Attack Archetype

Website Compromise
# Table of Contents

- Introduction .................................................................................. 4
- Types of Attack ............................................................................. 4
- Targeted Organizations ................................................................. 5
- Social, Political, and Economic Context ....................................... 5
- Community Context ....................................................................... 6
- Attack Impact ................................................................................ 6
- Process of the Attack .................................................................... 7
- Prevention ..................................................................................... 8
Introduction

This archetype describes a type of attack where the adversary has gained access to an organization’s website and has changed the content of the site in some way. This type of attack can be targeted or can be opportunistic. The focus of this archetype is the former: a targeted website compromise. Most of the time, this type of attack is not directly targeting the victim organization and isn’t meant to be detected, or at least not meant to be detected for as long as possible. These types of website compromise are actually a component in another attack targeting a third party and entail the content of the victim website being changed to host malware files for download or phishing content used in other campaigns. The more targeted variety of website compromise is a defacement where the adversary changes the front page or other pages of the website to display a message of some type. This second type of attack has the goal of threatening, discrediting, or intimidating the victim through a type of vandalism.

Types of Attack

The basic types of website compromise can be differentiated by what content on the website is changed and why. The primary form of targeted attack is a website defacement.1 However, the more prevalent type of attack is a website compromise with the intent of serving malware or phishing content to a third target. This latter type is not typically aimed at the entity which owns the website, even if the action is taken by a state sponsored adversary. Compromises that are used as a component of a different attack are typically selected via mass scan-

1 https://en.wikipedia.org/wiki/Website_defacement
ning the internet for vulnerable websites. Sites that fit the profile are then compromised using automated processes.

On the other hand, a website defacement is almost always a targeted attack. These are in essence a form of vandalism which rarely lead to further compromise of a victim’s computer or network. The reason for this is that most websites are hosted separately from a victim’s own network and computer, thus inherently containing the damage.

### Targeted Organizations

As opposed to other types of attack, a website compromise is typically aimed at organizations due to the higher likelihood of an organization operating a website than an individual. As far as the type of organizations that are targeted, website compromise 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, non-profit organizations, and think tanks focused on public policy, international affairs, or security.”

### Social, Political, and Economic Context

Most website compromises that are defacements tend to be an adversary that has a perceived grievance with the organization they target. However, these adversaries may be funded by or operating with a nation state which also wants to suppress, harass, intimidate, or discredit this same organization and use this adversary to achieve these ends. Alternatively, a nation state adversary may masquerade as hacktivists also to suppress, harass, intimidate, or discredit the victim organization. “An often-overlooked dimension of cyber espionage is the targeting of civil society actors. NGOs, exile organizations, political movements, and other public interest coalitions have for

---

4. [https://securitytrails.com/blog/dns-hijacking](https://securitytrails.com/blog/dns-hijacking)
5. [https://owasp.org/www-community/attacks/]
many years encountered serious and persistent cyber assaults. Such threats — politically motivated and often with strong links to authoritarian regimes — include website defacements...”

Community Context

Careful attention to and communication about website compromises can help prevent further attacks once one has been identified. If one organization or individual within a community is targeted by a website compromise, other organizations may be targeted by the same adversary at the same time or shortly afterwards.

Free websites that categorize vulnerabilities according to technology and version are available at CVE Details8 and VulDB9.

Attack Impact

Aside from the direct impact of damaging the website content in the case of a defacement type of website compromise, if the type of attack is an adversary using the website to launch other phishing and malware attacks, the IP address and domain reputation can be lowered. Once a website has been detected as serving malware or phishing content, it may be added to blocklists which can then impact the organization’s operations. The former, due to the nature of the website being defaced, is easily detected. However, the latter is not meant to be detected, or at least not detected quickly. Therefore, the longer the malicious content remains on the website, the more blocklists the domain and IP will be added to. Recovering from this can be difficult because of the distributed nature of blocklists: there are many different organizations which maintain these lists, and their responsiveness to requests to delist are varied. Using one of the aggregation sites10 to check across as many11 as possible is a good place to start if an IP or domain has been listed.

In addition to the direct impact a website compromise can have on an organization, there are secondary impacts that this type of attack can have on the organization’s reputation among its peers and funding sources. For a website defacement, this type of reputational damage can be one of the goals of the adversary in the first place.

---

7 http://www.circleid.com/posts/20130304_civil_society_hung_out_to_dry_in_global_cyber_espionage/
8 https://www.cvedetails.com/
9 https://vuldb.com/
10 https://iplists.firehol.org/
11 https://mxtoolbox.com/blacklists.aspx
Process of the Attack

Website compromises can start in a few different ways. Credentials that allow access to update content on the website may be stolen from the victim via a phishing attack. Alternatively, the password used may be weak, and the adversary used a brute-force process to discover the password through a repeated and structured guessing process. Another similar method is to try passwords found in credential dumps to see if they have been reused by the victim.

Another place the adversary can begin is with an exploit of a particular website vulnerability such as cross site scripting or SQL injection. In these cases, the adversary typically exploits the vulnerability and then installs a web shell that is tailored to the technology used to serve the website such as PHP or ASP.12 The webshell then gives the adversary full access to modify the content on the website without using the website’s own administration tools or access.

Once access is gained by the adversary, the next steps depend on the type of attack. If the aim is to vandalize or deface the website, the front page of the site is typically replaced with a new page that displays the attacker’s message. Alternatively, if the adversary is using the compromised website to serve phishing pages, those pages are typically not able to be navigated to from the legitimate website. This is to prevent detection for as long as possible. With the case of a website compromise with the aim of serving malware payloads, these are typically executables, archives, or obfuscated data files that are then downloaded as a component in a malware attack chain.

Something to really keep in mind with regards to website compromise is that most of these types of attacks are opportunistic and automated. Except for defacements, they typically target a third party. It is most important to make sure to maintain good off-site backups of the website and work out a disaster plan for what steps need to be taken in the event of a website compromise.

12 https://en.wikipedia.org/wiki/Web_shell
Prevention

A list of the top ten proactive security controls to prevent website compromise are provided by the Open Web Application Security Project (OWASP). Those ten controls are the following:

- Define Security Requirements
- Leverage Security Frameworks and Libraries
- Secure Database Access
- Encode and Escape Data
- Validate All Inputs
- Implement Digital Identity
- Enforce Access Controls
- Protect Data Everywhere
- Implement Security Logging and Monitoring
- Handle All Errors and Exceptions

Details about these controls and information about best practices and methods of implementation can be found on OWASP’s website.13

The above security controls and processes may seem daunting to implement and are geared towards development of the website in addition to hosting. There are, however, two simple security controls that are easy to implement and can prevent many types of attacks. First is to make sure that administration credentials use strong passwords or SSH keys. If passwords must be used, make sure to store and share the password using a password manager. Second is to use a web application firewall (WAF). Depending on the software used to serve the website, an open source WAF such as ModSecurity can be used.14 Alternatively, a cloud service can be used regardless of software used to serve the website. Free services such as Cloudflare are available which also provide DDoS protection.15 Or, if the organization that owns the website qualifies, Jigsaw’s Project Shield can be an option.16

13 https://owasp.org/www-project-proactive-controls/
14 https://modsecurity.org/
15 https://www.cloudflare.com/
16 https://projectshield.withgoogle.com/landing