out to complete a successful watering hole attack.

1. **Finding the Target:** The attacker finds out a target organization, but cannot attack head-on because of its tightened security.
2. **Discovering frequently visited websites of the target:** The attacker – with the help of internet tracking tools like KISSmetrics and AddThis – then discovers the websites frequented by the users of their target organization.
3. **Embedding the Malware:** The attacker then finds out vulnerabilities in those websites and plants malicious HTML or JavaScript code which redirects target users to a different website hosting the malware. The attacker then waits for the user to visit the website and upon access, malware is injected into the user’s system.
4. **Identifying vulnerabilities in User Machines:** Malware looks for vulnerabilities – outdated antivirus or browser – in the user system, and informs the attacker of the discovered vulnerabilities.
5. **Delivering the Exploit:** The target system receives the exploit by the attacker.
6. **Accessing information from the Target:** From here onwards, the user can access sensitive information of the target for personal gain, to steal financial data, to carry out a fraudulent activity or even further sell it away to criminals.

**Why Watering Hole Attacks Work?**

While spear phishing attacks may or may not work, watering hole attacks certainly do. They question is, why? The answer – simply because attackers can easily get information about which websites and links users click with the help of web analytics tools. Most of the time the attackers compromise legitimate websites which are not blacklisted and can be effectively used to deliver malware. They exploit zero-day vulnerabilities which cannot be detected by anti-virus and have no IDS signatures. It would certainly not look feasible if you ban your mobile developers to look online for an important resource that they require to get their job done. Again, you cannot stop a government official from contributing to an online policy resource. Hackers understand this, and this is how they succeed in conducting successful watering hole attacks.

**What is the Impact of Watering Hole Attacks?**

Unlike other social engineering techniques, a watering hole attack is strategically planned. Rather than targeting random websites, the attackers carefully select legitimate and trustworthy ones to compromise. Relying on visiting trusted sites alone to avoid online threat can no more be considered as a safe practice. Other than financial loss and leakage of critical information, watering hole attack can also impact the organizational operations. If a watering hole attack is successful in dropping a Remote Access Trojan (RAT), the attacker can also get to carry out commands on the infected servers. This can include monitoring and spying the target organization’s activities. Once the attackers infiltrate into the network, they can also modify or delete crucial files and initiate harmful attacks resulting in huge losses to the organization.

**Real Life Examples**

In the past few years, some high-profile incidents of watering hole attacks have been documented. Let us look at some of those.

In mid of 2012, a campaign called VOHO was identified by RSA, which aimed a specific group of organizations – particularly local government agencies and businesses in some specific geographical locations. Attackers selected the sites carefully and inserted malicious JavaScript, thus delivering a Gh0st RAT variant.

In December 2012, the website of Council of Foreign Relations (CFR) was compromised by attackers who hosted a zero-day exploit in the Internet Explorer. Visitors were dispensed with backdoor malware.

In November 2014, a group of Chinese attackers infected Forbes website and targeted visitors from US defense and financial service industry. The Advanced Persistent Threat (APT) exploited two zero-day vulnerabilities. One was in Microsoft Internet Explorer and the other in Adobe Flash Player. The campaign appeared to last only for a few days, but the possibility of it staying for a longer period of time could not be ruled out.

**Watering Hole VS Spear Phishing**

It’s been a while now that watering hole attacks have been proven to be successful attack strategy by hackers. After analyzing some of the prominent examples of these attacks, many in the industry now consider them to be a preferable alternative to spear phishing. But the truth is that, like many other tools, both spear phishing and watering hole attacks have their own strengths and weaknesses and may work better than the other in specific situations. Instead of considering watering hole attacks as a replacement, they can better be seen as an additional technique at the disposal of cyber criminals.

These attacks do have a competitive edge though – and that is – their ability to work without employing exhaustive social engineering techniques. It involves lesser work on part of the attacker and only requires compromising a website that is frequented by the target users. But then again, once a large number of users visiting the website are compromised, the flood of information gets difficult to be handled. The attackers then need to thoroughly scan huge data and break it down to find valuable information.

On the other hand, spear phishing allows attackers to focus on specific targets and gather precise information. In case a spear phishing attack is successful, it grants immediate access to the target’s system. Though spear phishing can exploit zero-days to inject malware on hosts, it does not depend upon vulnerabilities to do that. However, a spear phishing attack requires careful social engineering techniques to identify targets and its success depends only upon how well-crafted and seemingly genuine an email is – so as to compel the target to respond positively.

**How to Prevent a Watering Hole Attack?**

Although not necessary, watering hole attacks usually make use of new tactics and exploits that are unknown to signature-based approaches, which rely on past knowledge of threats. To ensure advanced security levels, organizations need to put in additional layers of protection – like behavioral analysis – which has a higher probability to detect these zero-day threats.

Let us look at some prevention measures organizations can take to minimize the occurrence of watering hole attacks.

**Updating Software Regularly**

Although watering hole attacks are usually carried out with new exploits and vulnerabilities, keeping systems up to date with latest software patches can reduce the probability of those employing old vulnerabilities for the attack.

**Shielding Vulnerabilities with Virtual Patching**

Virtual patching is the act of shielding new vulnerabilities as they are discovered, before they can be exploited. Software vulnerabilities are discovered every month. It is often impossible or too expensive to develop timely patching solution for them. Virtual patching makes use of intrusion detection and prevention systems to shield the vulnerabilities before being exploited. This can help you in getting immediate protection of your endpoints and servers before patches can be set up.

**Detecting Suspicious Network Traffic**

Regardless of the exploits launched by the attackers, traffic generated by the malware during communication with command-and-control server remains steady. With the help of Network Traffic Analysis tools, such communications can be detected and security measures can be implemented by organizations to decelerate the attack.

**Scanning Websites for Malware Detection**

Large enterprises, on their behalf, should implement processes to ensure that their websites are malware-free and not used for conducting watering hole attacks. Some of the techniques that are used for securing Web 2.0 widgets can be used for malware detection as well. Other than that, services by Internet security providers – such as Commodo and GeoTrust – can be attained for daily scanning of websites for potential malware.

On the other hand, organizations that suspect being a target of such attacks should monitor and inspect top websites favored by their employees on a regular basis. If the monitoring system detects malicious links, block the traffic and warn the user. More preferably so, block the site if it continues to host malware, and contact their admin.

**Some Useful Tips to Follow:**

* Identify and block all the analytics trackers that are monitoring your user activity e.g. KISSmetrics, AddThis, Chartbeat, etc.
* Blog http redirect by using browser plugins
* Allow “auto-updates” of web browsers
* Maintain the visibility of all tracking services being used - to identify and block any new services
* Use Web Application Firewalls from trusted vendors with cross-site scripting, SQL injection and command injection rules in the deny mode
* Restrict access to your Content Management System to specific geographical areas
* Create a plan to disable third-party content such as advertisements, etc. in case its provider gets compromised
* Secure your name servers and DNS registration to prevent attackers from redirecting your domain to arbitrary locations