MUNICH CYBER TACTICS
TECHNIQUES AND PROCEDURES | 24

MCTTP

Automation Tactics For Threat Emulation

mcttp.de | #mcttp

VOGEL IT AKADEMIE

About Me (Arun Nair)

Full time memer, part time hacker

Go by the name Dazzy Ddos (@dazzyddos)

A hardcore anime fan

Explorer at heart, thrives on discovering new places - ChatGPT ;)

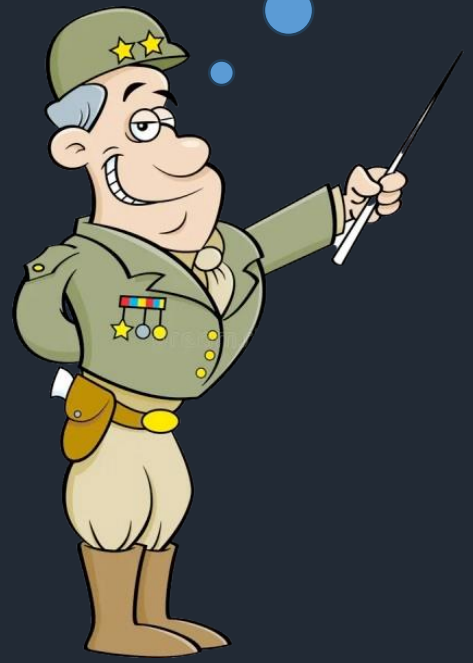
About Nikhil

Team Red @Deloitte

Loves to Travel (By Road)

Love/Hate relationship with EDRs

Setup a mind-blowing infra for next engagement



1

2

Using socat to redirect web traffic from one server to the local

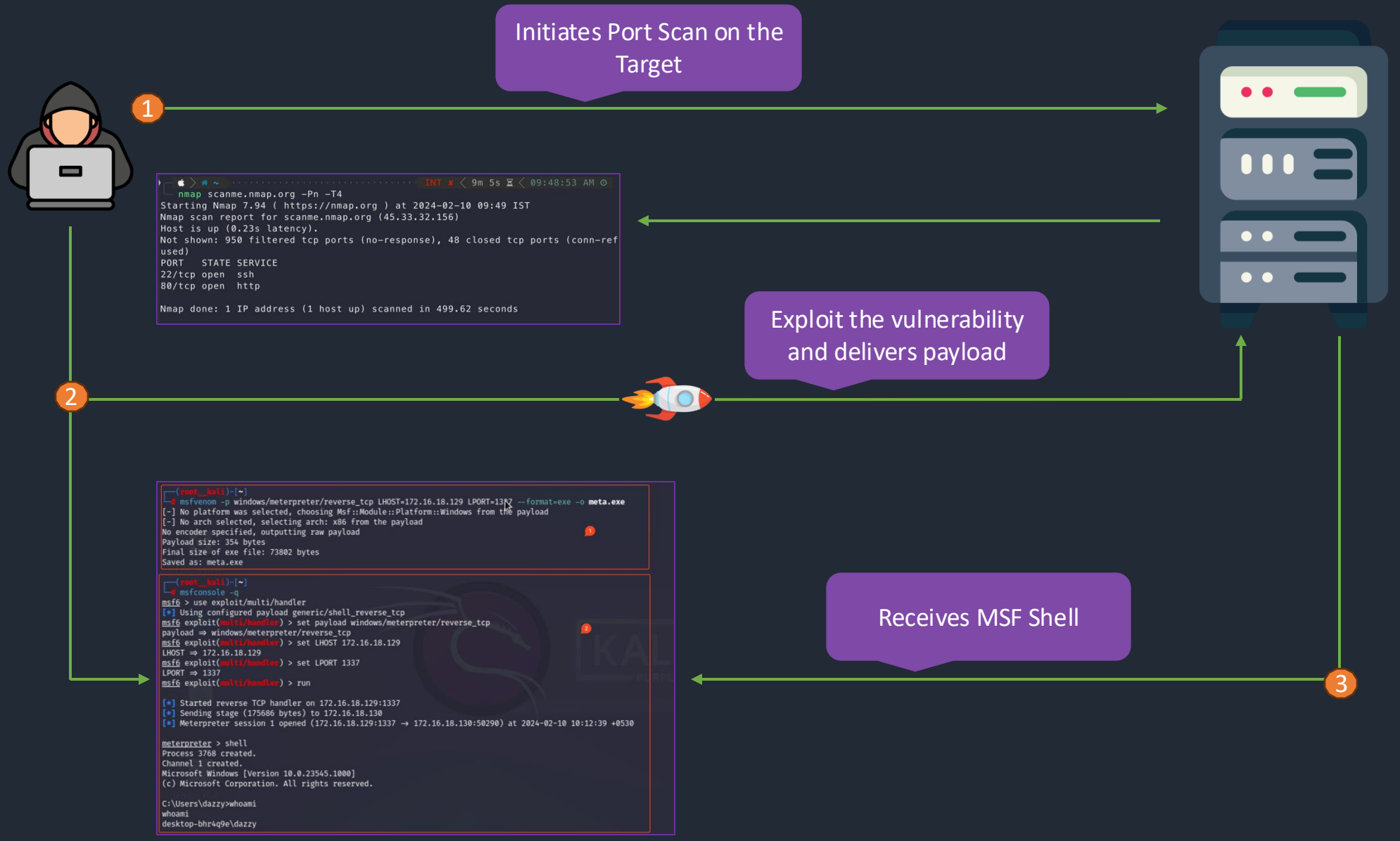
3

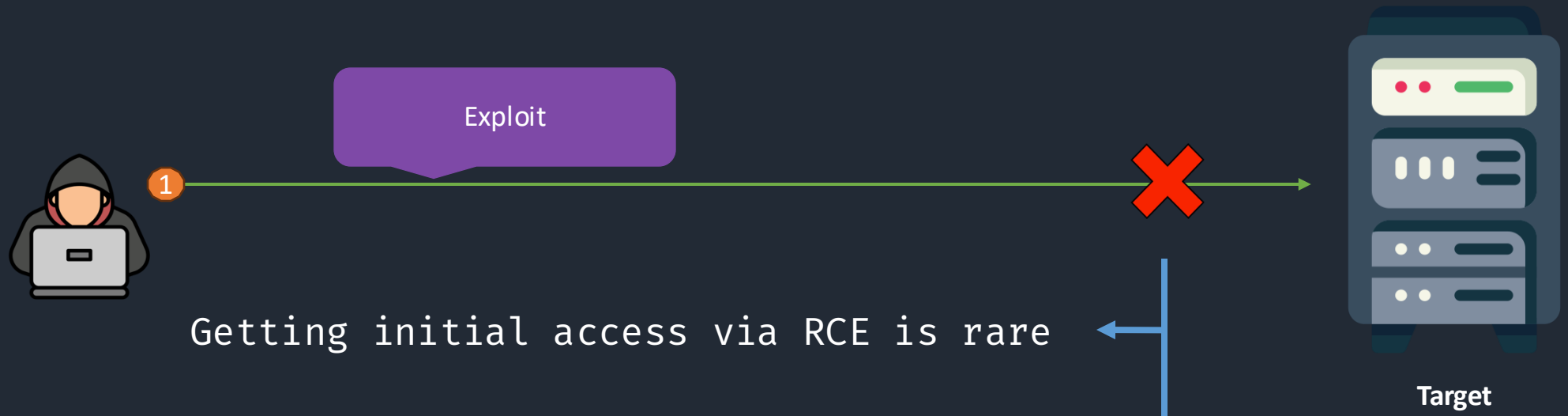
Teamserver Port Accessible on Internet

Using socat Redirector (Redirect Everything)

SSH on internet for instances

Ya'll Still Play CTF?





Getting initial access via RCE is rare

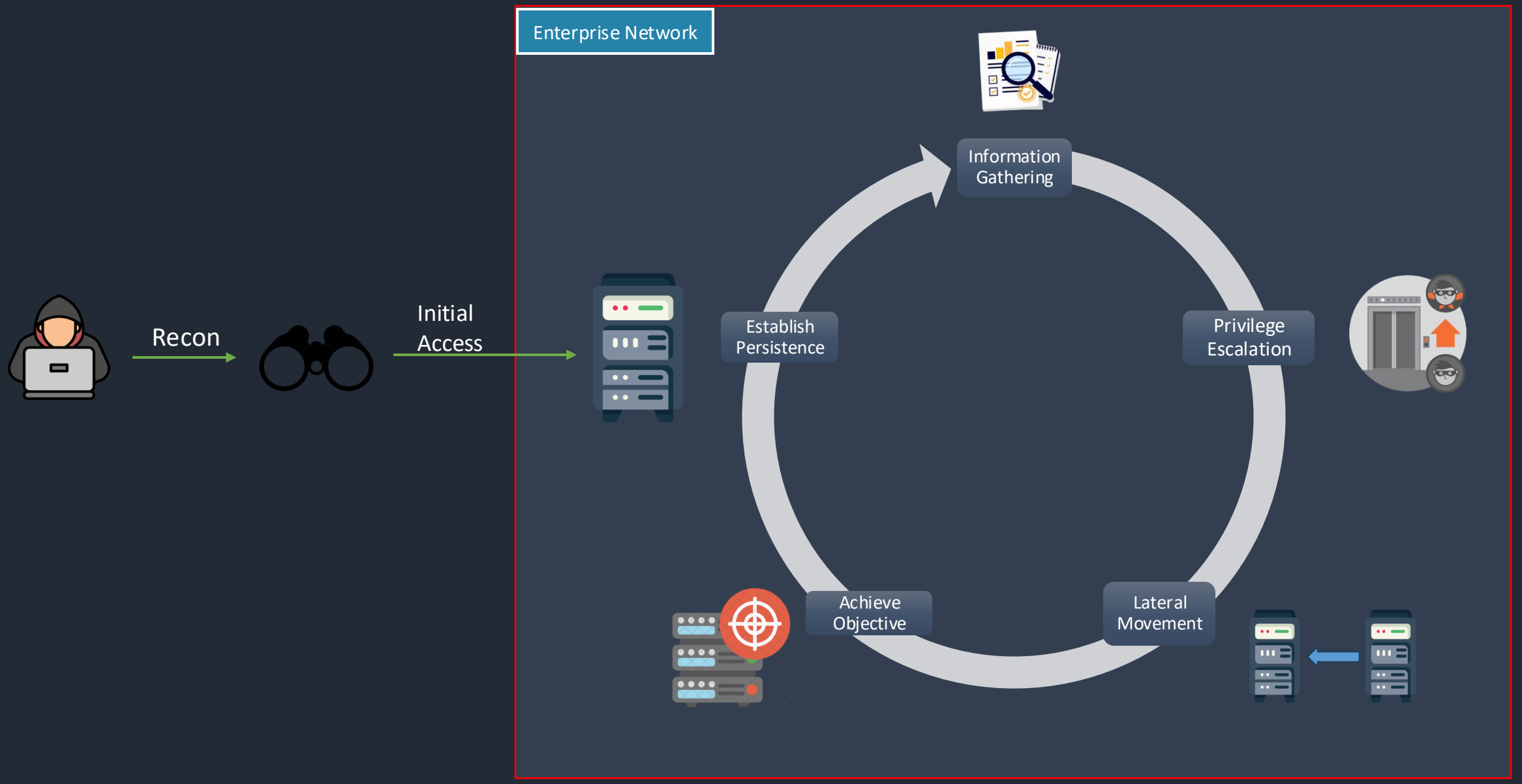
You wouldn’t wanna disrupt your target

Payload needs to be delivered in deliverable method

Reverse shell payload subject to Web proxy and EDR

And more…

Red Team Phases



Fitting Infrastructure Components to Phases

Recon

Attack Box
(Proxy)

Initial
Access

Redirector
Server

Phishing
Server

Payload
Server

Logging
Server

C2 Server

MalDev CI/CD

Enterprise
Network

Target

Red Team Infrastructure Design Essentials

SCALABLE

The infrastructure should be ready to expand or change as needed without missing a beat

SECURITY

All data must be encrypted as it moves in and out and there should be a system to monitor and log activities

STREAMLINED

Infrastructure should leverage automation tools for efficient setup, tear-down and management

Traditional v/s Modern Infrastructure

	Traditional	Modern
Bastion Host	✗	✓
Smart Redirectors	✗	✓
Logging Server	✗	✓
Cloud Services Integration	✗	✓
Opsec Practices	✗	✓
Automated Tools and Scripts	✗	✓

