HADESS.IO

# TALE OF PHISHING

Some Phishing Techniques & Awareness

HADESS

# Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

# Leveraging CSRF and Open Redirects

For this we can leverage common web application vulnerabilities

https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fappengine.google.com%2F_ah%2Fconflogin%3Fcontinue%3Dhttps%3A%2F%2Fattacker.domain%2F&service=ah

- allinurl:%3Dhttps*
- allinurl:%253Dhttps*
- allinurl:%3Dhttp*
- allinurl:%253Dhttp*
- allinurl:"<keyword>=https"
- allinurl:"<keyword>=http"
- allinurl:<keyword>=https
- allinurl:<keyword>=http
- allinurl:<keyword>%3Dhttps
- allinurl:<keyword>%3Dhttps*
- allinurl:<keyword>%253Dhttps
- allinurl:<keyword>%253Dhttps*
- allinurl:<keyword>%3Dhttp
- allinurl:<keyword>%3Dhttp*
- allinurl:<keyword>%253Dhttp
- allinurl:<keyword>%253Dhttp*

# Creating trustworthy-looking redirect forms

Targeting PayPal example
To understand how can this be achieved programmatically study the following

- Man-In-The-Middle Capabilities
- Wireshark
- Browser Extension

- capture_and_redirect.js
https://gist.github.com/anonymous/3bf8342c76eba4da3f660cbffa24f5d8
- PayPal phishing HTML form:
https://gist.github.com/anonymous/75b5eb6578bbc5bfcabe44e8fbb952ea
- jquery.ba-hashchange.min.js:
https://gist.github.com/anonymous/950a70cdebd3e78b6e88312fa7d93250

# URL Spoofing Techniques

https://dwbank.com

↓

https://dwbank.app

https://dw-bank.com

https://dwbànk.com

https://www-dwbank.com

HADESS.IO

# URL Spoofing Techniques

We will start discussing URL spoofing techniques with a word of advice: There is nothing better in phishing campaigns than a carefully selected and legitimate-looking phishing domain.

- https://elitedomains.de/tools/domain-typo-generator

- https://domaincheckplugin.com/typo

- https://www.expireddomains.net/

Some of URL Spoofing Techniques:

- Data URIs
  - https://gist.github.com/anonymous/907cc8e9dcc43c6a4412e682e5d5c2cd
- Phishing with Unicode Domains
- Full Frame with IFrame
- Encrypt HTML and Javascriptipt

BeEF


# ./beef

The Browser Exploitation Framework Project
Two Scenraio for use beef in phishing capmpaign

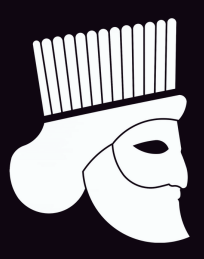
1. XSS + SAMEORIGIN + Autocomplete = Admin Credential
2. XSS -> CSRF bypass -> Admin level access

# Mimicking DYRE banking trojan's spread method

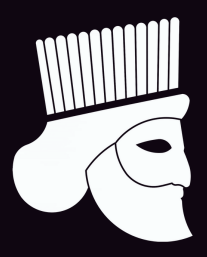
This technique misuses Messaging Application Programming Interface (MAPI) on Windows systems and mimics the way DYRE banking trojan spread.
PowerShell will be used since it can easily access the MAPI through an Outlook ComObject.
For example Retrieve the Primary SMTP Address for each person, then pipe the address into Invoke-SendMail as targets.

```
Get-SubFolders -DefaultFolder "Inbox" -
FullObject | Where-Object {$_.Name -eq
"TemporaryAccountPasswords"} | Get-
EmailItems -MaxEmails 20
```

