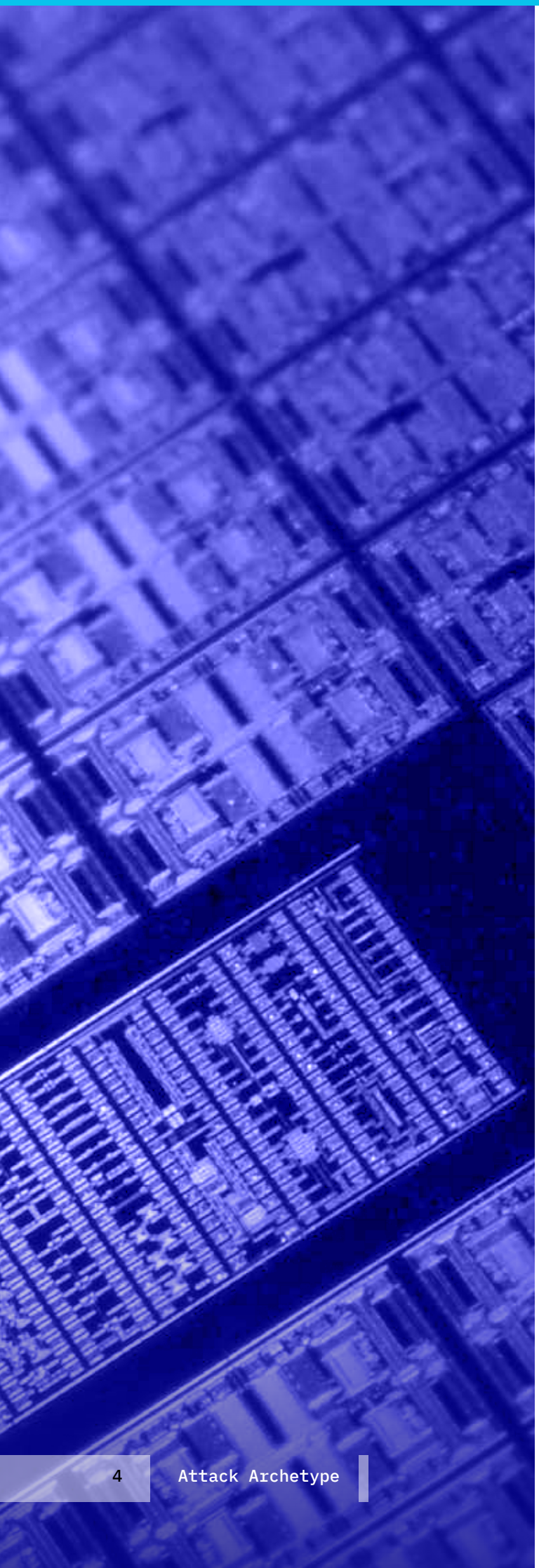
Attack Archetype

Watering Hole


Internews

Table of Contents



Introduction

This archetype describes a particular adversary tactic of attacking indirectly through a website or system that the victim is likely to visit. A direct attack is difficult. Therefore, compromising a website with weak defenses and loading it up with one or more exploits and then waiting for the victim to visit it can be quite effective. A prime example of this type of attack is the group of compromised websites that were loaded with iOS iPhone exploits, all of which were targeting Uyghurs in China.[1] A watering hole attack may actually compromise more individuals than the adversary is aiming for. However, among that group is likely to be the victims that are actually being targeted.

Types of Attack

In essence, a watering hole attack resembles a drive-by download attack in that both employ a website and both use an exploit to deliver malware to the victim's computer. The difference is in the delivery. A drive-by is actively sent to the victim in a malicious communication. A watering hole attack is passive: the exploit is set up on the website and it waits for the victim to visit.

The major types of watering hole attack, therefore, can be categorized in two main ways:

- The technology targeted by the exploit: browser, OS, plugins, phone, or computer.
- Direct exploit or replacing files to be downloaded with trojanized versions.

1 https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

This second type is also a form of supply chain attack. This form of watering hole attack is where a legitimate document for download is replaced with a malicious document that then installs malware on the victim's computer. Alternatively, this second form of watering hole attack can target a particular software that the victim is known to use. The legitimate update of that software is replaced with a trojan. A famous example of this kind of software download replacement is the CCleaner attack in 2017.[2]

Targeted Individuals and Organizations

Watering hole attacks can affect any type of organization or any specific individual, but according to the 2020 Microsoft Digital Defense Report, "nation state activity is significantly more likely to target organizations outside of the critical infrastructure sectors. The most frequently targeted sector has been non-governmental organizations (NGOs), such as advocacy groups, human rights organizations, nonprofit organizations, and think tanks focused on public policy, international affairs, or security."[3]

However, in addition to the victims that an adversary is aiming for, a watering hole attack can affect all the visitors to the watering hole, not just the intended victims.

