Evilginx 3.0 + Evilginx Mastery

By Kuba Gretzky

Published: 2023-05-10 · Archived: 2026-04-29 02:05:36 UTC

This post has been long coming and I'm glad to finally be able to make it happen!

Today I'm finally releasing Evilginx 3.0, together with **Evilginx Mastery** online course, into which I've poured everything I know about Evilginx and how to use it in the most effective manner.

Evilginx hasn't seen any updates for nearly two and a half years. That's why it was a great surprise to me to hear, that even though I haven't released any updates, a lot of red teamers still use this tool for phishing simulations with many successes. I've been amazed to come across some great posts about Evilginx, like the ones by Jan Bakker, Jeffrey Appel or Pepe Berba.

Talking to people in the industry motivated me to give Evilginx a quality of life refresher, in order to build stronger foundations for future updates. It's been nearly 6 years, since I've released the first version of Evilginx, which was nothing more than a LUA script for custom version of *nginx.* Back then I couldn't have foreseen such great reception, the tool would receive, over the years.

It's a fact, that a lot of people have been struggling to figure out how to properly use Evilginx or create their own phishlets. Lack of official documentation to guides didn't help and you could only get so far, analyzing public phishlets and trying to figure out how they work through trial & error.

Additionally, to my surprise, during recent years, not many websites have attempted to develop their own detections for reverse proxy phishing. I need to actually hand it to Google and Microsoft as they seem to have been one of the few companies doing anything to protect their users against reverse proxy phishing.

All this will hopefully change today. Here is, in detail, what I've been working on, for the past year, and what I'm today releasing to the public:

Evilginx Mastery Course

Public version of Evilginx will always remain open-source and free to use. You can use the tool as you see fit. To fund further development, I decided to publish a paid online course, with which I could demonstrate my whole knowledge about Evilginx and share hands-on step by step video footage showing how I personally use Evilginx, myself.

Big thanks to SEKTOR7 and Rasta Mouse for encouragement to make an attempt in creating an Evilginx course.

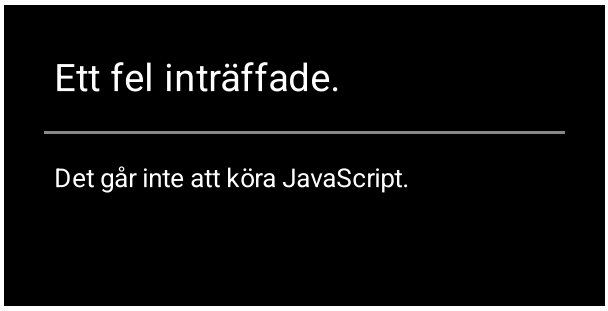
The course is also prepared with defenders in mind. Seeing how little websites do to protect from reverse proxy phishing, nowadays, I've included tips on what defenders can do to make reverse proxy phishing attacks extremely hard or nearly impossible to pull off.

If you decide to purchase the course, thank you in advance and keep in mind that it helps me greatly to continue working on Evilginx and will definitely be a great contribution to my levels of motivation.

If you plan to purchase access to the course for multiple employees in your company, please contact me directly at kuba@breakdev.org and we can work out a discount.

You can buy the course online and watch the lessons, at your own pace, whenever you want: Evilginx Mastery - Reverse Proxy MFA Phishing Guide For Red Teams

To know more about the course, take a look at my attempt to make a promotional video for the course. And yes I know how to blink :D



Evilginx 3.0

This version is not delivering flashy big features, but rather it serves as a quality-of-life update. I've fixed numerous issues, which have been lingering in Evilginx for a long time and updated some mechanics to make the tool work better than before.

GitHub: https://github.com/kgretzky/evilginx2

Here are some highlights of what has changed:

Improved TLS certificate management

I've ditched the old GO library for managing LetsEncrypt certificates and switched to well-maintained certmagic library. This change now allows to perform automated retrieval of TLS certificates, from LetsEncrypt, more efficiently and most importantly, Evilginx will now automatically renew expiring certificates, so you won't have to ever worry about your phishing campaigns expiring without warning.

Session tokens can now be extracted from response body or HTTP Headers

Ever since Evilginx was released, I've only considered a single scenario where session tokens are to be transmitted as HTTP cookies. Over the years, I've learned this approach was wrong, as now it is becoming more and more common for session tokens to be retrieved in JSON packets and later stored as LocalStorage values. This is now especially common practice with web applications relying heavily on JavaScript functionality like messenger applications.

It is now possible to look for session tokens in HTTP response packets body or in contents of HTTP headers like the `Authorization` header.

I've covered how to handle such scenario in one of the training labs from Evilginx Mastery course.

Example phishlets no longer available in main repository

My main goal has always been to deliver a reverse proxy phishing framework for red teamers. The provided example phishlets were always meant to serve as a learning material to learn how to make your own phishlets. Keeping them updated, was honestly an impossible feat. This is why I've made a decision to cease support for example phishlets in the main Evilginx repository.