Ref:
http://www.xorrior.com/phishing-on-the-inside/

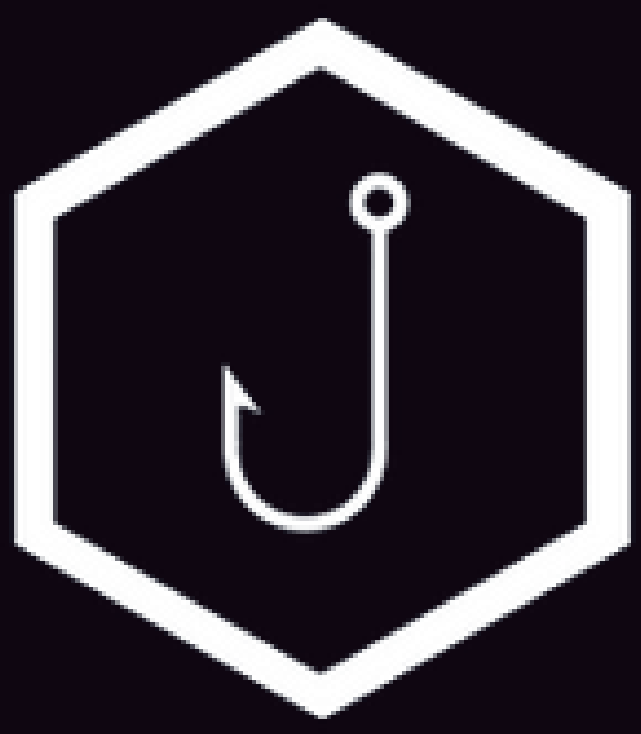


# Tools



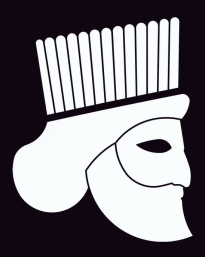
HADESS.IO

# Gophish



1. Set Templates & Targets
2. Launch the Campaign
3. Track Results

Repo:
https://github.com/gophish/gophish

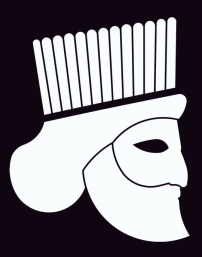


# DnsTwist


Domain name permutation engine for detecting homograph phishing attacks, typo squatting, and brand impersonation

dnstwist --registered domain.name

Repo: https://github.com/elceef/dnstwist



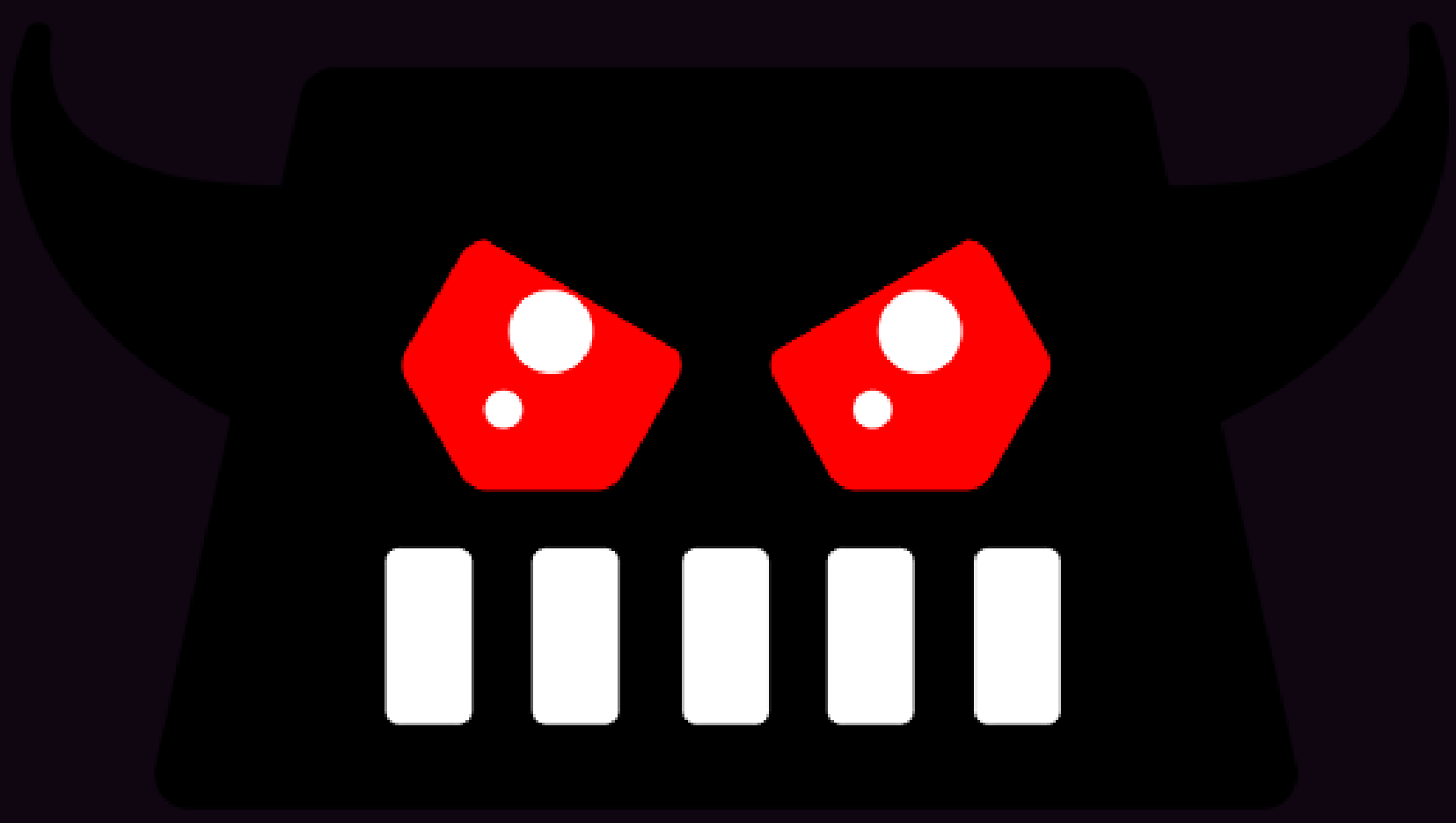
HADESS.IO

# Muraena


The tool re-implements the 15-years old idea of using a custom reverse proxy to dynamically interact with the origin to be targeted, rather than maintaining and serving static pages.

