LEVELING UP YOUR PHISHING GAME ON MODERN PLATFORMS

Aaron Martin and Savannah Lazzara
INTRODUCTION

Aaron Martin

• Senior Security Consultant
• 10 Years Experience as Information System Security practitioner with U.S Military and Gov. Entities
• Adversary Simulation Services Operator

Savannah Lazzara

• Security Consultant
• OSCP
• Hack The Box Tampa Ambassador
• Advisor for Root@UT
AGENDA

• Introduction

• Phishing Phases

• How To Setup A Phishing Campaign

• Questions
OVERVIEW

In Today's world, Phishing is one of the most common attack vectors Enterprise's encounter on a regular basis.

Companies have advanced their tactics and approach to defending against unsolicited phishing emails with modern security controls in place.

To circumvent these ever-changing defenses in mature environments, it is important to understand the different layers at which these security controls are implemented and what can be done to bypass them.
PHASES

- Open Source Intelligence
- Plan Attack Scenario
- Build Infrastructure
- Execute Attack Scenario
GATHERING INFORMATION ON TARGET

• Conducting a successful phishing campaign is dependent on diligent open-source research.

• Sites like zoominfo and linkedin provide valuable information on targets such as job titles and location.

• Tailoring phishing campaigns towards individuals is crucial to not set off any alarms.
DOMAINT SELECTION

- When choosing a Domain for a Phishing engagement, options vary widely
- Sites like Godaddy.com, namecheap.com are common domain purchasing platforms
- Assimilate with the target company’s business sector or domain URL naming scheme
- Sites such as expiredomains.net provide access to purchasing recently expired domains that have established reputation
PHISHING SERVER SETUP

• Setting up a Phishing Server is one of the first steps in a Phishing Campaign

• Cloud instances are among the most popular such as EC2, Azure and Digital Ocean

• Tools needed to successfully complete the campaign should be installed such as evilginx and gophish which we discuss later in this presentation
**SMTP SERVER (AKA MAIL SERVER)**

- **Mailgun** - a free email service used to send, receive, and track emails through its API. We can leverage Mailgun for sending emails out. Follow the steps below to get Mailgun setup:

1. Setup MailGun account
2. Add domain
3. Mailgun will generate 2 TXT (SPF and DKIM) records
4. Add DNS records to Cloudflare
5. Make note of your SMTP server user/password
LEVERAGING CLOUDFLARE (FREE TIER)

Point your name servers to Cloudflare

Name servers
Name servers store the configuration of your domain as a collection of resource records. If you use the Google rest of this page to configure your domain. Alternately, you can enter up to 13 custom name servers here and use a different DNS provider. Learn more

- Use the Google Domains name servers
- Use custom name servers

- elisabeth.ns.cloudflare.com
- pablo.ns.cloudflare.com

This is an example, your name servers may be different

Update DNS Records

DNS management for yourdomain.com

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Content</th>
<th>TTL</th>
<th>Proxy status</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNAME</td>
<td></td>
<td>yourdomain.com</td>
<td>Auto</td>
<td>Proxied</td>
<td>Edit</td>
</tr>
<tr>
<td>CNAME</td>
<td>login</td>
<td>yourdomain.com</td>
<td>Auto</td>
<td>Proxied</td>
<td>Edit</td>
</tr>
<tr>
<td>CNAME</td>
<td>www</td>
<td>yourdomain.com</td>
<td>Auto</td>
<td>Proxied</td>
<td>Edit</td>
</tr>
<tr>
<td>MX</td>
<td></td>
<td>mxb.mailgun.org</td>
<td>10</td>
<td>DNS only</td>
<td>Edit</td>
</tr>
<tr>
<td>MX</td>
<td></td>
<td>mxa.mailgun.org</td>
<td>10</td>
<td>DNS only</td>
<td>Edit</td>
</tr>
<tr>
<td>TXT</td>
<td>pic_domainkey</td>
<td>yourdomain.com</td>
<td>Auto</td>
<td>DNS only</td>
<td>Edit</td>
</tr>
<tr>
<td>TXT</td>
<td></td>
<td>yourdomain.com</td>
<td>Auto</td>
<td>DNS only</td>
<td>Edit</td>
</tr>
<tr>
<td>A</td>
<td></td>
<td>yourdomain.com</td>
<td>Auto</td>
<td>Proxied</td>
<td>Edit</td>
</tr>
</tbody>
</table>
LEVERAGING CLOUDFLARE (FREE TIER)

