PHISHING MADE EASY WITH EVILGINX2

YOUR MFA ISN'T THAT SAFE METHOD

AGENDA

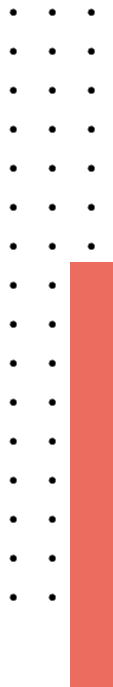
- Quick words on phishing
- Evilginx: what – why – how
- Demo
- Lessons

PHISHING

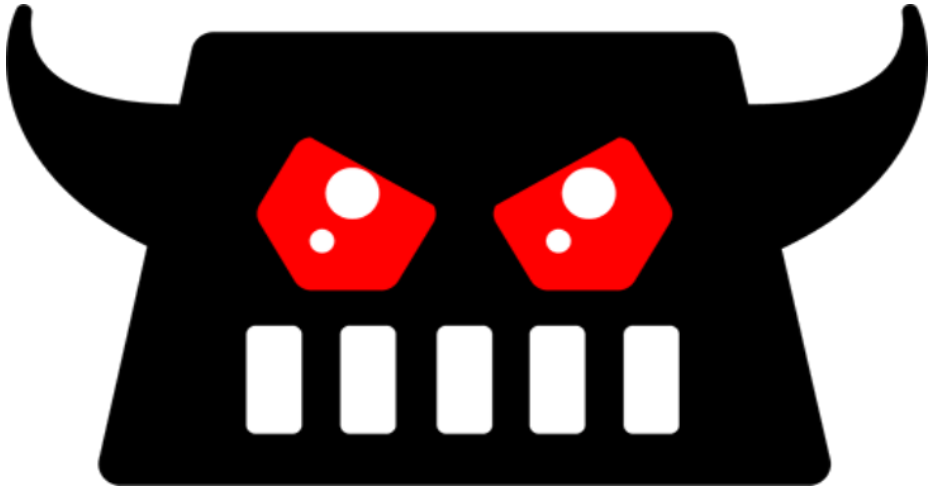
- To trick people to enter sensitive data to a fake website
- Popular red team technique to get into a target's network

POPULAR PROTECTION METHODS

- Encryption (HTTPS)
- Entity Validation (Certificate Authority)
- Multi Factor Authentication (MFA)



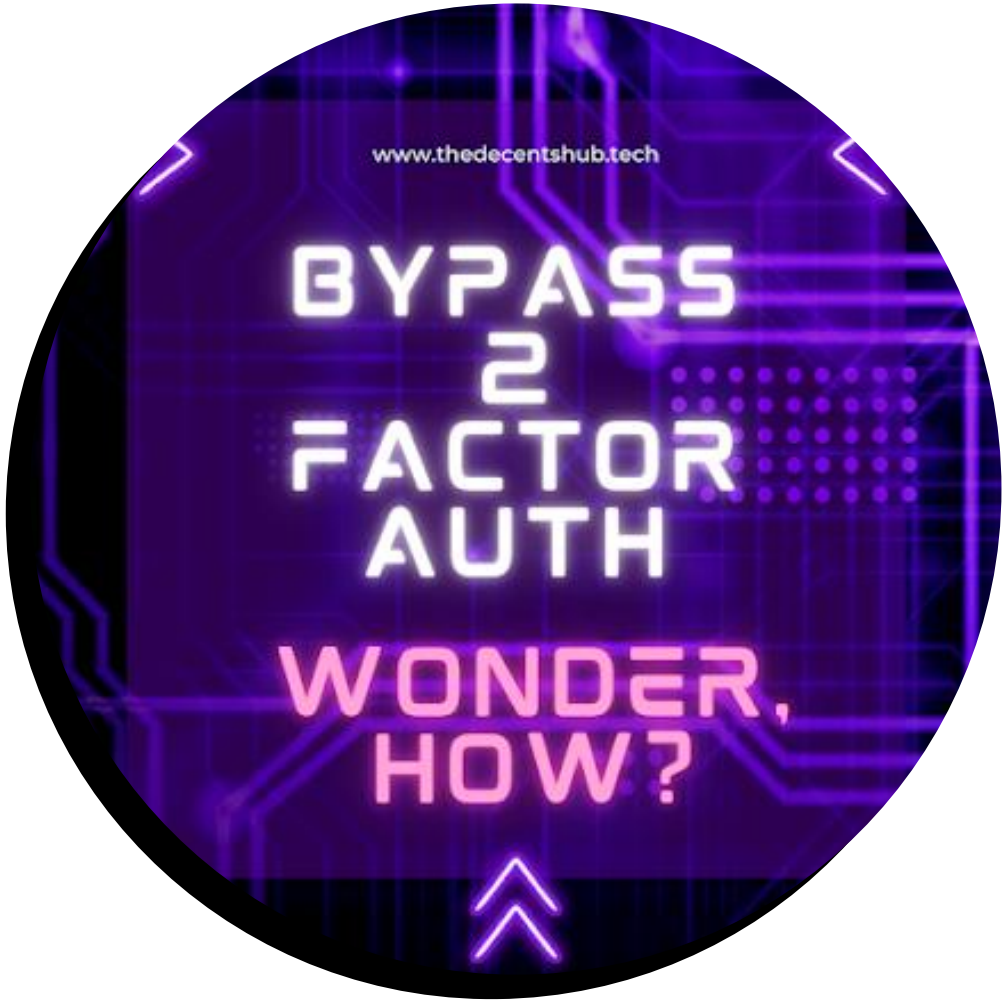
EVILGINX2



- Opensource phishing tool
- Was inspired by nginx proxy_pass feature (but now only EVIL , no nginx)
- Easy to use
- Leverage web cookies to bypass everything

EVILGINX

- Classic man-in-the-middle (MITM) attack
- Intercept traffic from client
- Replay it to real website
- Pass back answer to the victim
- Capture cookies in the final step
- Redirect victim to real website once again
- Get out of the flow



DEMO

- Simple QC phish
- Bypass outlook MFA

HOW EASY IT IS ?

- Prerequisite:
  - A domain
  - A host with public IP
  - An evil mind
- Use existing phishlet template
- Edit my cookies extension

HOW TO WRITE A CUSTOM PHISHLET

- Burp proxy to capture traffic
- Identify the requires cookies
- Understand phishlet format

LESSONS

- MFA is not a perfect guarantee(*)
- Human is still the weakest link
- Be careful , I'm sending phishing email soon

Shane Huntley
@ShaneHuntley

2FA is super important but please, please stop telling people that by itself it will protect people from being phished by the Russians or governments. If attacker can trick users for a password, they can trick them for a 6 digit code.

11:29 AM · Jul 22, 2018

REFERENCES

- https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/
- https://github.com/kgretzky/evilginx2/wiki/Phishlet-File-Format-(2.3.0)
- https://github.com/An0nUD4Y/Evilginx2-Phishlets
- https://www.vice.com/en/article/5d35yd/the-uber-hack-shows-push-notification-2fa-has-a-downside-its-too-annoying