Evilginx 2.2 - Jolly Winter Update

By Kuba Gretzky

Published: 2018-11-22 · Archived: 2026-04-29 02:11:03 UTC

Tis the season to be phishing!

I've finally found some free time and managed to take a break to work on preparing a treat for all of you phishing enthusiasts out there. Just in time for the upcoming holiday season, I present you the chilly Evilginx update.

[Download Evilginx 2 from GitHub](https://github.com/kgretzky/evilginx2)

If you've arrived here by accident and have no idea what I'm writing about, do check the first post about Evilginx 2 release.

Without further ado, let's jump straight into the changelog!

Changelog - version 2.2

First, here is a full list of changes made in this version.

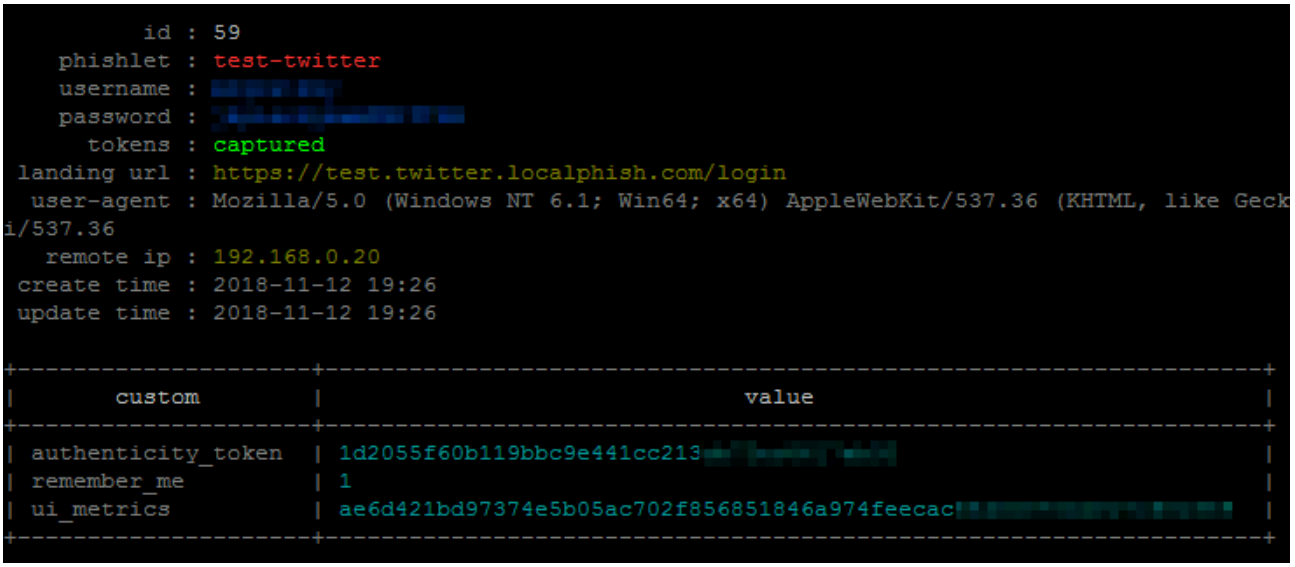
- Added option to capture custom POST arguments additionally to credentials. Check `custom` field under `credentials`.
- Added feature to inject custom POST arguments to requests. Useful for silently enabling **"Remember Me"** options, during authentication.
- Restructured phishlet YAML config file to be easier to understand (phishlets from previous versions need to be updated to new format).
- Removed `name` field from phishlets. Phishlet name is now determined solely based on the filename.
- Now when any of `auth_urls` is triggered, the redirection will take place **AFTER** response cookies for that request are captured.
- Regular expression groups working with `sub_filters`.
- Phishlets are now listed in a table.
- Phishlet fields are now selectively lowercased and validated upon loading to prevent surprises.
- All search fields in the phishlet are now regular expressions by default. Remember about proper escaping!

Now for the details.

> **Added option to capture custom POST arguments**

You can now capture additional POST arguments in requests. Some people mentioned they often need to capture data from other fields like PINs or tokens. Now you can.

Captured field values can be viewed in captured session details.



Find out how to specify custom fields for capture in the official documentation.

> **Added feature to inject custom POST arguments to requests. Useful for silently enabling "Remember Me" options, during authentication**

Almost all websites provide an option to login, without permanently remembering the logged in user. This results in the website storing only temporary session cookies or cookies with short lifespan, which are later invalidated both on the server and the client.

