Cybersecurity

2.2.5 - Watering Hole Attacks and Typosquatting

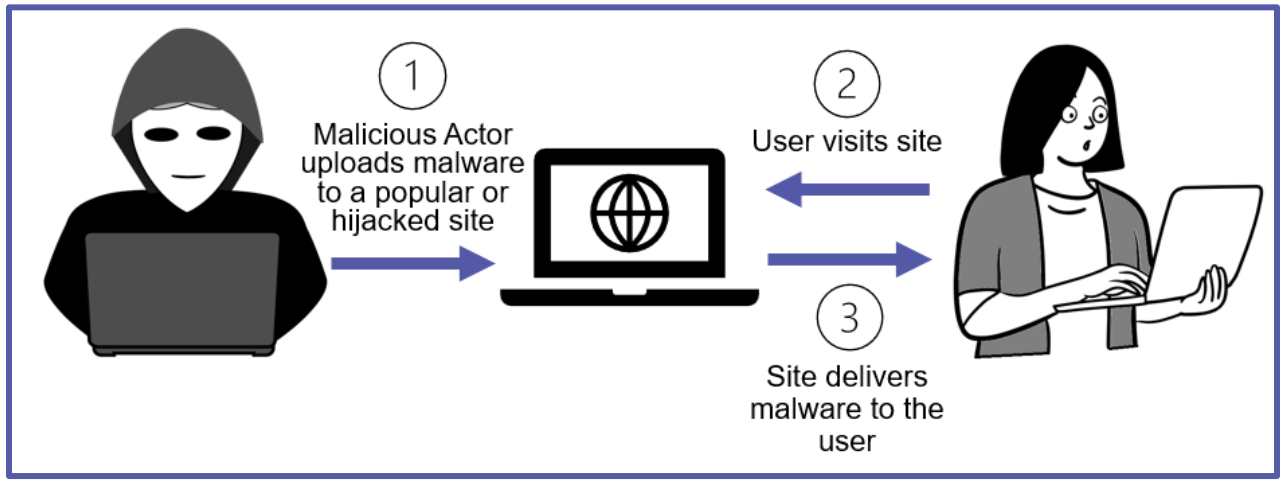
CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Watering Hole Attacks

- Taken from the same behavior observed from animals in the wild do when they return to the same areas for water and nutrition every time
- A watering hole is a metaphor for a place that users go to seeking information or resources online.

Watering Hole Attacks cont'd

- This is typically paired with a popular site that has been compromised or a fake site setup to mimic a legit site.
  - In either case the site serving as the watering hole usually contains malware and is activated from a user visiting the page.
  - The frequency of visits to the page allows little effort on the part of the malicious user but has potential for a high reward

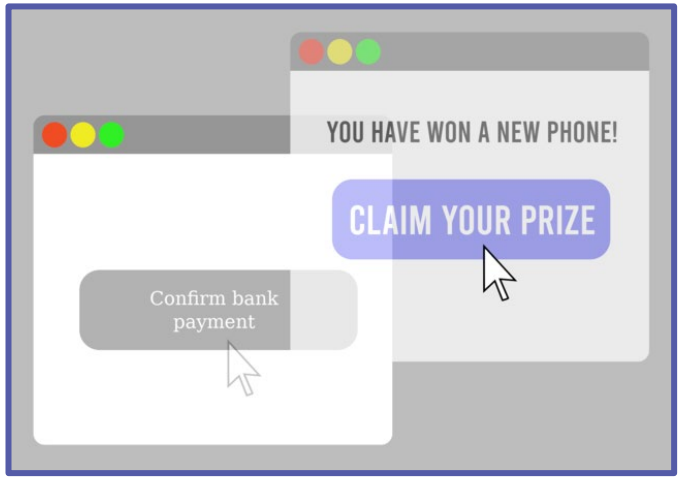


Defending Against Watering Hole Attacks

- Many times, little to nothing can be done about the watering hold itself; however, being proactive in your defenses is key to protecting yourself.
  - Keeping anti-malware/ anti-virus software updated
  - Being attentive to what is downloaded, noticing things like downloads occurring without any input from the end-user
  - Take note of changes in your devices and how well it functions as less optimal performance might be a sign of something malicious

Hijacking Hijinks

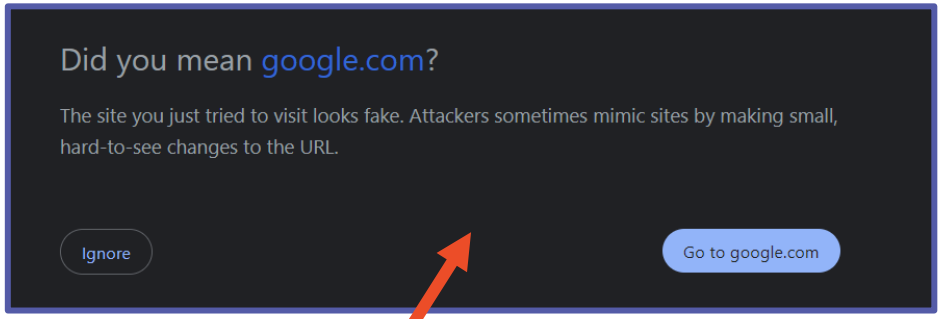
- Client hijacking involves concealing malicious links to malware and sites, so they appear to be legitimate to the casual user.
  - Clickjacking involves hiding a link or object containing a link above the object the user would normally click on, such as an image.
  - URL hijacking involves slight changes to URLs to mimic the original, such as typos, which is where the term typosquatting comes from.



Typosquatting

- Involves slightly changing the URL, such as seen in day-to-day typos, to resemble a well-known website.
- There are signs to look for such as:
  - Spelling
  - Domain listed such as .com vs .net
  - Security checks such as http vs. https
- Google owns a few domains that are commons typos for Google as shown in the table to prevent things such as typosquatting

Google owned domains with common typos
Gooogle.com
Gogle.com
Gogole.com
Googl.com



Appears when attempting to go to a page where there is a typo in Google

Session Hijacking

- Cookies are small bits of information that save authentication data and other website preferences.
- Session hijacking occurs when an attacker steals the cookie used to authenticate a user on a website.
- Once stolen, the unauthorized user can login to sites with the victim's cookie