CWL
CyberWarFare Labs

SIMULATING SERVERLESS AITM ATTACK

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has two primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform

About Speakers :

Yash Bharadwaj

Co-Founder & Technical Director at CW Labs UK Pvt. Ltd.

With over **6.5 Years** of Experience as Technologist. Highly attentive towards finding, learning and discovering new TTP's used during offensive engagements.

His area of interest includes **designing, building & teaching** Red / Blue Team Lab Simulation.

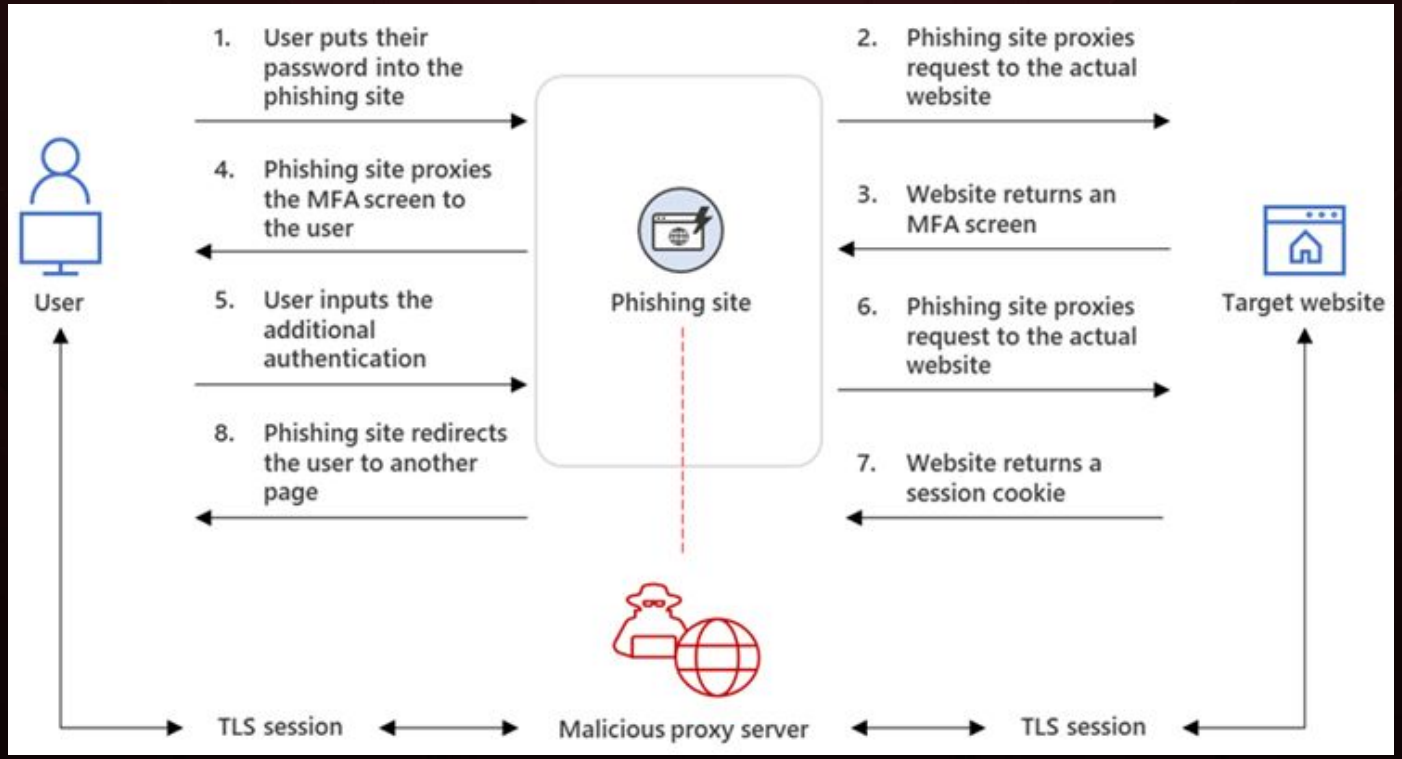
Previously he has delivered hands-on red / blue / purple team trainings / talks / workshops at Nullcon, X33fCon, NorthSec, BSIDES Chapters, OWASP, CISO Platform, YASCON etc

You can reach out to him on Twitter **@flopyash**.

