**Watering hole attack**

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Watering_hole_attack#mw-head) [Jump to search](https://en.wikipedia.org/wiki/Watering_hole_attack#searchInput)

This article is about the computer hacking technique. For the place to obtain alcoholic drinks, see [pub](https://en.wikipedia.org/wiki/Pub). For other uses, see [Watering hole (disambiguation)](https://en.wikipedia.org/wiki/Watering_hole_(disambiguation)).

**Watering hole** is a [computer attack](https://en.wikipedia.org/wiki/Attack_(computing)) strategy, in which the victim is of a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with [malware](https://en.wikipedia.org/wiki/Malware). Eventually, some member of the targeted group becomes infected.[[1]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-Gradigo2012-1)[[2]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-HaasterGeversSprengers2016-2)[[3]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-Miller2014-3) Hacks looking for specific information may only attack users coming from a specific [IP address](https://en.wikipedia.org/wiki/IP_address). This also makes the hacks harder to detect and research.[[4]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-:1-4) The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.[[5]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-5)



**Contents**

* [1 Defense techniques](https://en.wikipedia.org/wiki/Watering_hole_attack#Defense_techniques)
* [2 Examples](https://en.wikipedia.org/wiki/Watering_hole_attack#Examples)
  + [2.1 2018 Chinese country-level attack](https://en.wikipedia.org/wiki/Watering_hole_attack#2018_Chinese_country-level_attack)
  + [2.2 2017 Montreal based International Civil Aviation Organization attack](https://en.wikipedia.org/wiki/Watering_hole_attack#2017_Montreal_based_International_Civil_Aviation_Organization_attack)
  + [2.3 2017 CCleaner attack](https://en.wikipedia.org/wiki/Watering_hole_attack#2017_CCleaner_attack)
  + [2.4 2017 NotPetya attack](https://en.wikipedia.org/wiki/Watering_hole_attack#2017_NotPetya_attack)
  + [2.5 2016 Polish banks](https://en.wikipedia.org/wiki/Watering_hole_attack#2016_Polish_banks)
  + [2.6 2013 US Department of Labor](https://en.wikipedia.org/wiki/Watering_hole_attack#2013_US_Department_of_Labor)
  + [2.7 2012 US Council on Foreign Relations](https://en.wikipedia.org/wiki/Watering_hole_attack#2012_US_Council_on_Foreign_Relations)
* [3 References](https://en.wikipedia.org/wiki/Watering_hole_attack#References)

**Defense techniques**

Websites are often infected through [zero-day](https://en.wikipedia.org/wiki/Zero-day_(computing)) vulnerabilities on browsers or other software.[[4]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-:1-4) A defense against known vulnerabilities is to apply the latest software patches to remove the vulnerability that allowed the site to be infected. This is assisted by users to ensure that all of their software is running the latest version. An additional defense is for companies to monitor their websites and networks and then block traffic if malicious content is detected.[[6]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-Grimes2017-6)

**Examples**

**2018 Chinese country-level attack**

There was a country-level watering-hole attack in China from late 2017 into March 2018, by the group "LuckyMouse" also known as "Iron Tiger", "EmissaryPanda", "[APT](https://en.wikipedia.org/wiki/Advanced_persistent_threat) 27" and "Threat Group-3390."[[7]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-7)

**2017 Montreal based International Civil Aviation Organization attack**

There was an organization-level watering-hole attack in Montreal from 2016-2017 by an unknown entity causing a data breach. [[8]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-8)

**2017 CCleaner attack**

From August to September 2017, the installation binary of [CCleaner](https://en.wikipedia.org/wiki/CCleaner) distributed by the vendor's download servers included malware. CCleaner is a popular tool used to clean potentially unwanted files from Windows computers, widely used by security-minded users. The distributed installer binaries were signed with the developer's certificate making it likely that an attacker compromised the development or build environment and used this to insert malware.[[9]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-CiscoCcleaner2017-9)[[10]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-Piriform2017-10)

**2017 NotPetya attack**

In June 2017, the [NotPetya](https://en.wikipedia.org/wiki/Petya_(malware)) (also known as ExPetr) malware, believed to have originated in Ukraine, compromised a Ukrainian government website. The [attack vector](https://en.wikipedia.org/wiki/Attack_vector) was from users of the site downloading it. The malware erases the contents of victims' hard drives.[[11]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-11)

**2016 Polish banks**

In late 2016, a Polish bank discovered malware on computers belonging to the institution. It is believed that the source of this malware was the [web server](https://en.wikipedia.org/wiki/Web_server) of the [Polish Financial Supervision Authority](https://en.wikipedia.org/wiki/Financial_Supervision_Authority_(Poland)).[[12]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-:0-12) There have been no reports on any financial losses as a result of this hack.[[12]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-:0-12)

**2013 US Department of Labor**

In early 2013, attackers used the [United States Department of Labor](https://en.wikipedia.org/wiki/United_States_Department_of_Labor) website to gather information on users' information. This attack specifically targeted users visiting pages with nuclear-related content.[[13]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-Cisco2017-13)

**2012 US Council on Foreign Relations**

In December 2012, the [Council on Foreign Relations](https://en.wikipedia.org/wiki/Council_on_Foreign_Relations) website was found to be infected with malware through a zero-day vulnerability in Microsoft's [Internet Explorer](https://en.wikipedia.org/wiki/Internet_Explorer). In this attack, the malware was only deployed to users using Internet Explorer set to English, Chinese, Japanese, Korean and Russian.[[14]](https://en.wikipedia.org/wiki/Watering_hole_attack#cite_note-Mimoso2012-14)