2 https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

3 https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738

Social, Political, and Economic Context

The context around a particular watering hole attack is very important to understanding the attack. A watering hole attack relies almost entirely on understanding what sites a victim visits frequently and why. Many watering hole attacks utilize government websites that the victim will definitely visit. Others leverage news sites or blogs that have topics of focus that the victim is known to have an interest in. Many times, these types of sites have lax defenses and require less effort to compromise than a direct attack on the victim would require.

Community Context

Careful attention to and communication about watering hole attacks can help prevent further attacks once one has been identified. It can be difficult to detect an infected website that has some type of exploit kit[4] installed on it. However, once it has been identified, sharing this threat data with other organizations in the community is critical. This type of sharing can prevent other organizations from encountering the same malicious watering hole, especially since this type of attack is more general and can, in effect, target an entire community that all utilize the same watering hole.

4 https://en.wikipedia.org/wiki/Exploit_kit

Attack Impact

Because this type of attack is more of a particular delivery method than a radically different attack, the impacts are identical to other types of malware attacks. The impact of a malware attack can be severe if undetected. Malware capabilities with the goal of avoiding detection can allow an adversary to maintain access to the victim's computer for long periods of time. Over the course of this, the adversary can download files and data from the victim's computer, monitor the victim's actions, record keystrokes, and take screenshots, among many other potential actions.

In addition to direct impacts to the organization or individuals being targeted, a watering hole attack can affect all other organizations and individuals that also frequent the compromised online resource. Even if the adversary is targeting one organization or individual, these types of attacks can affect the entire community as well as that organization's peers.

Some of the most worrisome impacts of an attack can include, but are not limited to, the following:

- Keylogger records the victim's keystrokes.
- Web inject changes what the victim sees when they visit a legitimate website.
- Files and data are downloaded from the victim's computer.
- Victim's files are modified by the adversary.
- Audio and video from the microphone and camera on the victim's computer are recorded surreptitiously.
- Other computers and systems on the same network as the victim's computer are compromised by the adversary during lateral movement.
- Other organizations and individuals in the entire community are affected.

Process of the Attack

A watering hole attack requires much more reconnaissance effort on the part of the adversary than other types of direct attack. The online habits of the victim must be stud-

ied carefully, and locations that the victim is most likely to visit are selected. The steps in one scenario are the following:

- The adversary makes a list of websites that the target is likely to visit.
- Additionally, the adversary has discovered the IP address of the victim.
- Each of the possible sites are probed for vulnerabilities and ones that are easier to compromise rise in the list and ones that are not obviously vulnerable fall off the list.
- For this example, the adversary finds that the website of a local news station is using an old version of a Wordpress plugin that is vulnerable to exploitation.
- The adversary exploits this vulnerability and gains access to the web server.
- Next, the known IP of the victim is used to scan the website's logs whereby the adversary discovers the version of the web browser the victim is using from the user agent field of the logs.
- As the news site publishes stories, each of these pages now loads an additional blob of javascript that runs an exploit that targets the version of web browser the victim uses.
- The malware runs on the victim's computer and installs a copy of itself in a persistent way.
- The command and control infrastructure of the adversary now has direct access to the victim's computer.
- The malware reports back to the command and control infrastructure the names of directories and files on the victim's computer.

Prevention

Since a watering hole attack is a special case of malware or phishing attack, in addition to the standard preventions and mitigations used for each of those two types of attack, a watering hole attack should be reported properly to the responsible party. This can prevent other organizations and individuals from being victimized by visiting the same site.

If the resources and time are available, working through an abuse reporting process can get the malicious website cleaned up or taken down. This can be as simple as looking up the abuse email address on abuse.net and reporting the website to the responsible party.[5]

> Care should be given to not reveal any sensitive information even to a hosting provider when submitting an abuse report.

In addition to reporting to the responsible party, the malicious URL can be reported to one of the Google Safe Browsing forms depending on whether the malicious URL leads to phishing[6] or malware[7]. Additional resources for reporting abuse in a variety of ways can be found here.[8]

5 https://www.abuse.net/

6 https://safebrowsing.google.com/safebrowsing/report_phish/

7 https://safebrowsing.google.com/safebrowsing/report_badware/

8 https://decentsecurity.com/#/malware-web-and-phishing-investigation/


Internews