Modern

Traditional

Prerequisites for Red Team Infrastructure

T1583.001
Acquire Domains
- namecheap
- GoDaddy
- route53

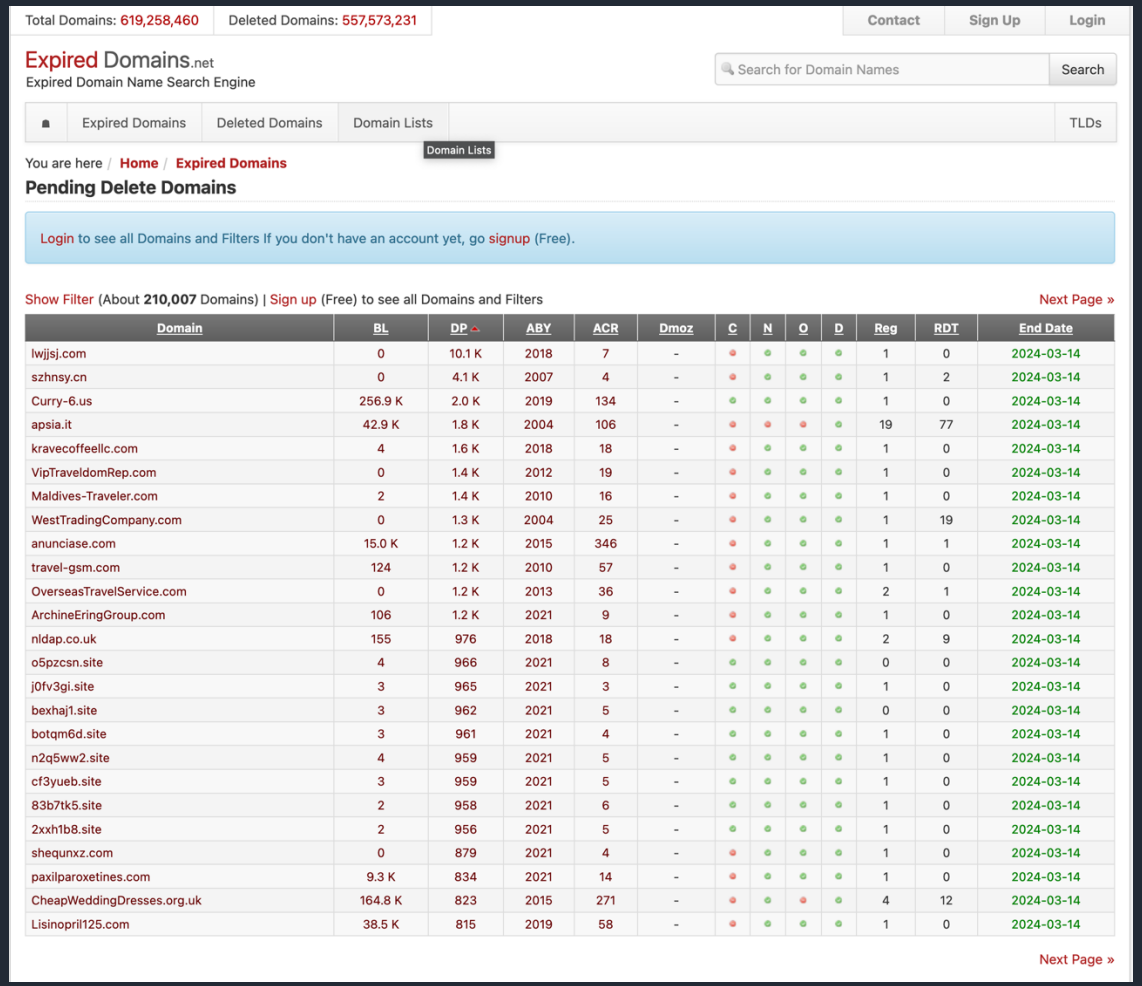
T1583.003
Acquire VPS
- EC2
- Azure VMs
- Digital Ocean Droplet

T1583.006
Acquire Web Services
- Mailgun
- SendGrid

T1587
Develop Capabilities
- SSL certificates
- Code Signing certificates

https://attack.mitre.org/tactics/TA0042/
https://scythe.io/library/attack-infrastructure-red-teams-vs-malicious-actors

Expired Domains



Domain	BL	DP	ABY	ACR	Dmoz	C	N	O	D	Reg	RDT	End Date
lwjjsj.com	0	10.1 K	2018	7	-					1	0	2024-03-14
szhnsy.cn	0	4.1 K	2007	4	-					1	2	2024-03-14
Curry-6.us	256.9 K	2.0 K	2019	134	-					1	0	2024-03-14
apsia.it	42.9 K	1.8 K	2004	106	-					19	77	2024-03-14
kravecoffeellc.com	4	1.6 K	2018	18	-					1	0	2024-03-14
VipTraveldomRep.com	0	1.4 K	2012	19	-					1	0	2024-03-14
Maldives-Traveler.com	2	1.4 K	2010	16	-					1	0	2024-03-14
WestTradingCompany.com	0	1.3 K	2004	25	-					1	19	2024-03-14
anunciase.com	15.0 K	1.2 K	2015	346	-					1	1	2024-03-14
travel-gsm.com	124	1.2 K	2010	57	-					1	0	2024-03-14
OverseasTravelService.com	0	1.2 K	2013	36	-					2	1	2024-03-14
ArchineEringGroup.com	106	1.2 K	2021	9	-					1	0	2024-03-14
nldap.co.uk	155	976	2018	18	-					2	9	2024-03-14
o5pzcsn.site	4	966	2021	8	-					0	0	2024-03-14
j0fv3gi.site	3	965	2021	3	-					1	0	2024-03-14
bexhaj1.site	3	962	2021	5	-					0	0	2024-03-14
botqm6d.site	3	961	2021	4	-					1	0	2024-03-14
n2q5ww2.site	4	959	2021	5	-					1	0	2024-03-14
cf3yueb.site	3	959	2021	5	-					1	0	2024-03-14
83b7tk5.site	2	958	2021	6	-					1	0	2024-03-14
2xxh1b8.site	2	956	2021	5	-					1	0	2024-03-14
shequnxz.com	0	879	2021	4	-					1	0	2024-03-14
paxilparoxetines.com	9.3 K	834	2021	14	-					1	0	2024-03-14
CheapWeddingDresses.org.uk	164.8 K	823	2015	271	-					4	12	2024-03-14
Lisinopril125.com	38.5 K	815	2019	58	-					1	0	2024-03-14

Filtering domains by Age, Rank, Backlinks, Traffic and more

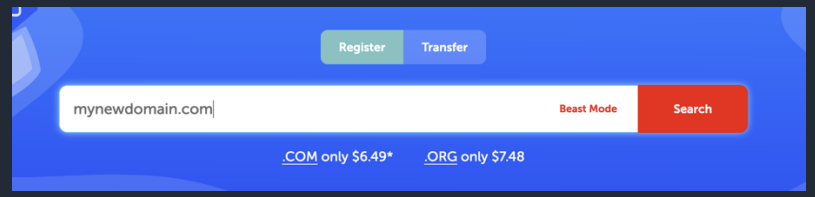
Using domains with existing history to increase chances of phishing

Acquire domain that matches target profile

https://expireddomains.net

Domain Categorization

Buy a domain



1

Host website on server

2

Send for categorization

3

Categorization in URL Filter database version '553168'

	URL	Status	Categorization	Reputation
	http:/[redacted].com	Uncategorized URL		Unverified

Some sites for checking/submitting domain categorization

Bluecoat/Symantec - https://sitereview.bluecoat.com/#/
McAfee - https://www.trustedsource.org
Palo Alto Wildfire - https://urlfiltering.paloaltonetworks.com
Websense - https://csi.forcepoint.com & https://www.websense.com/content/SiteLookup.aspx (needs registration)
FortiGuard - https://www.fortiguard.com/webfilter
IBM X-force - https://exchange.xforce.ibmcloud.com
Cyren - https://www.cyren.com/security-center/url-category-check-gate
Checkpoint - https://www.checkpoint.com/urlcat/main.htm (needs registration)

Before vs After Categorization

URL: [redacted]

Categories: Parked

Risk Level: Low-Risk

Category: Parked

Description: URLs which host limited content or click-through ads which may generate revenue for the host entity but generally do not contain content that is useful to the end user

Example Sites: www.parked.com

Risk Level: Low-Risk

Description: Any site that is not High Risk or Medium Risk. This includes sites that were previously confirmed as malicious but have displayed benign activity for at least 90 days

Example Sites: www.google.com, www.schwab.com, www.amazon.com

Request Change

no-reply-url-feedback@paloaltonetworks.com

to me

Thanks again for your URL re-categorization request. As a result of our re-evaluation, we have made the following changes:

URL: [redacted]
Previous category: parked
You suggested: business-and-economy
Accepted category: business-and-economy

URL: [redacted]

Categories: Business-and-Economy

Risk Level: Low-Risk

Category: Business-and-Economy

Description: Marketing, management, economics, and sites related to entrepreneurship or running a business. Includes advertising/marketing firms as well as shipping site such as fedex.com and ups.com. Corporate websites might be categorized with their technology instead of this category

Example Sites: www.bothsidesofthetable.com/, www.ogilvy.com, www.geisheker.com/, www.imageworksstudio.com/, www.linearcreative.com/

Risk Level: Low-Risk

Description: Any site that is not High Risk or Medium Risk. This includes sites that were previously confirmed as malicious but have displayed benign activity for at least 90 days

Example Sites: www.google.com, www.schwab.com, www.amazon.com

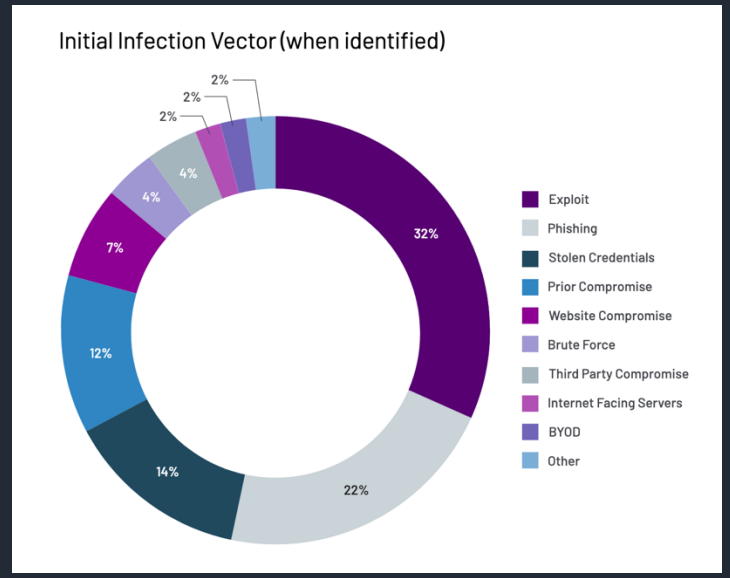
Request Change

Persistent Threat of Phishing

Phishing continues to be the most common initial access vector for cybersecurity incidents.

