<https://www.fortinet.com/resources/cyberglossary/watering-hole-attack>

**What is a Watering Hole Attack? <** Description of Watering Hole Attacks **>**

A computer attack strategy in which an attacker guesses or observes websites an organization often uses and infects one or more of the websites with malware.

(Think of a crocodile that waits for prey at the watering holes.)

A watering hole attack differs from phishing and spear-phishing attacks, which typically attempt to steal data or install malware onto users’ devices but are often equally targeted, effective, and challenging to prevent.

A phishing attack is a type of cybersecurity threat that targets users directly through email, text, or direct messages. Spear-phishing attacks are highly targeted, hugely effective, and difficult to prevent.

**Pg4** Watering hole attacks target legitimate websites that cannot be blacklisted, and cyber criminals deploy zero-day exploits that antivirus detectors and scanners will not pick up.

**How Does a Watering Hole Attack Work? <** Techniques used in Watering Hole Attacks **>**

In a watering hole attack, cyber criminals lurk (wait in a place) on legitimate websites and for an opportunity to target victims.

Normally attackers driven by financial gain or to build a botnet can compromise popular consumer websites; visited by professionals from specific industries: discussion boards, industry conferences, and industry-standard bodies.

Attackers profile their targets, who are often employees of large organizations or government agencies and discover the websites they tend to visit most frequently.

**Pg6** Attacker searches for a vulnerability within a site, creates an exploit to compromise it, infects the website, and lurks in wait for a victim.

Websites are injected with malicious Hypertext Markup Language (HTML) or JavaScript code which redirects victims to a spoofed website that hosts the attacker’s malware.

<https://www.malwarebytes.com/spoofing>

**Spoofed:** Spoofing, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, money, or spread malware. Spoofing attacks come in many forms: Website and/or URL spoofing, Email spoofing, Caller ID spoofing, Text message spoofing, GPS spoofing, Man-in-the-middle attacks, Extension spoofing, IP spoofing, Facial spoofing

Fraudsters rely on the naiveté of their victims, if you never doubt the legitimacy of a website and never suspect an email of being faked, then you're likely to become a victim of a spoofing attack at some point.

**Website spoofing:** is all about making a malicious website look like a legitimate one. The spoofed site’s login page will look like that of the website you frequent—down to the branding, user interface, and even a spoofed domain name that looks the same at first glance. A spoofed website will generally be used in conjunction with an email spoof, in which the email will link to the website.

Cybercriminals use spoofed websites to capture your username and password (aka login spoofing) or drop malware onto your computer (a drive-by download): unintended download of one or more files, malicious or not, onto the user’s system without their consent or knowledge. Malware like a Remote Access Trojan (RAT), which gives them remote access to the victim’s computer.

Protect from spoofed websites:

Make sure that the Web site uses Secure Sockets Layer/Transport Layer Security (SSL/TLS) and check the name of the server before you type any sensitive information. (By checking the name on the digital certificate user for SSL/TLS)

**What Can You Do to Prevent Such Attacks? <** Countermeasures **>**

Watering hole attacks may be discovered by web gateways that detect known attack signatures.

* <https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-secure-web-gateway.html>
* <https://cybersecurity.att.com/solutions/secure-web-gateway/what-is-a-secure-web-gateway>

**Secure web gateway: -** A network security device (a checkpoint) that keeps unauthorized traffic from entering an organization's network. Can prevent sensitive information (like intellectual property, data, and confidential documents) from leaving an organization's site (also known as exfiltration).

Best practices will help organizations prevent their networks and users from falling prey to watering hole attacks:

1. **Regular security testing:** Organizations need to regularly test security solutions to verify that they provide the necessary defence level. This ensures that users always browse the internet securely, prevents intentional and unintentional downloads of malware or malicious websites.
2. **Advanced threat protection:** Security solutions that protect organizations against advanced attack vectors are crucial to preventing watering hole attacks. Advanced threat protection tools include behavioural analysis solutions, which give organizations a better chance of detecting zero-day exploits before attackers can target users.
3. **System and software updates:** An essential best practice for avoiding watering hole attacks is to update systems and software and install operating system patches as soon as they are made available by vendors. Attackers infect websites by discovering vulnerabilities in their code, making it imperative to spot flaws or gaps in software before cyber criminals find them.
4. **Treat all traffic as untrusted:** Organizations need to consider all traffic to be untrusted until verified as legitimate. This is especially important with third-party traffic and should be a standard approach to internet traffic, regardless of whether it has come from partner websites or popular internet properties like Google domains.
5. **Test and secure against exposure:** Secure web gateways (SWGs) help organizations enforce their internet access policies and filter unwanted or malicious software from reaching user-initiated internet connections. This is crucial with the rise in the Internet-of-Things (IoT) and cloud applications, which increase organizations’ attack surfaces. SWGs protect organizations from external and internal threats with application control, Uniform Resource Locator (URL) filtering, data loss prevention (DLP), remote browser isolation, and deep Hypertext Transfer Protocol Secure (HTTPS) inspection. These solutions are crucial to protecting businesses from the risk of advanced cybersecurity threats like watering hole attacks.