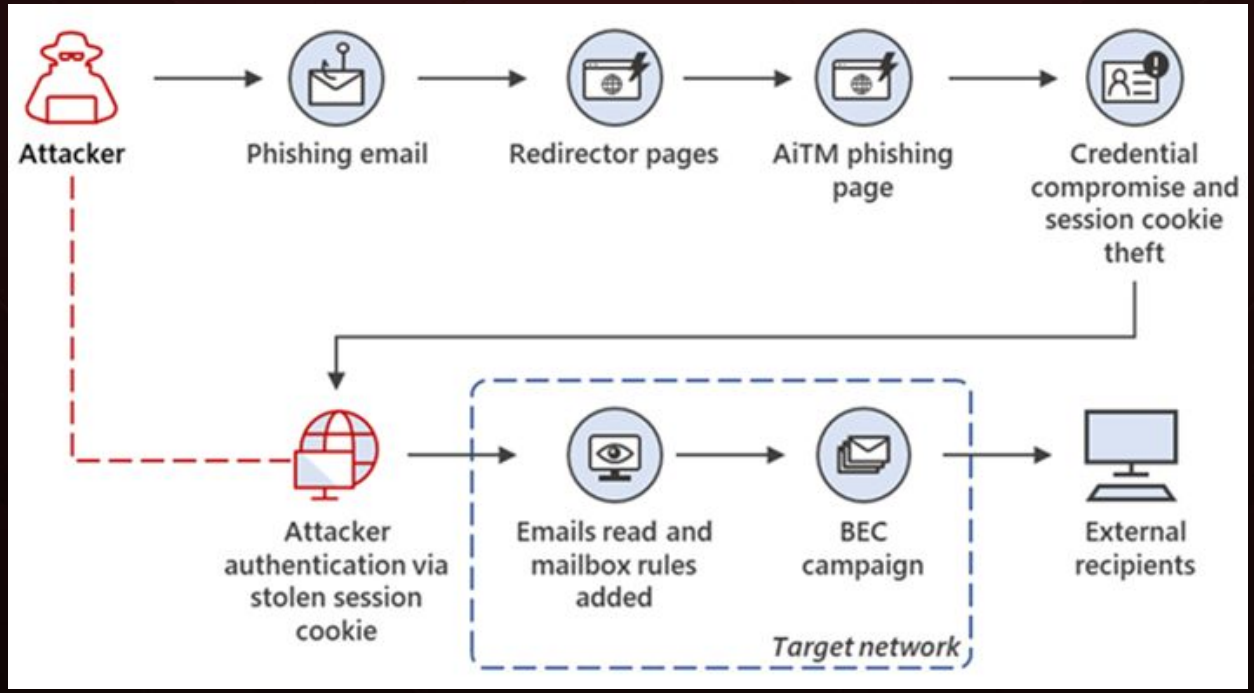
Agenda

- AiTM Working
- Case Study
- Server vs Serverless
- Demonstration
- Defenses
- Giveaway & Details