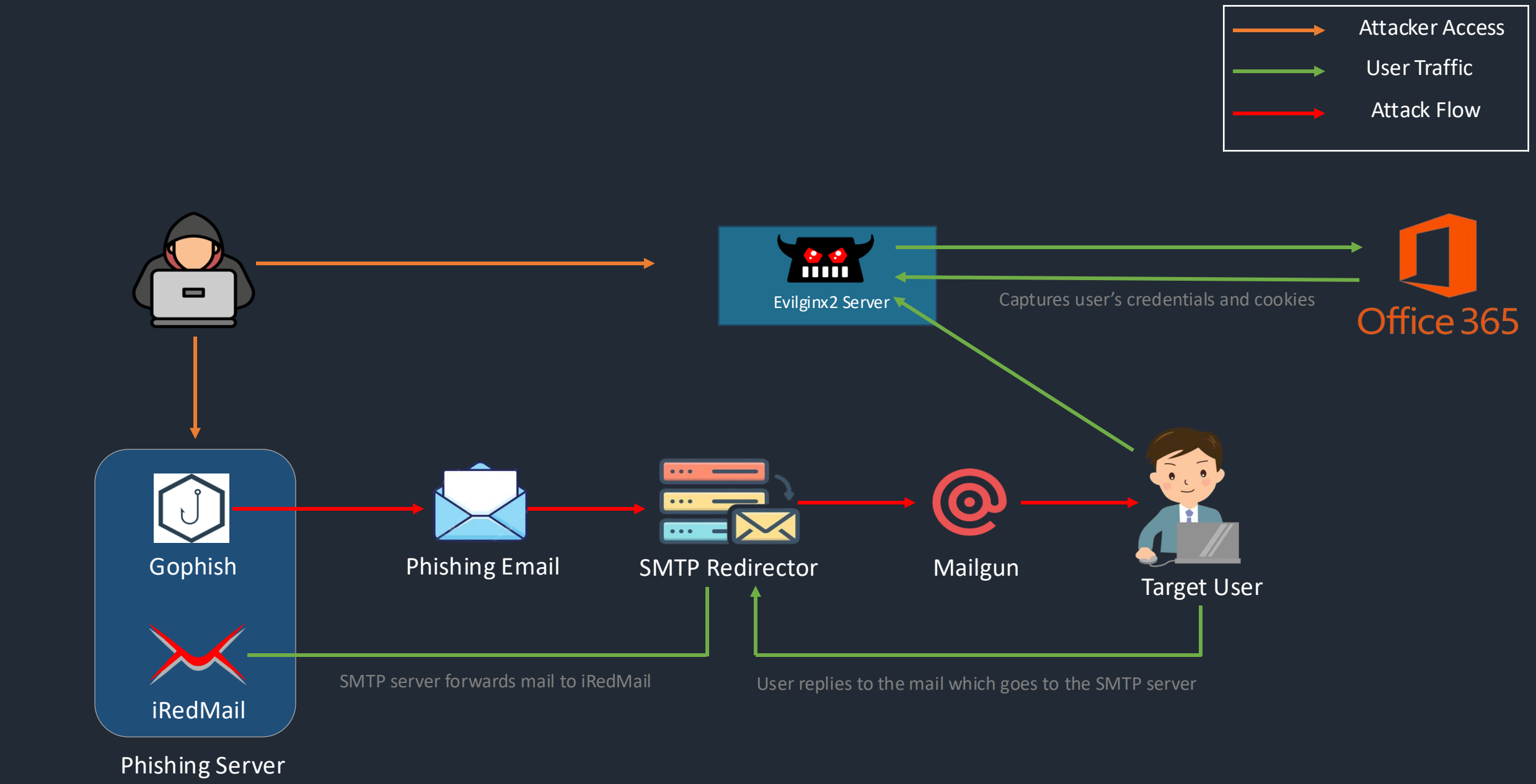
Phishing has been a go-to method for getting into systems for a long time. Hackers keep coming up with new tricks to make sure phishing stays effective.

- https://www.bleepingcomputer.com/news/security/microsoft-teams-phishing-pushes-darkgate-malware-via-group-chats/
- https://jeffreyappel.nl/aitm-mfa-phishing-attacks-in-combination-with-new-microsoft-protections-2023-edt/

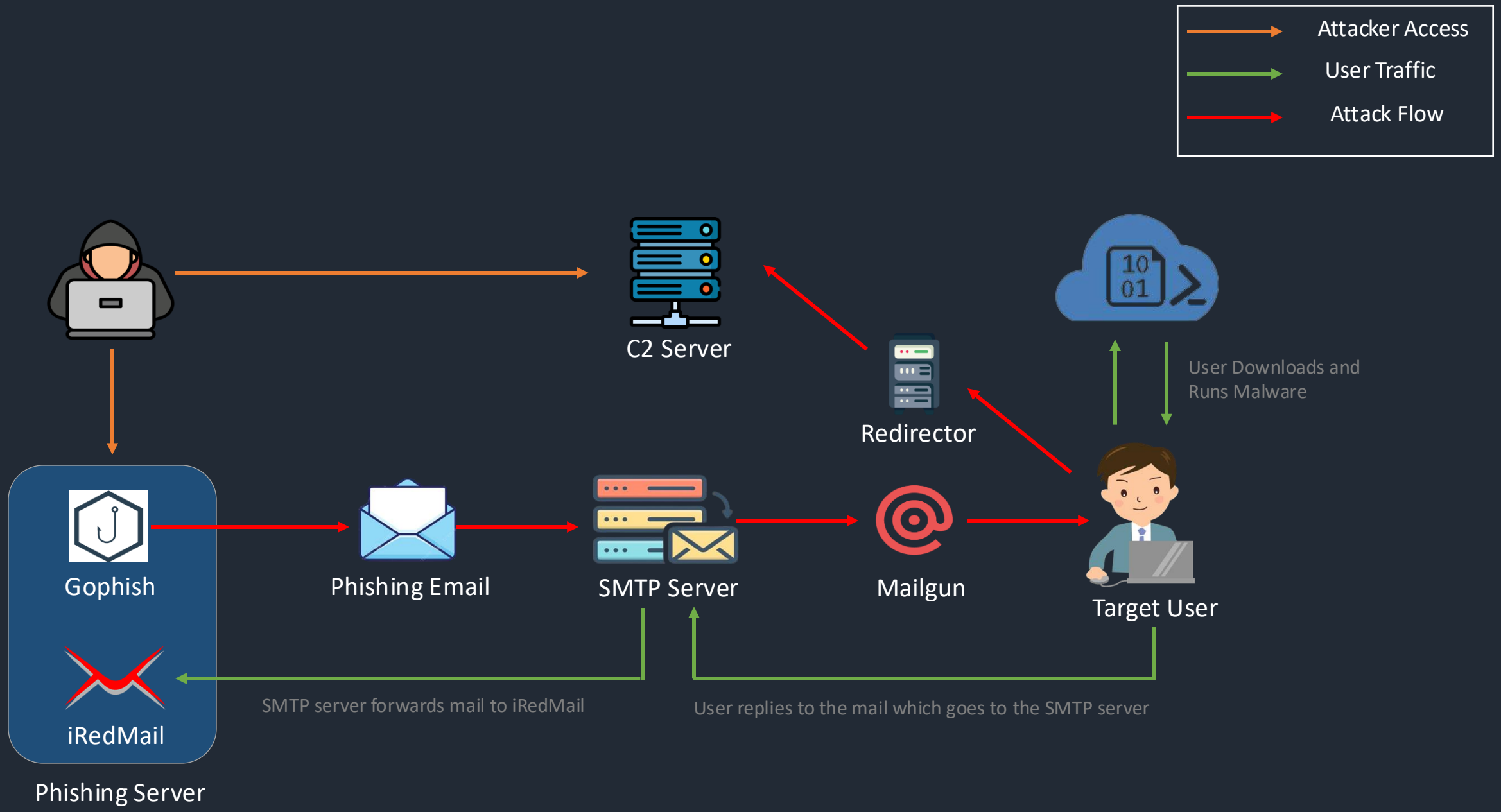


mandiant.com/m-trends

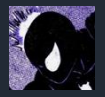
Phishing Setup for Credentials

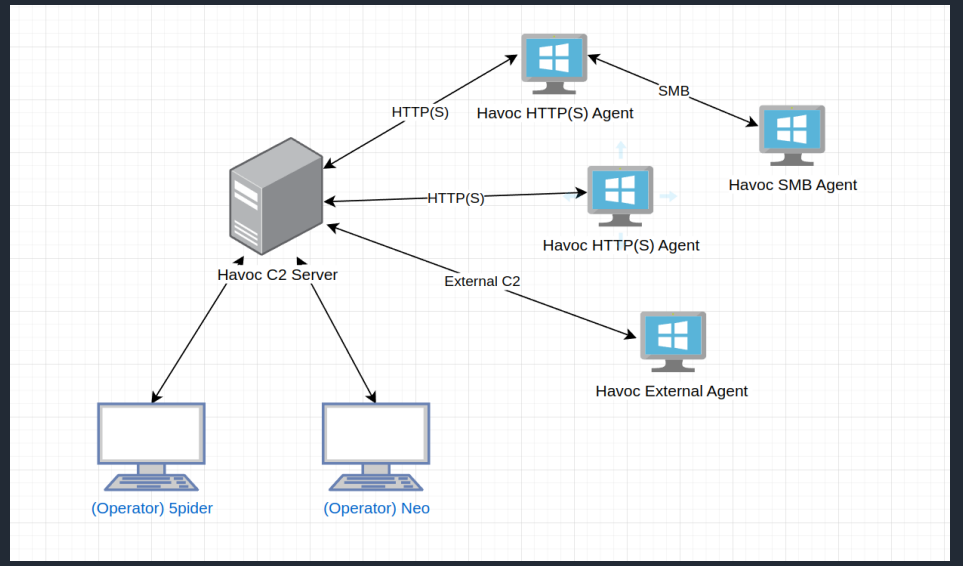


Phishing Setup for Malware



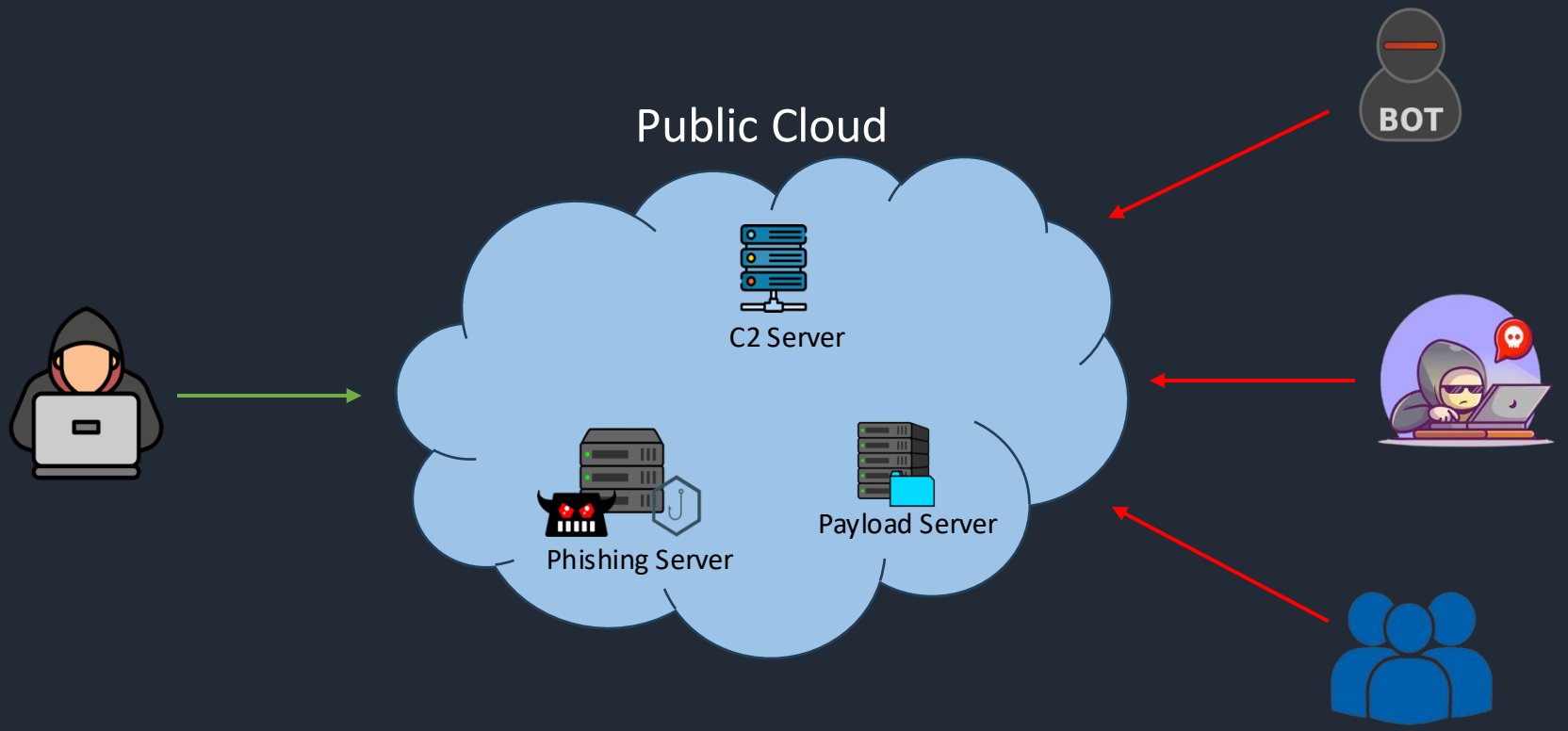
Havoc C2 Overview

- Open Source C2 Framework by @C5pider (Paul Ungur) 
- Well documented at https://havocframework.com/docs/welcome
- Havoc operates through a two-part architecture:
  - **Teamservers:** These are the nerve centers of Havoc, managing connections from operators and routing instructions to agents. They are responsible for parsing callbacks, managing listeners, and handling files or screenshots received from agents. Teamservers are typically hosted on public Virtual Private Servers (VPS) to ensure accessibility for authenticated operators.
  - **Clients:** These serve as the interface for the Teamservers, offering a platform for operators to issue commands to agents and review the resulting data or outputs.



