Cybersecurity

Watering Hole Attacks

Watering Hole Attack

- Instead of laboring over ways to attack a target network, what if they come to you?
- Go where they go
  - Organizations usually visit certain websites routinely
    - Either vendors, reference information, or Software as a Service (SaaS) sites
- Ever a URL incorrectly?
  - What you meant: `google.com`
  - What you typed: `gogle.com` or `gooogle.com` or `ggle.com`
  - Google knows people will make mistakes and have registered the first two.
    That third one is <u>not</u> owned by Google!

Watering Hole Attack

- Setup official-looking website but loaded with malicious code -or- infect actual site the targets frequent
- Wait for *them* to come to *you*!

Executing the Watering Hole Attack

- Determine sites the target frequents
  - Educated guess
  - Industry-related sites
- Infect a third-party site
  - Exploit vulnerability on web server
  - Send malicious email attachments
- All visitors to the site get hit
  - Filter for specific victims

Defending from a Watering Hole

- Defense-in-depth
  - Layered defense
  - Never just one thing
- Firewalls and IPS
  - Stop bad network traffic
- Keep Anti-virus & Anti-malware updated
  - Always update