AiTM Working



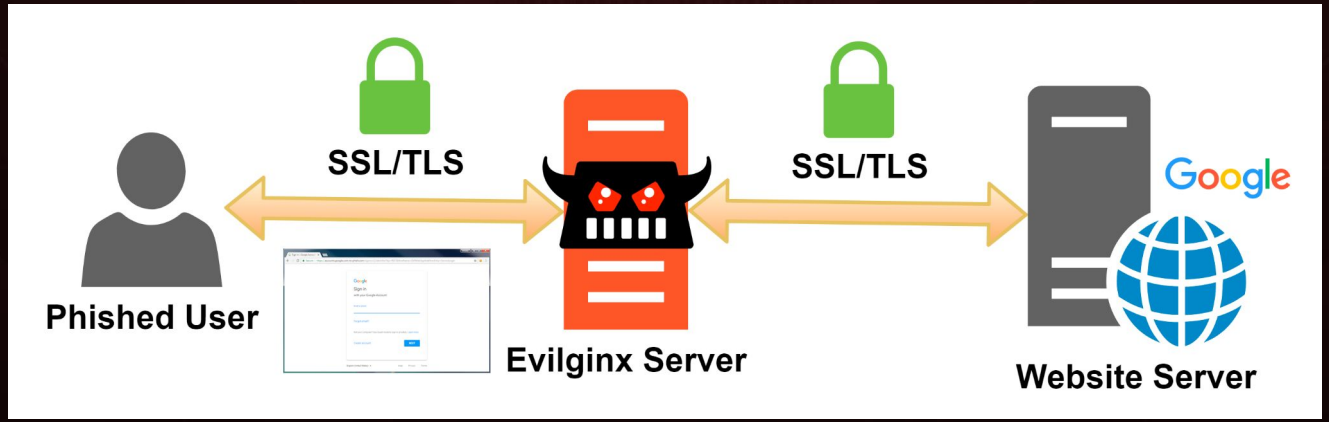
Case Study : Cookie theft to BEC



Reference :
https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

Server based AiTM

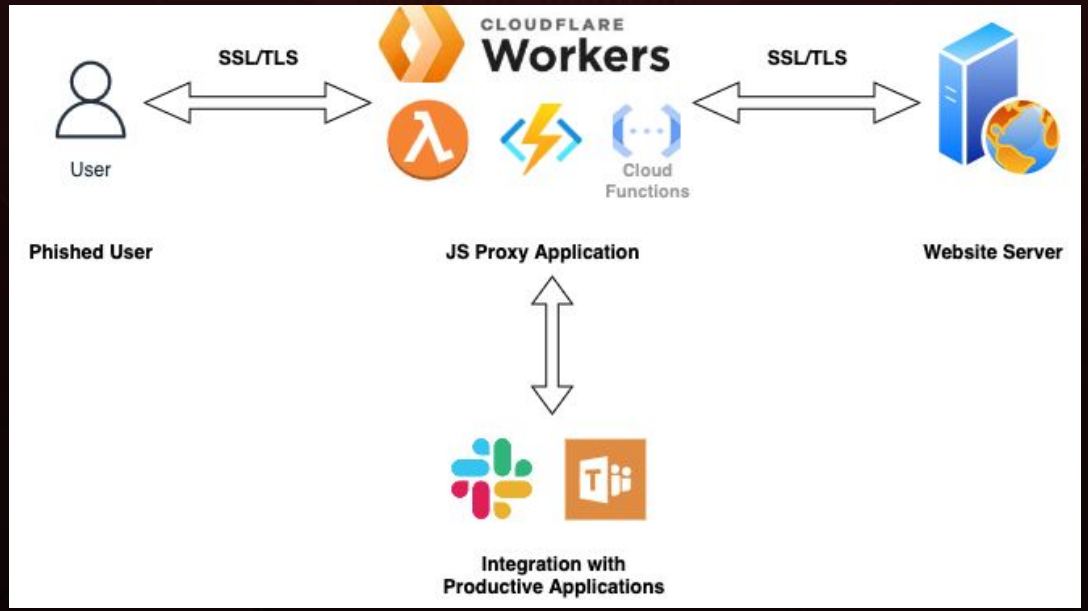
- Well known tools like **Evilginx, modlishka** etc operates in server based models



Reference : https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

Server-less AiTM

- **Serverless computing solutions** can run single file applications (JS, TS code etc), which proxies the connection to the original website



Comparison

Server-less Model	Server based Model
Costing : as per request received	Costing : Till the time server is UP
Cloud services provides certificate support	Mostly manual certificate setup
Wealth of available cloud domains	Depends on owned domains
Custom integration support with productive apps like Slack, Teams	Custom integration support with productive apps
Easy customized setup to proxy with legitimate website (More on this later)	Depends :(

[Demo] Simulating Serverless Phishing

- **Cloudflare workers**
  - Provides **serverless execution platform**, which allows to run applications without any infra headache.
  - Provides a custom "**workers.dev**" domain
  - Resolve 3rd party library dependency
  - Custom JS code which single-handedly manages the phishing operation

Demo JS Code : https://gist.github.com/RedTeamOperations/33f245a777c9b322b0466b59d6687f15

[Demo] Simulating Serverless Phishing

- **Integration with Slack Workspace for updates**
  - Create a slack **workspace** & organize a group ex. "**give-me-cookies**"
  - Create a **slack application "Cookie Updates"** from scratch
  - Enable incoming **webhook**
  - Allow app to post updates to posts messages from external sources to slack

Demo JS Code : https://gist.github.com/RedTeamOperations/33f245a777c9b322b0466b59d6687f15

Defenses

- Implement AiTM resistant solutions like **Smart Cards, WHfB or FIDO2 keys. However,** there are still various ways to downgrade the above authentication mechanism to legacy methods.
- Implementing **Conditional Access Policies** blocks most of the complex phishing attacks.
- Continuous phishing assessments & employee training can be followed as per organization policies.

Special thanks to Mr Wesley @wesleyneelen from Zolder.io

CWL Giveaway:

- Giveaway of any **interested CWL Red Team Course** to lucky candidate whose comment got **0 Like**, To participate visit: LinkedIn Event
- Webinar Attendance Certificate to all attendees
- Access of this webinar recording & PPT Material [PDF File]

CWL
CyberWarFare Labs

Thank You!

If you like the webinar, please feel free to shout out & tag us at social media platforms.

For any technical questions / doubts related to the content please email us at ***support@cyberwarfare.live***

For Professional Red / Purple Team Labs & Technical Training Services kindly email at ***info@cyberwarfare.live***