Source: https://havocframework.com/docs/welcome

Risks of Hosting Red Team Infrastructure On the Internet



C2IntelFeedsBot
@drb_ra

Cobalt Strike Server Found
C2: HTTPS @ 192[.]3[.]101[.]133:4433
C2 Server: 192[.]3[.]101[.]133,/dpixel
Country: United States (AS36352)
ASN: HostPapa
#C2 #cobaltstrike

8:18 AM · Feb 10, 2024 · **86** Views

John F
@Abjuri5t

Now tracking the C2 servers of #NjRAT

SarlackLab @SarlackLab · Jan 29
live #njrat #C2 server
206.189.80[.]59:22614

confirmed 2024-01-28

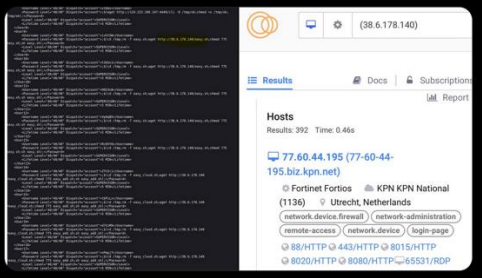
3:13 AM · Jan 29, 2024 · **204** Views

Fox threatintel
@banthisguy9349

search.censys.io/search?resourc...

Vpn server from threatactor that is observed regarding the #mirai #botnet.
The ip is exposed on the infected devices. 38.6.178.140. @NserversC

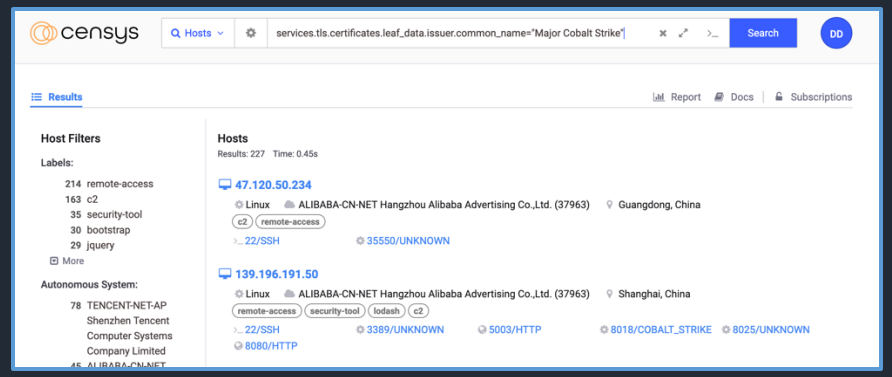
Who can help me report this vpn server?
The more reports the better.



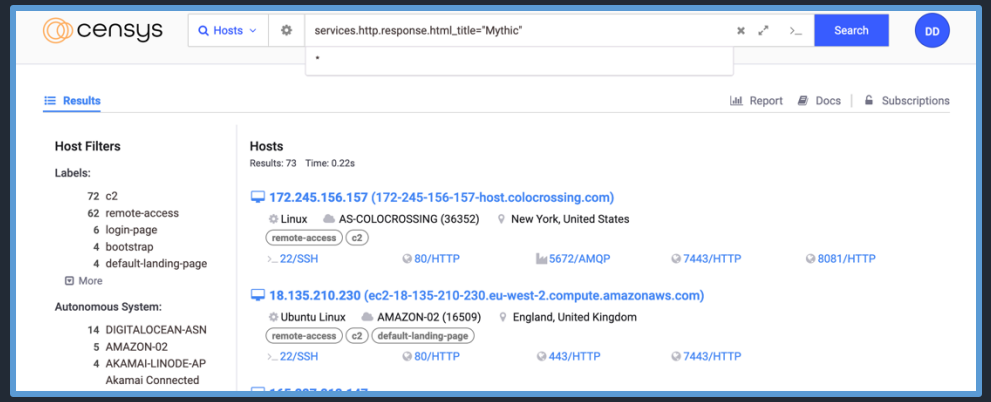
2:45 AM · Feb 10, 2024 · **581** Views

Hunting Malicious Infrastructure 101

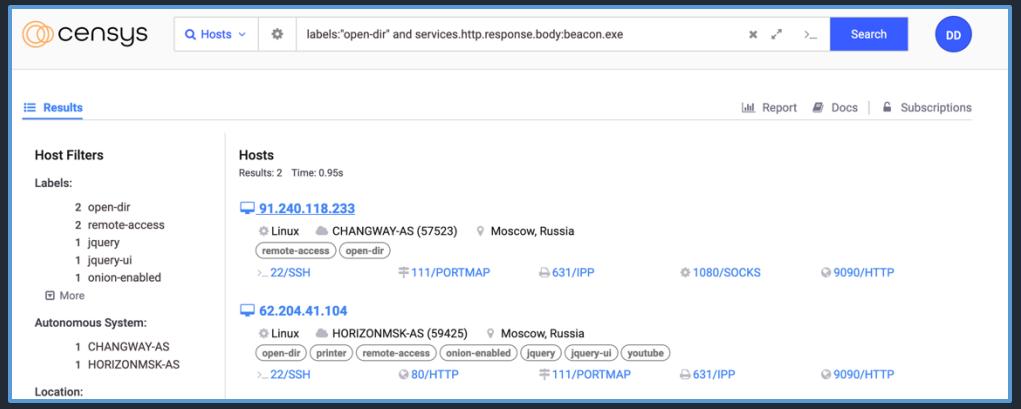
Hunting Cobalt Strike with TLS Certificate

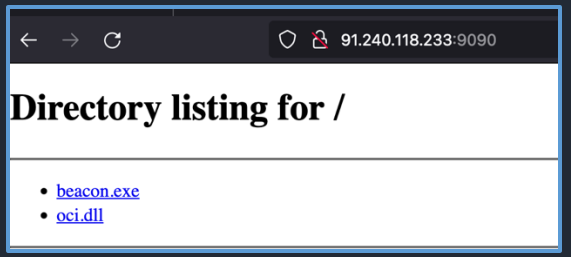


Hunting Mythic with HTTP Response Title



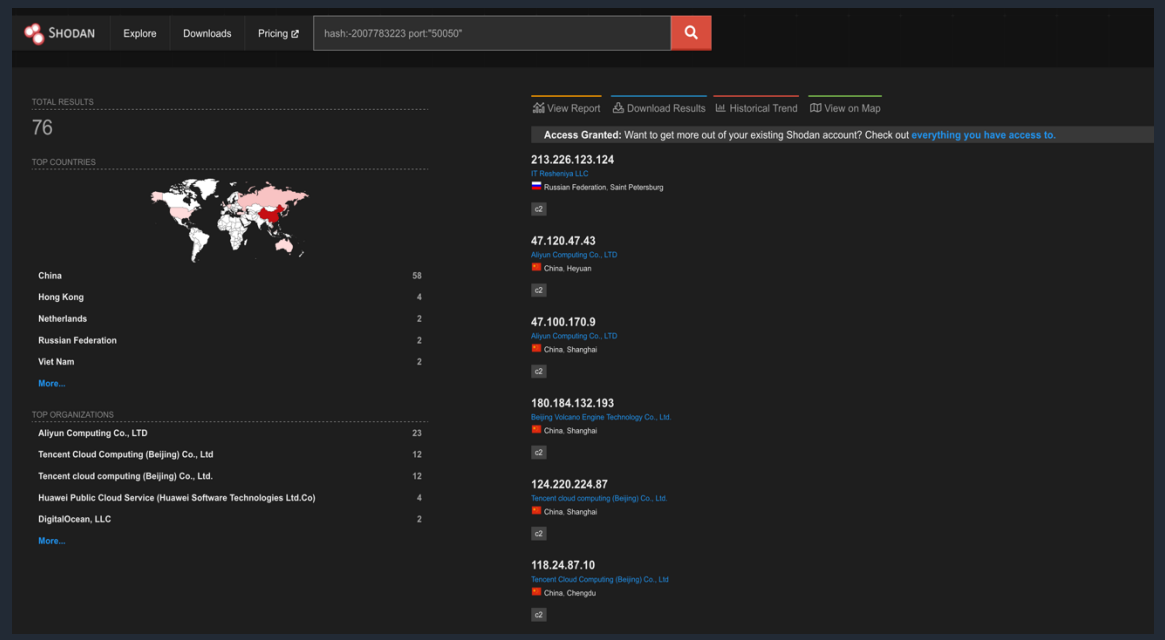
Hunting Cobalt Strike with Open Directories