Capturing session cookies, in such scenario, does not give the attacker permanent access. This is why it is most important that phished user ticks the **"Remember Me"** checkbox to inform the server that persistent authentication is requested. Till now that rested on phished user's shoulders and they could make the decision.

In this version it is now possible to inject an argument into the POST request to inform the server that the **"Remember Me"** checkbox was ticked (even though it could've been deliberately left unchecked).

As an example, this part of a phishlet will detect the login POST request, containing username and password fields and will add/replace the `remember_me` parameter to always have a value of `1`:

```
force_post:
 - path: '/sessions'
   search:
     - {key: 'session\[user.*\]', search: '.*'}
     - {key: 'session\[pass[a-z]{4}\]', search: '.*'}
   force:
     - {key: 'remember_me', value: '1'}
   type: 'post'
```

Play around with it and I'm sure this feature may have other uses that I haven't thought about yet.

> **Remade phishlet YAML file format**

Preparing for a final version of the phishlet file format, I did some restructuring of it. You will need to do some minor modifications to your custom phishlets, to make them compatible with Evilginx 2.2.0.

I've now also properly documented the new phishlet file format, so please get familiar with it here:
[Phishlet File Format 2.2.0 Documentation]

> **Removed `name` field from phishlets**

Many of you reported proxy returning TLS errors when testing your own custom phishlets. They were caused by custom phishlets having the same `name` as another loaded phishlet.

That `name` field caused enough confusion, so I decided to remove it altogether. Phishlet name is now solely determined by the phishlet filename without the `.yaml` suffix. This should provide full uniqueness for each phishlet name as two same filenames can't exist in same directory, from which phishlets are loaded from.

> **Now when any of `auth_urls` is triggered, the redirection will take place AFTER response cookies for that request are captured**

In previous versions, whenever any of `auth_urls` triggered the session capture, the redirection would happen immediately, before Evilginx could parse the response, received from the server.

This resulted in Evilginx not being able to parse and capture cookies returned in responses to that last request that would trigger the session capture and redirection.

This is now changed and you can safely pick the trigger URL path that still returns session cookies in the response, as they will be captured and saved, before the redirection happens.

> **Regular expression groups working with `sub_filters`**

I've been asked about it recently and upon checking, I figured out that it has already been implemented since Evilginx release.

You can define a regular expression group, as you'd normally do, with parenthesis in `search` field and later refer to it in `replace` field with `${1}`, where `1` is the group index and you can naturally use more than one group.

Example:

```
    - {triggers_on: 'www.linkedin.com', orig_sub: 'cdn', domain: 'linkedinapis.com', search: '//{hostname}/([0-9a
```

Refer to GO language documentation to see exactly how it works (make sure to see the example section):
https://golang.org/pkg/regexp/#Regexp.ReplaceAllString

> **Phishlets are now listed in a table**

Simply said - phishlets listing was an ugly mess. Now it looks good.

```
: phishlets

+---------------+-------------+----------+------------+-----------------------------+
|   phishlet    |   author    |  active  |  status    |          hostname           |
+---------------+-------------+----------+------------+-----------------------------+
| twitter       | @white_fi   | disabled | available  | twitter.localphish.com      |
| amazon        | @customsync | enabled  | available  | amazon.localphish.com       |
| facebook      | @mrgretzky  | disabled | available  |                             |
| google        | @mrgretzky  | enabled  | available  | google.localphish.com       |
| linkedin      | @mrgretzky  | disabled | available  | linkedin.localphish.com     |
| outlook       | @mrgretzky  | disabled | available  | outlook.localphish.com      |
| reddit        | @customsync | disabled | available  |                             |
| test-twitter  | @white_fi   | enabled  | available  | test.twitter.localphish.com |
+---------------+-------------+----------+------------+-----------------------------+
```

> **Phishlet fields are now selectively lowercased and validated upon loading to prevent surprises**

Evilginx will now validate each phishlet on loading. It will try its best to inform you about any detected issues with an error message to make it easier to debug any accidental mistakes like typos or missing fields.

> **All search fields in the phishlet are now regular expressions by default**

The phishlet documentation now specifies which fields are considered to be regular expressions, so do remember about proper escaping of regular expression strings.

As a quick example, if you used to look for `login.username` POST key to capture its value, you need to now define the field as `key: 'login\.username'`, because `.` is one of the special characters used in regular expressions, which has a separate function.

Enjoy!

As always, I wanted to thank everyone for amazing feedback and providing ideas to improve Evilginx.

Keep the bug reports and feature requests incoming!

[Follow me on Twitter](https://twitter.com/mrgretzky)

[Download Evilginx 2 from GitHub](https://github.com/kgretzky/evilginx2)
