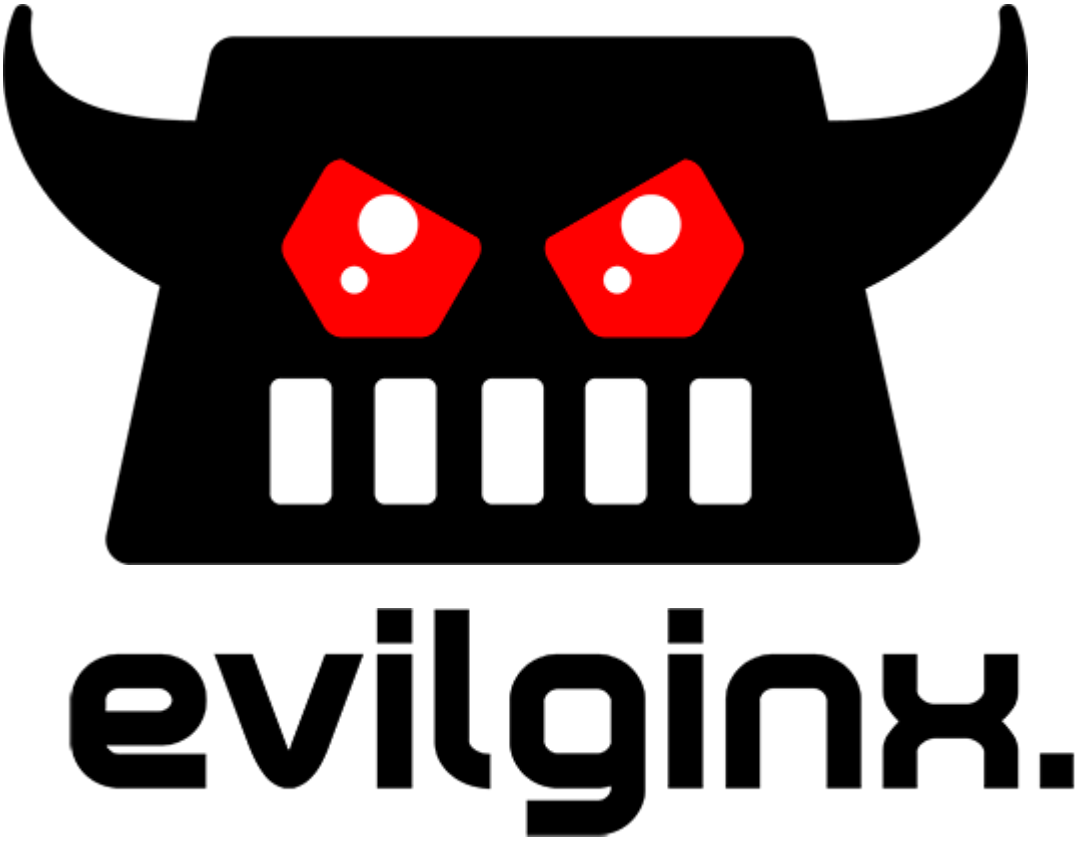
GitHub - kgretzky/evilginx2: Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication