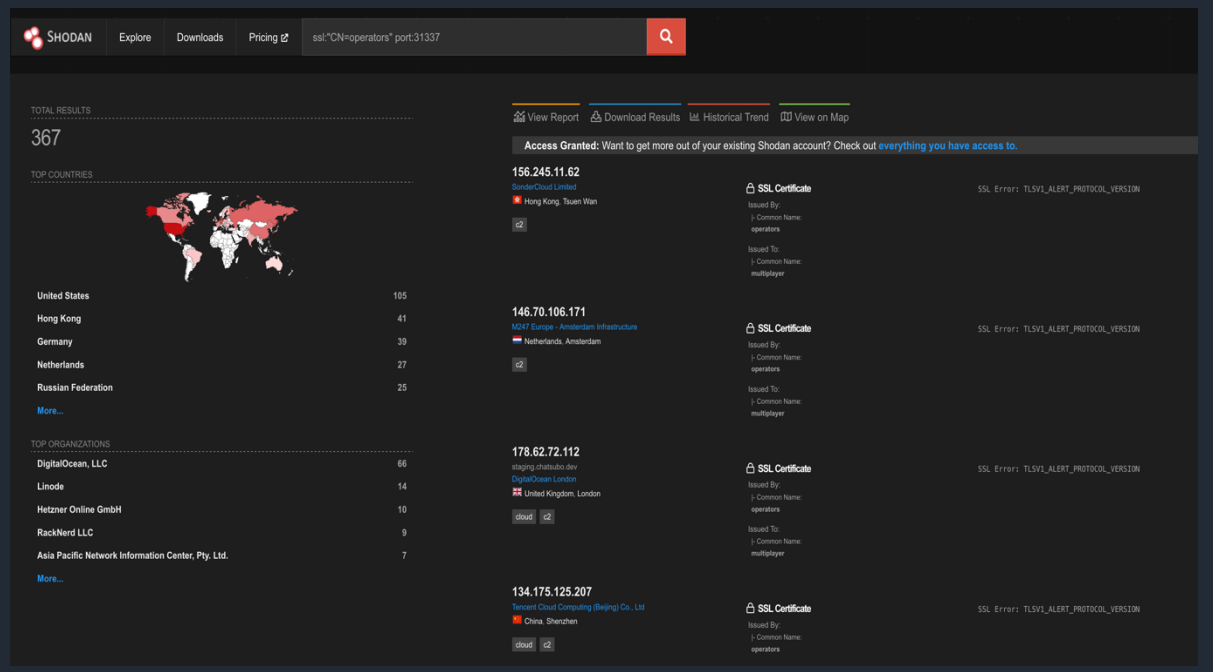


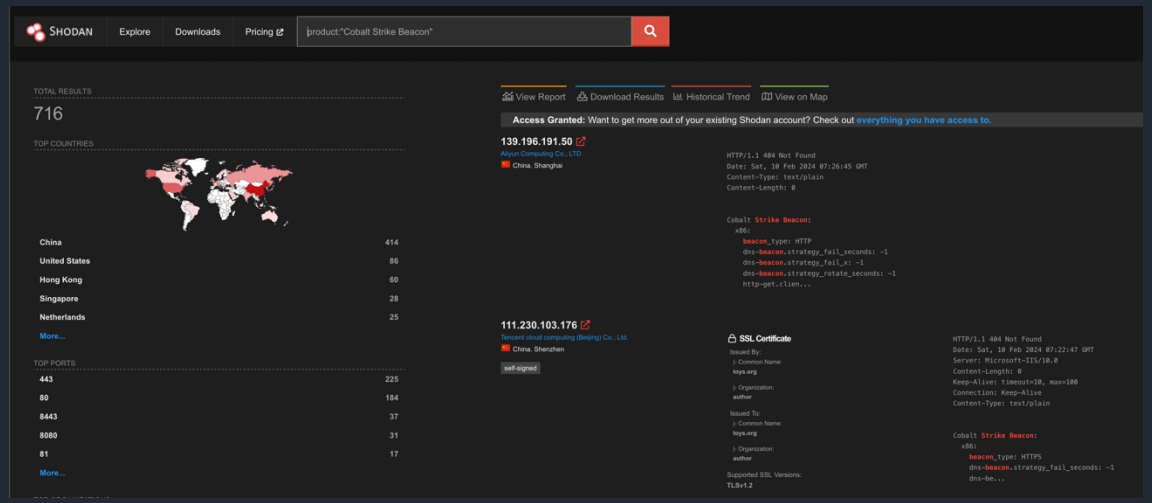


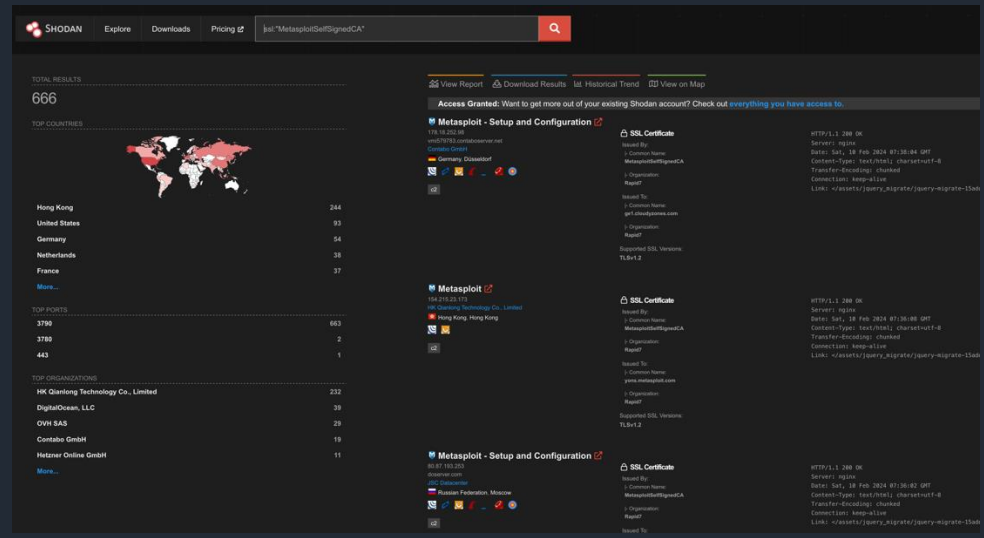
Source: https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/

Wanna Find Some More C2 Servers?



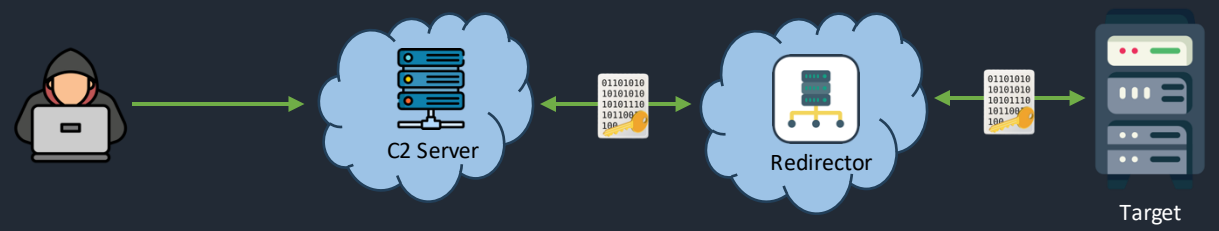




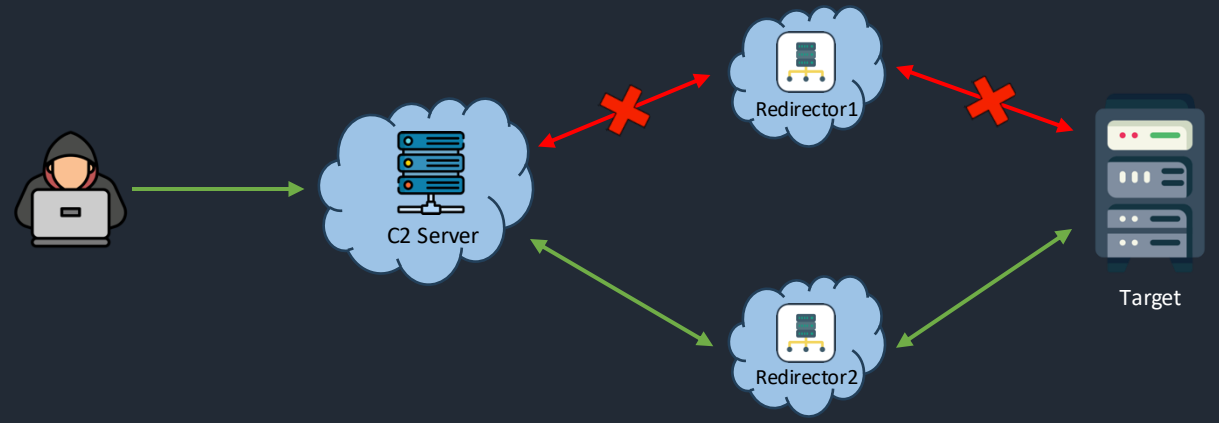


Redirectors to the Rescue

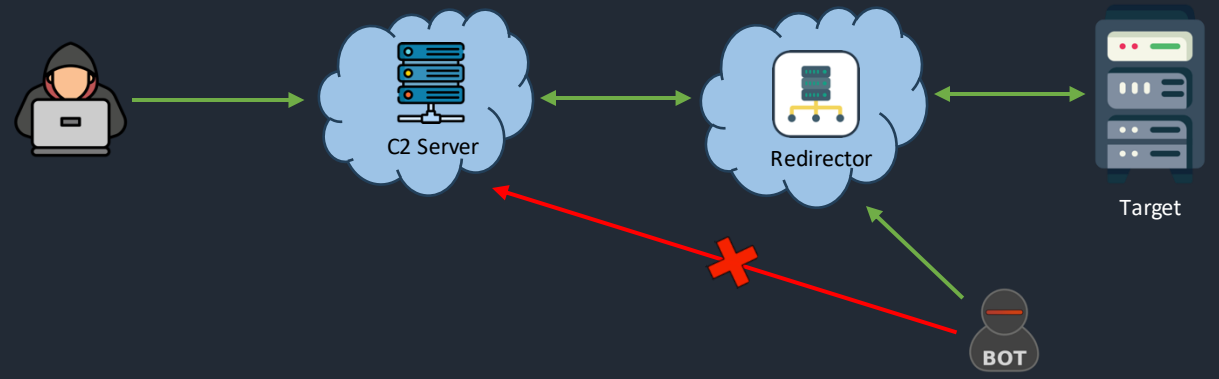
Obfuscate the source and nature of the malicious traffic



Provides an option for burnability by spinning up a new instance or rotating the IP



Works as an Intermediate layer to keep bots and scanners away



Redirector Goals

Purpose	Designed to handle specific types of traffic (HTTPS, SMTP, DNS) and only allow desired traffic to reach the private infrastructure, like C2 server or payload server
Deception	They can be configured to mislead investigators by controlling the outward appearance of the attack infrastructure
Cloud-Based	Typically hosted on cloud platforms for scalability. Easy to decommission and spin up
Lightweight and Minimalistic	Require minimal setup; often only a basic web server is necessary
Easily Automated	Can be quickly deployed or destroyed via automation tools, ideal of dynamic operation operations

Types of Redirectors (Dumb Redirector)

People call me dumb just because I am nice

Target User

Redirector

C2 Server

Send me whatever and I will forward that to my master

Types of Redirectors (Smart Redirector)

Nobody dare to touch my master

Target User

Redirector

C2 Server

URI Filtering

Host Header Filtering

IP Filtering

Geo Location Filtering

CDNs as a Redirector

CDNs are typically used to cache content, improving access speed

Advantages of CDN as a Redirector

Global Presence – CDNs have a widespread network of servers, making it harder to pinpoint the origin of traffic

Scalability – Easily and automatically scales to handle large volumes of traffic

Custom Domains – Mask the origin of content by using custom domains

Reputation Benefits – Utilizing CDN allows to piggyback on the trust and reputation of the Cloud provider's domain space, often whitelisted by organizations