Phishlets get outdated and stop working relatively fast and I always wanted to focus on developing the framework, rather then keeping the example phishlets constantly up-to-date. I encourage everyone to set up their own repositories with phishlets they want to share with the community. My priority now is to put effort into teaching people how to create their own phishlets.

Once I find several contributors, who may want to work on several phishlets for fun, I may set up a new repository just for aggregating several working and tested phishlets, made by others, and later have it integrated somehow with Evilginx installations.

Phishing pages can now be embedded within iframes

Few months ago, the legendary mr.d0x, released amazing research on BITB (browser-in-the-browser) phishing, where you could create a fake popup window, with JavaScript, showing a spoofed URL in fake address bar. I liked the idea so much that I really wanted to see it working with Evilginx.

Displaying phishing pages in iframes turned out to not be supported, by default. Now you can fully enjoy displaying your phishing page within iframes. Just make sure to fully rewrite the default BITB templates as they have been heavily flagged by Google as malicious content.

Also make sure to check out mr.d0x courses on Malware Development!

Configuration format changed to JSON

Evilginx configuration file was stored originally in YAML format. JSON, overall, is a much better option, with its syntax being easier to use than YAML, but maybe a bit harder to read. Nevertheless, with config file in JSON format, it will be easier to write custom deployment scripts, handling dynamic generation of configuration files.

Phishlets will remain in YAML format.

Phishing sessions are now created always when valid lure URL is opened

Evilginx would whitelist IP addresses of every target, making requests to valid lure URLs. This is required to later allow the proxying of requests, which cannot contain Evilginx session cookies, due to web browsers not allowing some requests to transmit cookies.

The bug in Evilginx would prevent creation of new reverse proxy sessions for valid lure URLs coming from IP addresses, which have already been whitelisted.

In 3.0 update, every time a target opens a valid lure URL, they will be assigned a new reverse proxy session. This fix will also make it possible to properly track the clicks to your lure URLs.

Child phishlets derived from phishlet templates

One of the problematic issues Evilginx users have encountered was targeting websites, which were hosted under customized hostnames.

Say you wanted to target a specific company's Okta portal, hosted on `evilcorp.okta.com` domain. To target custom domains, you'd have to manually edit the phishlet file and put the hardcoded `evilcorp.okta.com` into it.

With the phishlet templates feature, instead of having to modify a phishlet file manually, every time you'd need to target a different hostname, now you can create a phishlet template for Okta, setting up a placeholder for custom variables in your phishlet file e.g. `{subdomain}.okta.com`.

Having such template, whenever you'd need to target a specific hostname, you could just create a child phishlet as a derivative from your phishlet template and specify `subdomain=evilcorp`, as an example. Such created child phishlet can be then used as a normal phishlet with its own personalized setup.

You can learn how to create and use phishlet templates in my Evilginx Mastery course, as well.

URL redirection with JavaScript

Originally when all session tokens have been successfully captured, Evilginx would redirect the user to preconfigured `redirect_url` URL through HTTP `Location` header. I found this solution to not be ideal, since this approach exposed the phishing URL to destination website, through `Referer` header, when redirection took place.

Since 3.0, the redirection will happen via JavaScript injected into `text/html` content of the next web page, loaded after all session tokens have been captured. This approach will avoid populating the `Referer` header with your phishing URL. There is still one issue with redirecting the user if the website does not load any new pages after successful sign-in. This I will try to tackle in future updates.

License changed from GPL to BSD-3

In short - GPL requires to redistribute the tool with full source code. BSD-3 is more permissive, allowing to redistribute the tool without it.

Changelog

The full changelog for Evilginx 3.0 is as follows:

- Feature: TLS certificates from LetsEncrypt will now get automatically renewed.

- Feature: Automated retrieval and renewal of LetsEncrypt TLS certificates is now managed by `certmagic` library.
- Feature: Authentication tokens can now be captured not only from cookies, but also from response body and HTTP headers.
- Feature: Phishing pages can now be embedded inside of iframes.
- Feature: Changed redirection after successful session capture from `Location` header redirection to injected Javascript redirection.
- Feature: Changed config file from `config.yaml` to `config.json`, permanently changing the configuration format to JSON.
- Feature: Changed open-source license from GPL to BSD-3.
- Feature: Added `always` modifier for capturing authentication cookies, forcing to capture a cookie even if it has no expiration time.
- Feature: Added `phishlet <phishlet>` command to show details of a specific phishlet.
- Feature: Added phishlet templates, allowing to create child phishlets with custom parameters like pre-configured subdomain or domain. Parameters can be defined anywhere in the phishlet file as `{param_name}` and every occurence will be replaced with pre-configured parameter values of the created child phishlet.
- Feature: Added `phishlet create` command to create child phishlets from template phishlets.
- Feature: Renamed lure `templates` to lure `redirectors` due to name conflict with phishlet templates.
- Feature: Added `{orig_hostname}` and `{orig_domain}` support for `sub_filters` phishlet setting.
- Feature: Added `{basedomain}` and `{basedomain_regexp}` support for `sub_filters` phishlet setting.
- Fixed: One target can now have multiple phishing sessions active for several different phishlets.
- Fixed: Cookie capture from HTTP packet response will not stop mid-term, ignoring missing `opt` cookies, when all authentication cookies are already captured.
- Fixed: `trigger_paths` regexp will now match a full string instead of triggering true when just part of it is detected in URL path.
- Fixed: Phishlet table rows are now sorted alphabetically.
- Fixed: Improved phishing session management to always create a new session when lure URL is hit if session cookie is not present, even when IP whitelist is set.
- Fixed: WebSocket connections are now properly proxied.