Repo: https://github.com/muraenateam/muraena

# evilginx2



evilginx2 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.

```
sudo ./bin/evilginx -p ./phishlets/
```

Repo:

https://github.com/kgretzky/evilginx2

HADESS.IO

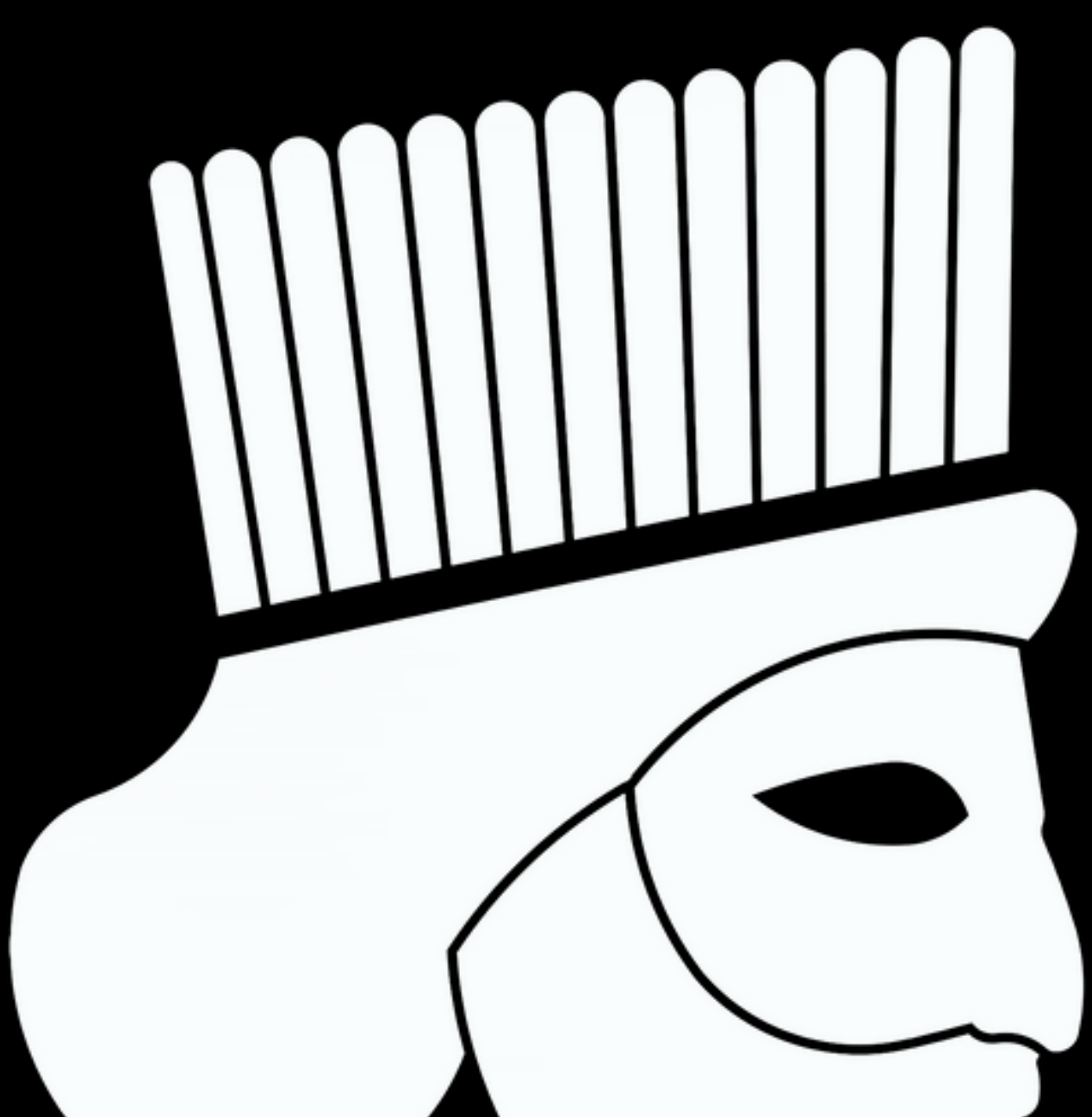
Hardening

Technology

Human

Awarenewss

- Employ common sense before handing over sensitive information.
- Never trust alarming message
- Do not open attachments
- Avoid clicking embedded links
- Keep your software and operating system up to date.
- Secure Web/Mobile/Desktop Applications
- Security with defence-in-depth



# HADESS