SSL\TLS Encryption – CDN supports encryption out of the box

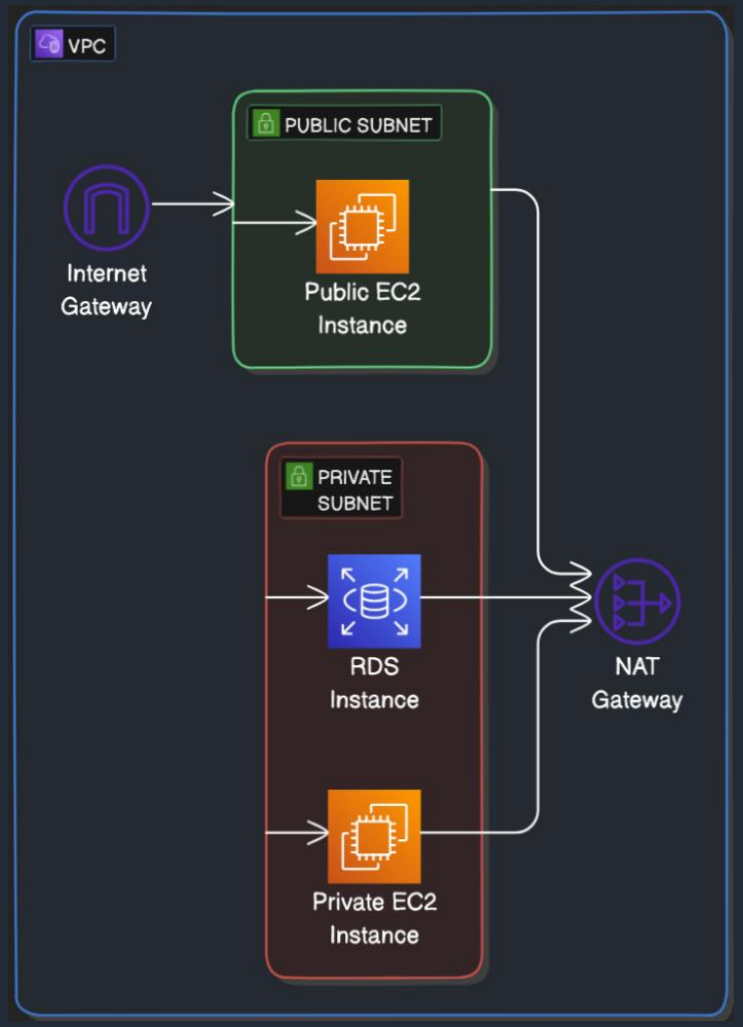
AWS CloudFront

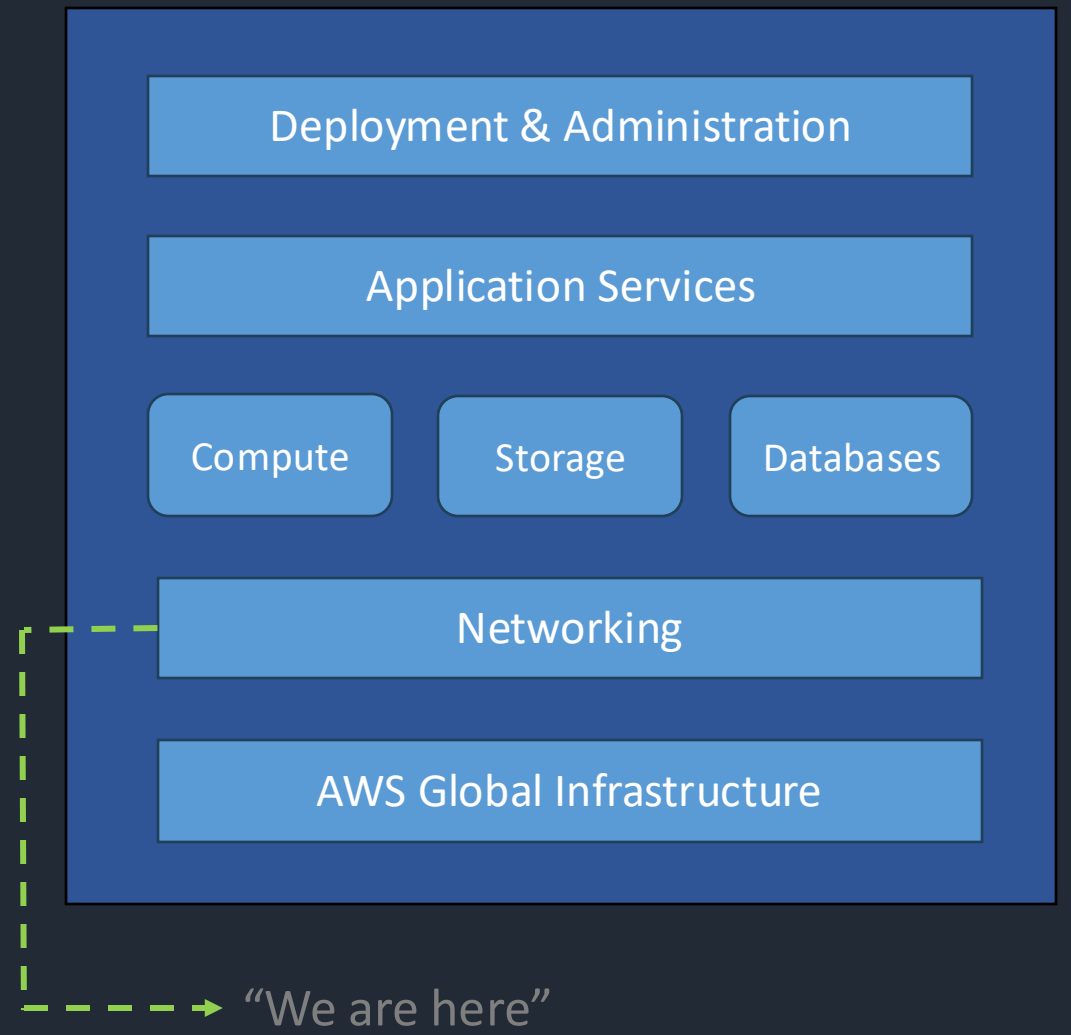
Azure CDN

CloudFlare

AWS Virtual Private Cloud

Secure, Isolated, and Customizable Networking





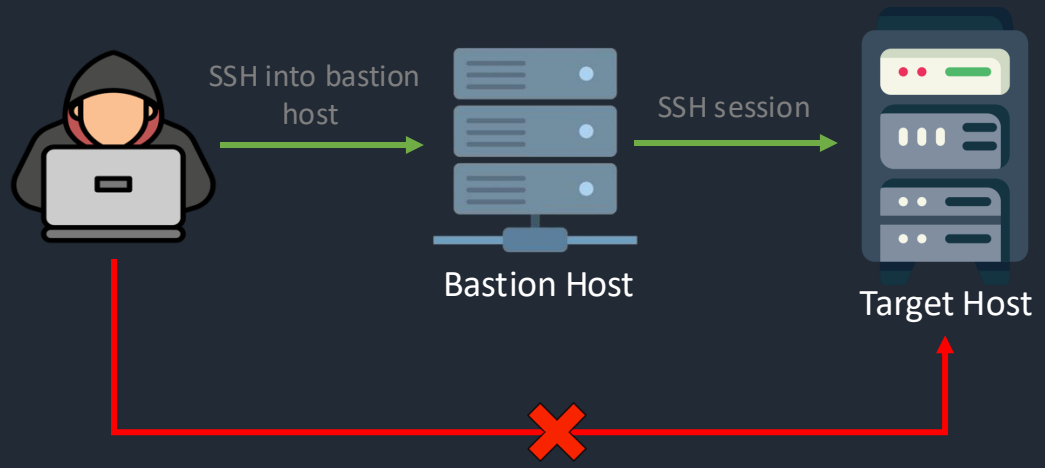
Bastion Host

Bastion Host, also known as “Jump Box”, serves as the entry point to a private network from an external network

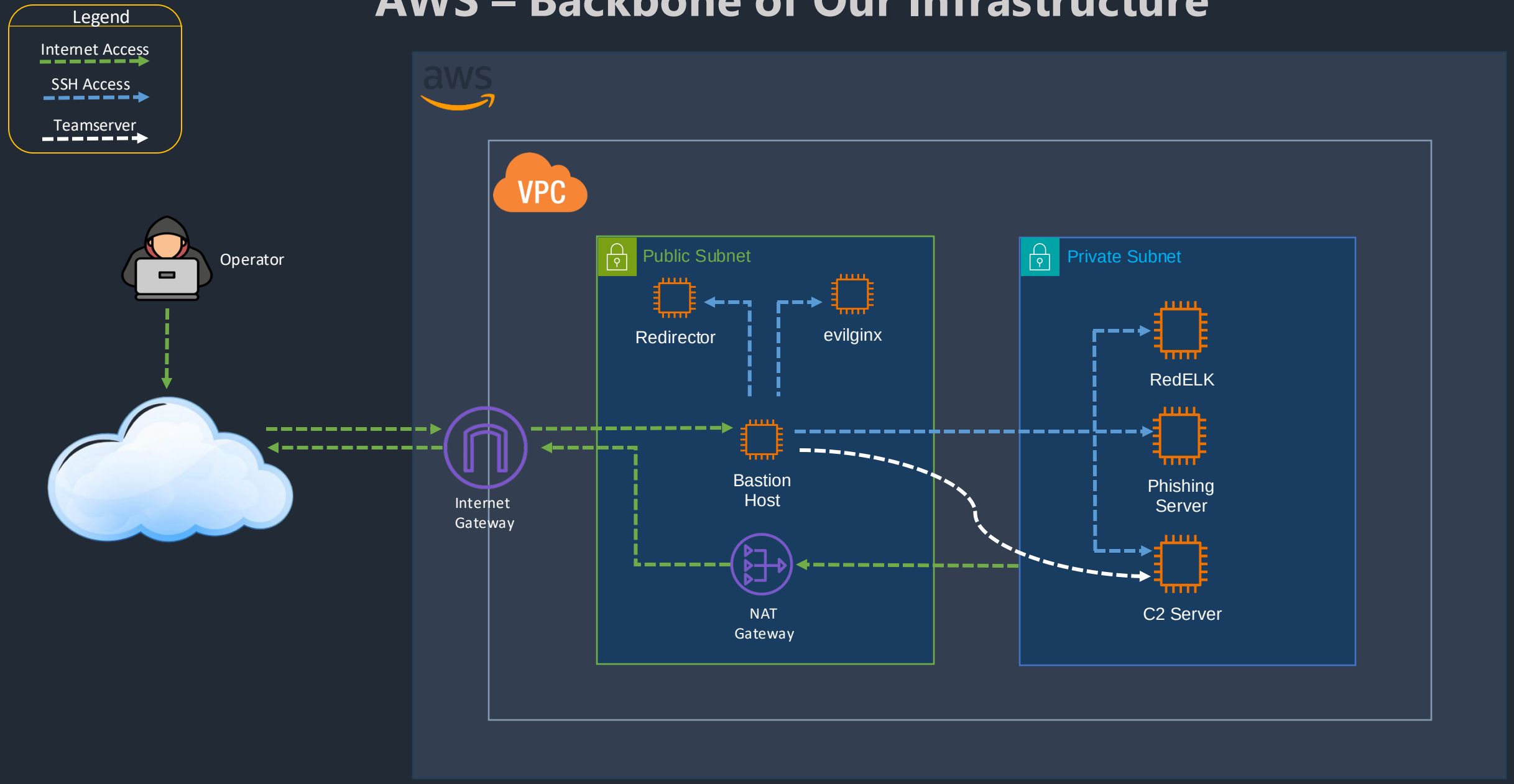
It provides a controlled and monitored entry point, limiting the exposure of other sensitive servers

We will setup our EC2 instances to accept SSH connections solely from the bastion host

Additionally, access to the C2 server’s Teamserver port will be exclusively through the bastion host which means to connect to C2 server, we’ll need to use port forwarding to channel the traffic via the bastion host



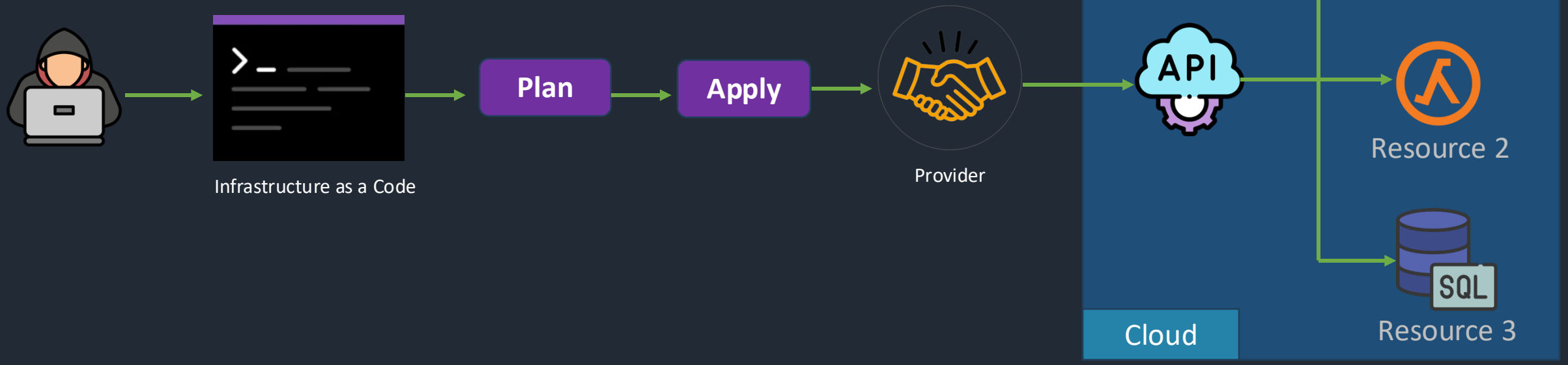
AWS – Backbone of Our Infrastructure



IaaC using Terraform

Terraform orchestrates and maintains infrastructure elements on cloud platforms by leveraging their respective APIs

Providers act as the bridge for Terraform, facilitating communication with various cloud services through these APIs enabling infrastructure automation

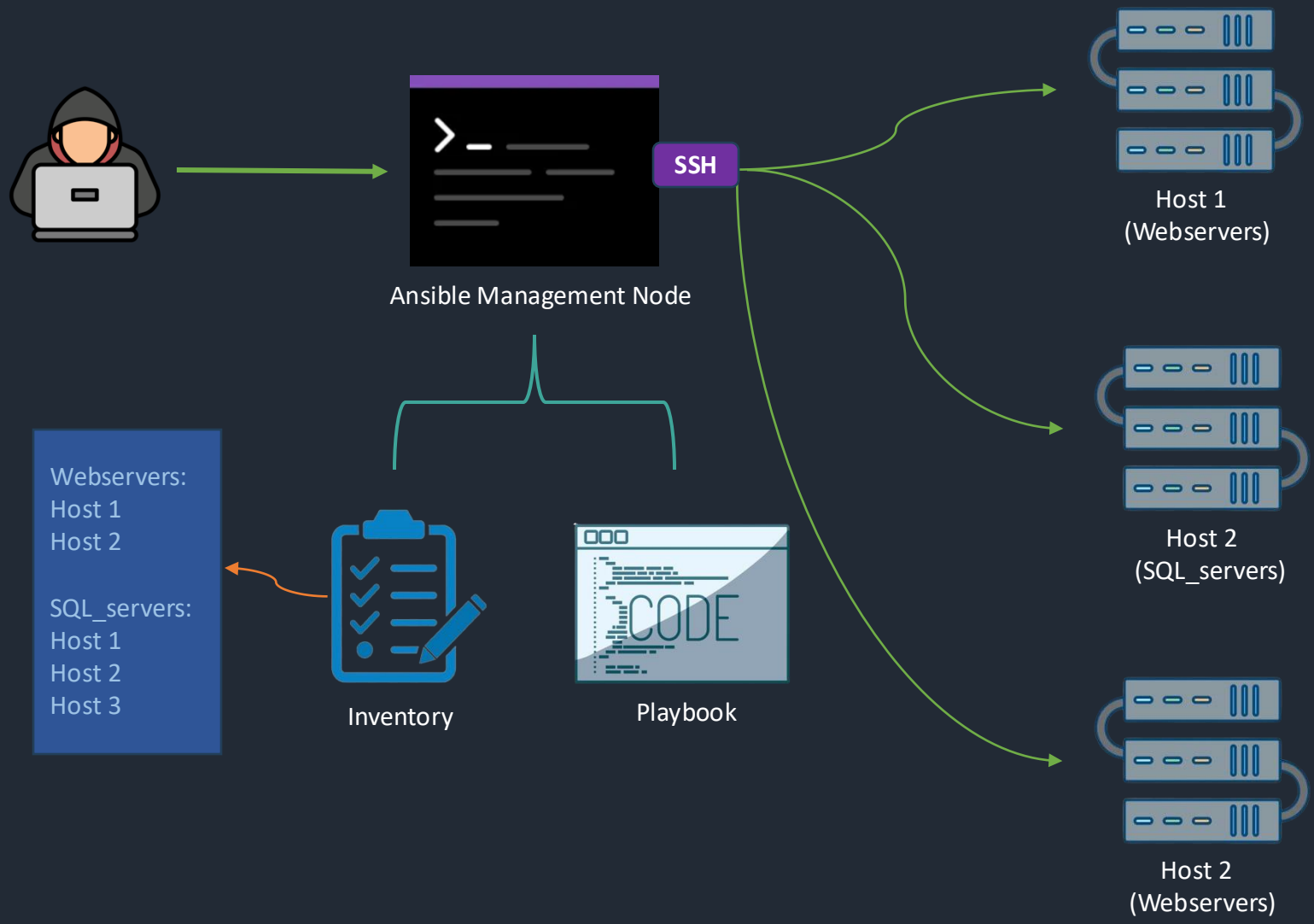


Configuration using Ansible

It runs everything over SSH, which is a secure way to access nodes remotely

Ansible automates tasks by connecting to nodes defined in the inventory and executes tasks defined inside the Ansible Playbook