Evilginx Online Documentation

As Evilginx kept growing it become harder and harder to keep up with all the features. GitHub Wiki kind of worked to, at least, provide documentation for the latest phishlet format, but I've never been fully satisfied with it.

I've always wanted the documentation to be easily accessible, well structured, easy to navigate and to have a quality look & feel. I can happily say, I may've found the perfect solution with Docusaurus.

Evilginx most up-to-date documentation, since today, will always be accessible through one official URL: https://help.evilginx.com

Check it out!

I honestly think, now with Evilginx having proper documentation, it will become much easier for everyone to use. I strongly hope you make good use of it! I'm often using it myself when I forget how the tool I made is supposed to work :P

Closing thoughts

The last 6 years have been a wild ride and I can't thank everyone enough for giving Evilginx a shot. I've never expected a tool, based on a simple idea, would eventually become a tool people use at work, to simulate phishing attacks. Mention of Evilginx even made it to TechCrunch, at one point.

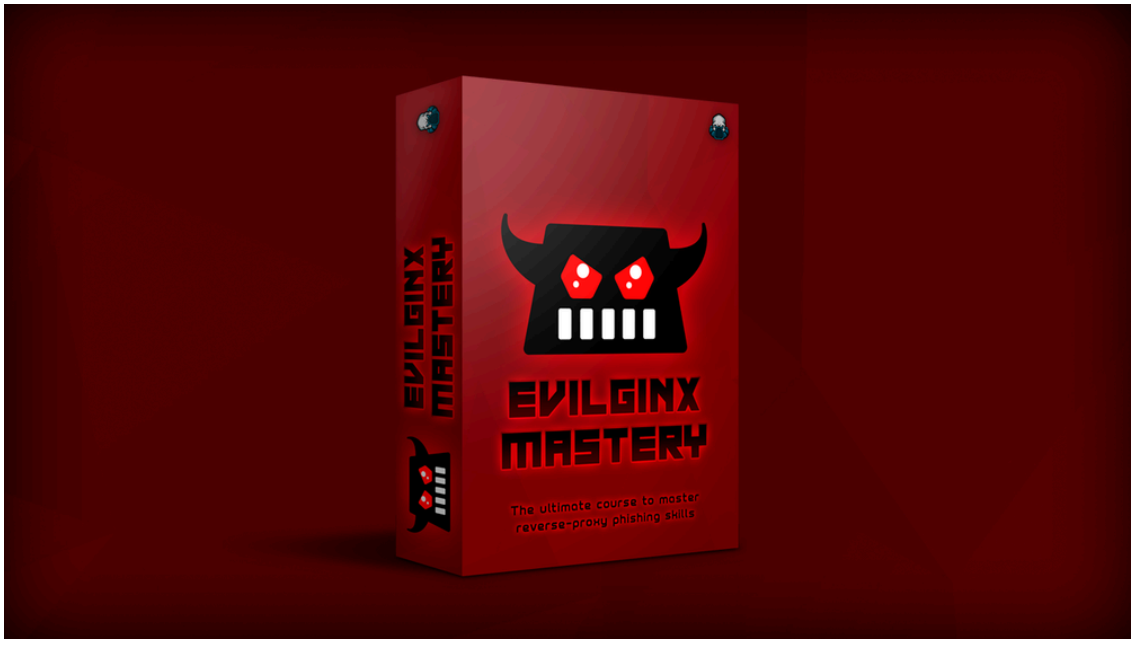
I really hope Evilginx will continue to serve its purpose in aiding you during your phishing engagements. Thank you, again, and if you decide to give Evilginx Mastery course a try, accept my eternal gratitude!

To end with a cliffhanger, I will say that Evilginx story is not over and there may be **Evilginx Pro** in the works, with some special features I decided to keep private for now. The pro version will most likely be licensed only to cybersecurity companies. Some of you may find mentions about private features in the official online documentation.

For updates follow me on Twitter @mrgretzky and Mastodon @mrgretzky@infosec.exchange.

If you have any inquires about company discounts or if you require any custom functionality in Evilginx, you can always contact me directly at: kuba@breakdev.org.

As always - enjoy and stay tuned!



Evilginx Mastery - Available NOW

Source: https://breakdev.org/evilginx-3-0-evilginx-mastery/