By kgretzky

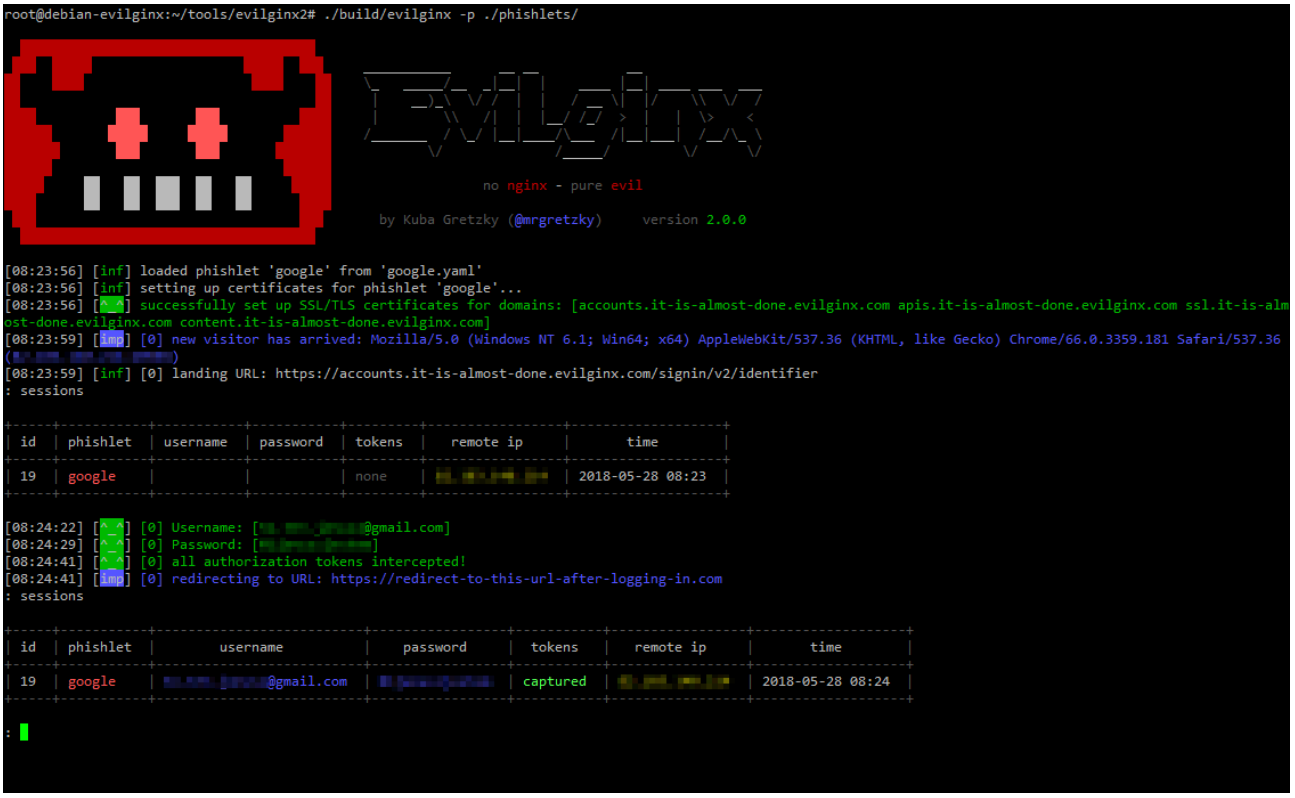
Archived: 2026-04-02 11:16:44 UTC



Evilginx 3.0

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to Evilginx, released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.



Disclaimer

I am very much aware that Evilginx can be used for nefarious purposes. This work is merely a demonstration of what adept attackers can do. It is the defender's responsibility to take such attacks into consideration and find ways to protect their users against this type of phishing attacks. Evilginx should be used only in legitimate penetration testing assignments with written permission from to-be-phished parties.

Evilginx Pro is now available!

This is it! After over two years of development, countless delays, and hundreds of manual company verifications, concluded with multiple hurdles related to export regulations, Evilginx Pro is finally live!

Evilginx Pro is the fruit of a passion I've had for a long time in developing offensive security tools for cybersecurity enthusiasts. The journey has just begun, and now that the product is officially released, I can focus on making it even better by implementing all the ideas I've planned for it.

Key features:

- Out-of-the-box **phishing detection evasion** (including Chrome's Enchanced Browser Protection)
- Tested and maintained **official phishlets database**
- **Botguard** to **prevent bot traffic** by default (same concept as Cloudflare Turnstile)
- **Evilpuppet** for advanced phishing capability (Google)
- External **DNS providers** with multi-domain support
- **Website spoofing** for unauthorized requests
- **JavaScript** & **HTML obfuscation**
- **Wildcard TLS certificates**
- **Automated** server deployment
- **SQLite** database support

Find out more on the official release blog post.

Evilginx Mastery Training Course

If you want everything about reverse proxy phishing with **Evilginx** - check out my Evilginx Mastery course!

Learn everything about the latest methods of phishing, using reverse proxying to bypass Multi-Factor Authentication. Learn to think like an attacker, during your red team engagements, and become the master of phishing with Evilginx.

Grab it here: https://academy.breakdev.org/evilginx-mastery

Official Gophish integration

If you'd like to use Gophish to send out phishing links compatible with Evilginx, please use the official Gophish integration with Evilginx 3.3. You can find the custom version here in the forked repository: Gophish with Evilginx integration

If you want to learn more about how to set it up, please follow the instructions in this blog post

Write-ups

If you want to learn more about reverse proxy phishing, I've published extensive blog posts about **Evilginx** here:

Evilginx 2.0 - Release

Evilginx 2.1 - First Update

Evilginx 2.2 - Jolly Winter Update

Evilginx 2.3 - Phisherman's Dream

Evilginx 2.4 - Gone Phishing

Evilginx 3.0

Evilginx 3.2

Evilginx 3.3

Help

In case you want to learn how to install and use **Evilginx**, please refer to online documentation available at:

https://help.evilginx.com

Support

I DO NOT offer support for providing or creating phishlets. I will also NOT help you with creation of your own phishlets. Please look for ready-to-use phishlets, provided by other people.

License

evilginx2 is made by Kuba Gretzky (@mrgretzky) and it's released under BSD-3 license.