Once Ansible completes the tasks, it cleans up after itself, leaving no extra software or agents behind



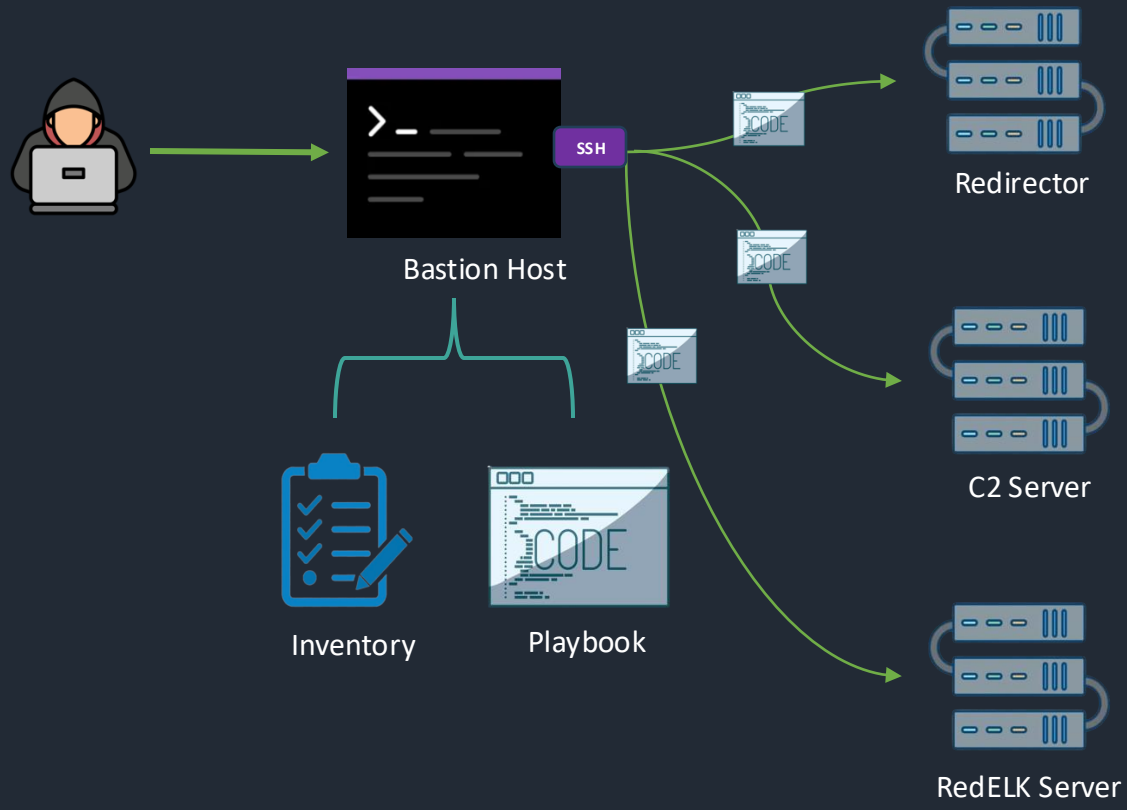
Terraform and then Ansible

Ansible is installed on the bastion host

Bastion host will be utilized for setting up each component via Ansible

For instance, following is the sample code for setting up Teamserver via bastion host

```
resource "null_resource" "setup_teamserver" {
    depends_on = [aws_instance.teamserver]

    count = var.install_redelk ? 1 : 0 # only run if redelk=true

    connection {
        type = "ssh"
        user = var.ssh_user
        host = var.bastionhostpublicip
       private_key = var.private_key
    }

    provisioner "remote-exec" {
        inline = [
          "ansible-playbook -i inventory.ini teamserver.yml"
        ]
    }
}
```



RedInfra Framework Structure

Clients/main.tf

1

```
# havoc teamserver
module "teamserver" {
  depends_on = [module.redteambastion]

  source              = "../../modules/aws/havoc-teamserver"
  ami_id              = data.aws_ami.latest_ubuntu.id
  install_redelk      = module.redteambastion.install_redelk
  vpc_id              = module.redteamvpc.vpc_id
  subnet_id           = module.redteamvpc.subnet2_id // private subnet
  avl_zone            = var.avl_zone
  key_name            = aws_key_pair.generated_key.key_name
  private_key         = tls_private_key.terra_sshkey.private_key_pem
  bastionhostprivateip = module.redteambastion.bastion-private-ip // for whitelisting
  bastionhostpublicip  = module.redteambastion.bastion-public-ip
  ssh_user            = var.ssh_user
  multiple_infra_users = true
  // Specify teamserver users below, it can be as many as you want
  teamserver_users = {
    "dazzy"   = "h4ck3r",
    "k3n"     = "[redacted]",
    "h4zm4tt" = "[redacted]!"
  }
  project_tags = var.project_tags
  environment  = "Live" // This argument takes either "Testing" or "Live". Testing envir
}
```

modules/main.tf

2

```
resource "aws_instance" "havoc-teamserver" {
    ami = var.ami_id
    instance_type = local.instance_type
    subnet_id = var.subnet_id
    vpc_security_group_ids = [aws_security_group.havoc-teamserver-sg.id]
    availability_zone = var.avl_zone
    key_name = var.key_name

    root_block_device {
        volume_type = "gp2"
        volume_size = local.root_volume_size
    }
}
```

playbook.yml

3

```
---
- name: Setup Havoc Environment
  hosts: all
  become: yes
  vars:
    project_directory: /opt/Havoc
  tasks:
  - name: Update apt packages
    apt:
      update_cache: yes

  - name: Install below programs
    apt:
        name: "{{ item }}"
        state: present
    with_items:
          - golang
          - unzip
          - tmux
          - net-tools
          - build-essential

  - name: Clone Havoc repository
    ansible.builtin.git:
      repo: 'https://github.com/HavocFramework/Havoc.git'
      dest: "{{ project_directory }}"
      clone: yes
      update: yes
      version: dev

  - name: Add deadsnakes PPA
    ansible.builtin.apt_repository:
      repo: 'ppa:deadsnakes/ppa'
      state: present
      update_cache: yes
```

GitHub Workflows

Automate CI/CD Pipeline in Github

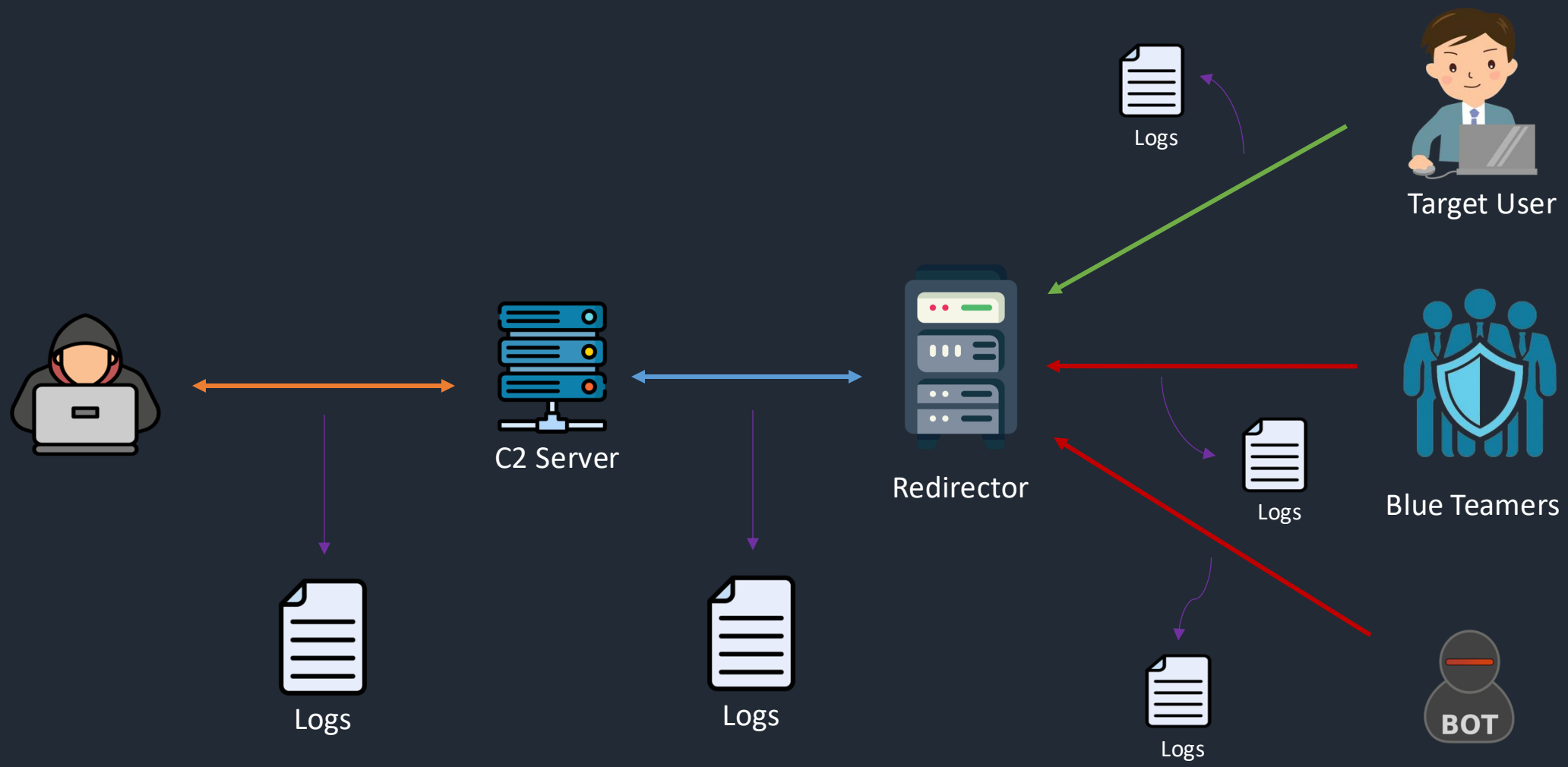
Triggered by events like push, pull requests, or scheduled times

Defined by YAML files in the .github/workflows directory

```yaml
name: Update on Pull Request

on:
  pull_request:
    branches:
      - main
jobs:
  update-third-party-content:
    runs-on: ubuntu-latest

    steps:
    - name: Checkout our repository
      uses: actions/checkout@v3

    - name: Clone third-party repository
      run: |
        git clone https://github.com/external/repo.git myrepo

    - name: Make changes in the third-party repository
      run: |
        echo “Updated” >> myrepo/important-file.txt

    - name: Commit and push to our repository
      run: |
        git config user.name "Your GitHub Username"
        git config user.email "your.email@example.com"
        git add ./external-updates/
        git commit -m "Updated with latest changes"
        git push origin HEAD:main
```

```
steps:
- name: Checkout repository
  uses: actions/checkout@v2
  with:
    token: ${{ secrets.ACCESSTOKEN }}

- name: Remove and Update evilginx2
  run: |
    if [ -d evilginx2 ]; then rm -Rf evilginx2; fi
    git clone https://github.com/kgretzky/evilginx2
    if [ -d "evilginx2/.git" ]; then rm -Rf "evilginx2/.git"; fi
    if [ -d "evilginx2/.github" ]; then rm -Rf "evilginx2/.github"; fi

- name: Remove specific the evilGinx Header
  run: |
    sed -i 's/req.Header.Set(p.getHomeDir(), o_host)/\/\/req.Header.Set(p.getHomeDir(), o_host)/' evilginx2/core/http_proxy
    sed -i 's/o_host := req.Host/\/\/o_host := req.Host/' evilginx2/core/http_proxy.go
    # sed -i 's/SetHttpsPort(443)/SetHttpsPort(8443)/' evilginx2/core/config.go
    # UComment the above line if you are using an Apache instance to protect the EvilGinx instance (like the EvilGoPhish se


- name: Update http_proxy.go for X-Forwarded-For support
  run: |
    sed -i '/remote_addr := parts\[0\]/a \ \ \ \ xForwardedFor := req.Header.Get("X-Forwarded-For")\n \ \ \ \ if xForwarded

- name: Push changes
  run: |
    git config --global user.name '<USERNAME>'
    git config --global user.email '<EMAIL>'
    git add .
    git add evilginx2
    git commit -m "Updated EvilGinx"
    git push
```