<https://www.techopedia.com/definition/31858/watering-hole-attack>

<https://www.youtube.com/watch?v=cqvaD2Do7UI>

**OFFICE MACRO ATTACKS**

* **What are Office Macros?**
* **Why It’s a Problem**
* **User Execution**
* **Demonstration**
* **Detection & Mitigation**
* **Reducing Attack Surface**
* **Detection**

**What are Office Macros?**

**Macros** are special-purpose programs used to automate procedures within a bigger application or software. These programs will be executed automatically by the application when a certain trigger takes place.

Within *Office Suites* Macros are implemented extensively for automation of common tasks and procedures.  For example, MS Office macros (written in VBA) can run executables and use networking capabilities.

**Why It’s a Problem**

Allowing the execution of customizable scripts in the background; attackers can exploit Office suites to run malicious code and compromise victims. Macro-malware acts as a leader in the infection chain, and will download and execute another payload before terminating.

The malware will be embedded in – you guessed it – an Office file, and implanted somewhere for the victim to access it, say a common file share or by e-mail. Once the file is opened, the malware will be executed (Spear *phishing Macro Attack*). Example of a macro-malware is the Melissa virus, which first appeared in 1999.

Macro threats can be designed to live “off the land”, meaning they don’t write anything to the disk and only use common tools to run code directly in memory.

**User Execution**

Spear phishing attacks rely on a vulnerability that is very hard to mitigate completely – human error. Moreover, relying on user execution also allows adversaries to target and lure non-technical users.

MS Office macro-execution is enabled by default or is allowed by a single mouse click upon opening the malicious file.

Once the malware is executed, it can embed itself in other Office files on the victim’s machine, rendering every document created on the machine compromised.

Macro-malwares are relatively easy to obfuscate. Obfuscation tools are readily available e.g. macro\_pack( <https://pentesttools.net/macro_pack-automatize-obfuscation-and-generation-of-ms-office-documents/> ) and VBA Purging( <https://www.mandiant.com/resources/purgalicious-vba-macro-obfuscation-with-vba-purging> ), furthermore, malicious code snippets can be even taken out of the macro source code and hidden in other file components like text labels.

**Demonstration**

* Step 1 – Generating VBA Payload
* Step 2 – Setting-Up a Connection Handler
* Step 3 – Embedding VBA Payload

**Detection & Mitigation**

One of the most efficient strategies to mitigate risk is limiting the use of macros across an organization due to Spear phishing. When macro use is essential, **policy** should be set to minimize exposure to attacks.

* **App Policy** – macros should only be enabled in apps where they are actually being used – be it Excel, Word, PowerPoint.
* **User Policy** – in an enterprise environment, macros should only be enabled for users that actually make use of that feature.

**Reducing Attack Surface**

An attack surface is the total number of ways or places in which an adversary may compromise a device or network.  Reducing endpoints’ attack surface by restricting access to resources that are essential for malware to operate.

* Block Office applications from creating executable code
* Block Office applications from creating child processes
* Block Office applications from injecting code to other processes

**Detection**

A macro may be deemed malicious if it:

* Executes scripts in PowerShell, VBA etc.
* Embeds itself in other Office files or Office template files
* Uses networking capabilities to download files from remote servers
* Creates processes

As threats are growing ever more obfuscated and complex, a need for more sophisticated detection techniques has risen. Starting from Windows 10, Microsoft added a new component called Anti-Malware Scan Interface (AMSI) to address this concern; which is an interface between script interpreters and anti-virus engines, allowing them more control over macro execution.

**\*In the process of completion\***

**Outlook Attack Using Macros:**

* Outlook Attack Method:- <https://office-watch.com/2017/a-new-outlook-attack-method-microsoft-in-denial/>
* Tutorial on Microsoft Outlook Macros: -

https://www.vogella.com/tutorials/MicrosoftOutlookMacros/article.html

* Writing useful Macros: <https://www.easytweaks.com/add-macros-outlook-2016/>
* Using Macros in Outlook <https://www.youtube.com/watch?v=8RnOrEbOyR4>
* Macro Instructions | Outlook Reply with Email Template: - <https://www.youtube.com/watch?v=rlNhCUKiGY0>