Block email filters source IPs from scanning your URL
LEVERAGING CLOUDFLARE (FREE TIER)

Utilize Cloudflare's SSL Certificate

Copy Certificate to EC2 Instance

```
cp cert.pem /root/.evilginx/crt/<domain>.com/<NAME_OF_PHISHLET>.crt

cp privkey.pem /root/.evilginx/crt/<domain>.com/<NAME_OF_PHISHLET>.key
```

Outcome

- You are securely connected to this site.
- Verified by: Cloudflare, Inc.
EVILGINX

• Most mature Enterprises utilize two-factor authentication for authentication with most login portals

• Tools such as Evilginx effectively capture session tokens and passwords to bypass 2FA

• Various phishlets come pre-deployed with Evilginx to assimilate with the target environment

<table>
<thead>
<tr>
<th>Application</th>
<th>User</th>
<th>Status</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>citrix</td>
<td>@424f424f</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>outlook</td>
<td>@mrgretzky</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>protonmail</td>
<td>@jamescullum</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>wordpress.org</td>
<td>@meitar</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>amazon</td>
<td>@customsync</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>linkedin</td>
<td>@mrgretzky</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>okta</td>
<td>@mikesiegel</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>onelogin</td>
<td>@perfectlylog...</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>coinbase</td>
<td>@An0nud4y</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>reddit</td>
<td>@customsync</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>tiktok</td>
<td>@An0nUD4Y</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>twitter-mobile</td>
<td>@white_hi</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>paypal</td>
<td>@An0nud4y</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>twitter</td>
<td>@white_hi</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>airbnb</td>
<td>@AN0NUD4Y</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>booking</td>
<td>@Anonymous</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>facebook</td>
<td>@charlesbel</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>github</td>
<td>@audibleblelink</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>instagram</td>
<td>@charlesbel</td>
<td>disabled</td>
<td>available</td>
</tr>
<tr>
<td>o365</td>
<td>@jamescullum</td>
<td>disabled</td>
<td>available</td>
</tr>
</tbody>
</table>
Another Benefit of using Evilginx is the ability to create lures.

Lures essentially direct your target to the specified domain that your phishing server is hosted.

These can be delivered via various methods such as embedded in an email.
CREATING AN EMAIL

- Formatting phishing emails play a critical role in the validity of a phishing scenario.

- Excess graphics should be avoided as to not trigger spam filters.

- Evilginx Lures aka phishing landing page should be embedded in the email with a reference to link as to not expose the actual URL.

- The Sender Email and context of the email should coincide with the evilginx phishlet to further add validity.
TESTING THE EMAIL

• Sites like Mailtrap.io provide feedback and spam score of a potential phishing email

• Gain Understanding of domain reputation and HTML configurations within email

• Test emails before sending to ensure successful delivery to recipient
LAUNCHING THE CAMPAIGN

- Tools to launch phishing campaigns vary from ease of use to tracking capabilities and bulk sending options.

- Tread carefully as these tools can trigger spam filters and implemented security controls.

- Alternate solutions include manually sending through tools such as Microsoft Exchange Admin.
LAUNCHING THE CAMPAIGN CONTINUED
LAUNCHING THE CAMPAIGN

• Once you launch your campaign through whichever provider you choose, you wait for the credentials and/or session cookies if targeting MFA.

• After obtaining credentials, you can perform post exploitation :)