Logs Everywhere



The Logs Which Are Everywhere

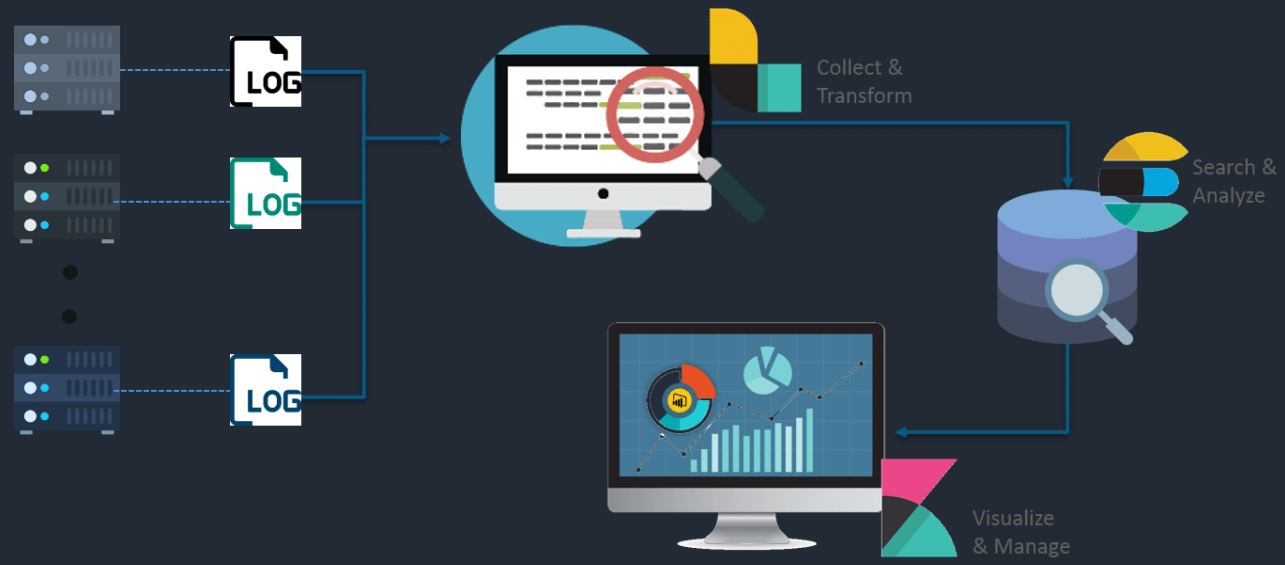
```
ubuntu@httpredir1:~$ cat /var/log/apache2/access-redelk.log
[02/Apr/2024:16:03:52 +0000] - apache[2946]: frontend:-/10.0.1.222:80 backend:decoy-amazon client:101.0.63.209:1765
1 xforwardedfor:- headers:{Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0|34.
207.82.92|-|-|-|-|-|} statuscode:302 request:GET / HTTP/1.1
[02/Apr/2024:16:04:01 +0000] - apache[2947]: frontend:-/10.0.1.222:80 backend:decoy-amazon client:101.0.63.209:1756
6 xforwardedfor:- headers:{Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0|34.
207.82.92|-|-|-|-|-|} statuscode:302 request:GET /google/abc HTTP/1.1
[02/Apr/2024:16:04:12 +0000] - apache[2946]: frontend:-/10.0.1.222:80 backend:decoy-amazon client:101.0.63.209:1763
7 xforwardedfor:- headers:{Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0|34.
207.82.92|-|-|-|-|-|} statuscode:302 request:GET /google/aslsl HTTP/1.1
[02/Apr/2024:16:10:02 +0000] HOSTNAME apache[2946]: frontend:www-http/10.0.1.222:80 backend:c2 client:101.0.63.209:
17726 xforwardedfor:- headers:{Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0
|34.207.82.92|-|-|-|-|-|} statuscode:503 request:GET /ramukaka/abc HTTP/1.1
[02/Apr/2024:16:10:03 +0000] - apache[2947]: frontend:-/10.0.1.222:80 backend:decoy-amazon client:101.0.63.209:1753
1 xforwardedfor:- headers:{Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0|34.
207.82.92|-|-|-|-|-|} statuscode:302 request:GET /favicon.ico HTTP/1.1
[02/Apr/2024:16:12:07 +0000] - apache[2947]: frontend:-/10.0.1.222:80 backend:decoy-amazon client:82.32.97.79:48794
 xforwardedfor:- headers:{-|34.207.82.92|-|-|-|-|-|} statuscode:302 request:GET / HTTP/1.1
ubuntu@httpredir1:~$
```

```
06/19 14:04:54 [metadata] beacon_28131 -> 172.16.20.80; computer: GRANITE; user: raffi; pid: 5332; version: 6.1
06/19 14:04:53 [output]
established link to parent beacon: 172.16.20.80

06/19 14:04:56 [input] <neo3> ps
06/19 14:04:56 [task] Tasked beacon to list processes
06/19 14:04:57 [checkin] host called home, sent: 12 bytes
06/19 14:04:57 [output]
[System Process]        0       0
System  0       4
smss.exe        4       312
csrss.exe       396     420
wininit.exe     396     516
csrss.exe       508     528
winlogon.exe    508     592
services.exe    516     616
lsass.exe       516     648
lsm.exe 516     656
svchost.exe     616     764
```

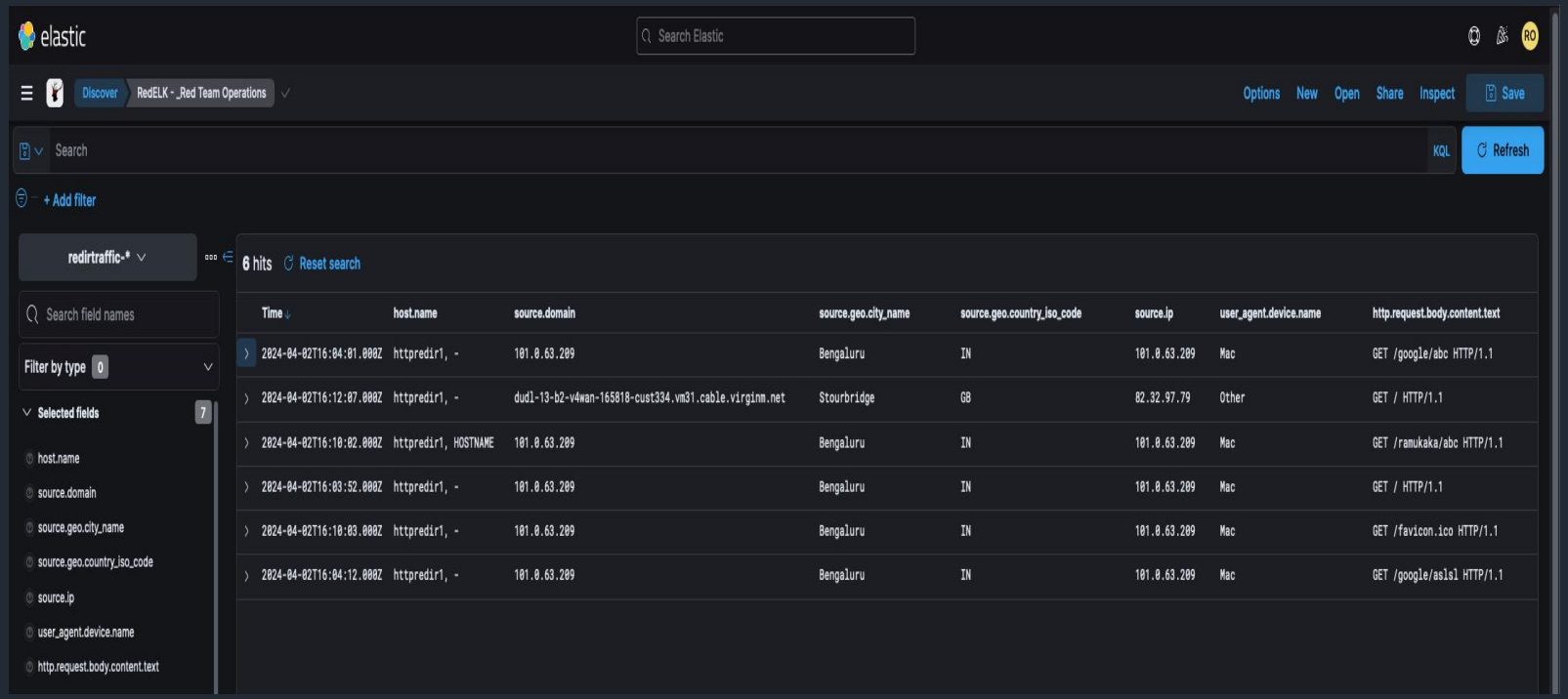
ELK Stack

ELK Stack is a collection three open-source products; Elasticsearch, Logstash and Kibana

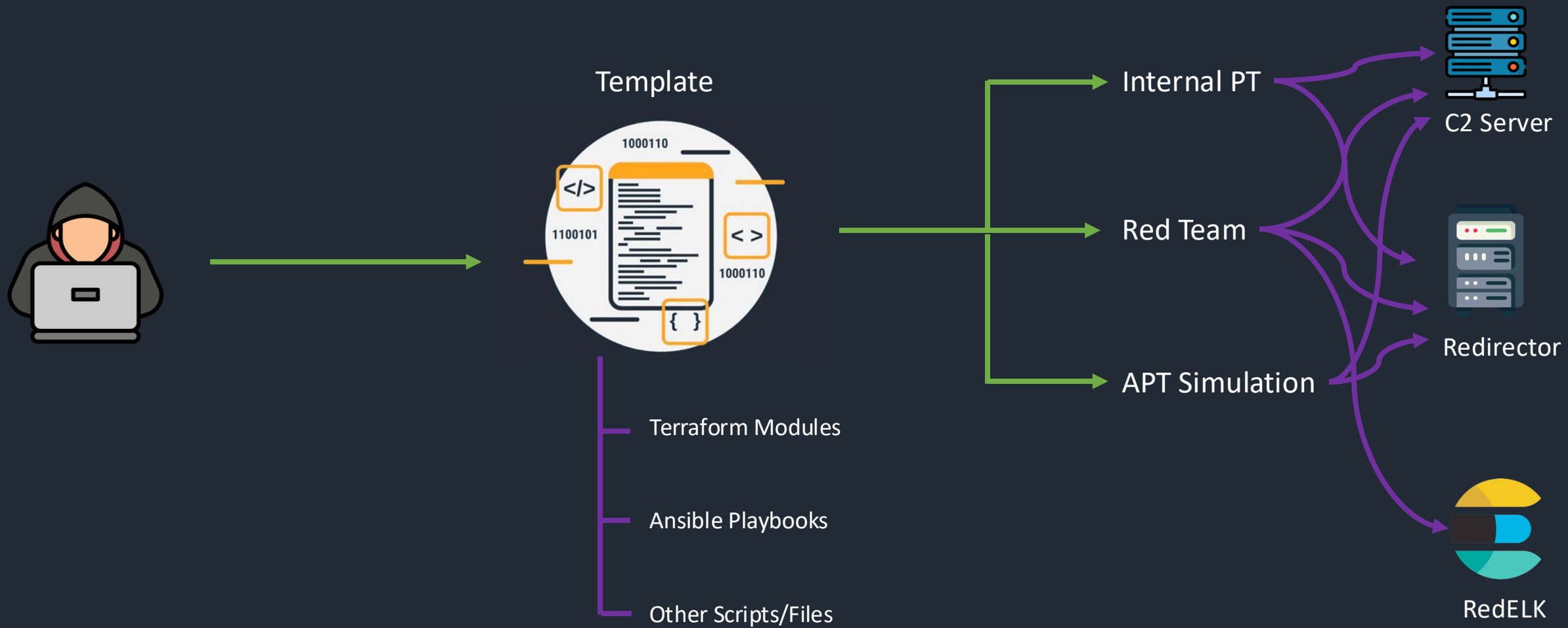
Elasticsearch: Store, Search and Analyse
Logstash: Collect logs and events data, Parse and Transform
Kibana: Explore, Visualize and Share
Beats: Data Shipper



Logging with RedELK



Template Based Infra Provisioning



Thank You

Any Questions or Feedback?