Attack Infrastructure for the Modern Red Team

@TTimzen

@r00tkillah

Who Are We?

Michael “@r00tkillah” Leibowitz

NSA Playset

Principle Infra Monkey

Topher Timzen (@TTimzen)

C# Malware is <3

Also a Principle Infra Monkey

RED TEAM ! ! !

Agenda

- What is a Red Team
- Requirements for Red Team Infrastructure
- Deep dive of Infrastructure
- DEMO, DEMO, DEMO, DEMO
- Show me the source, Luke!
- Future Work
- Closing

Introduction to Red Teaming

Alternative Analysis & Threat Emulation/Attack Modeling

Acts as a sparring partner for your defensive teams, commonly referred to as blue, to increase their efficacy.

Operation types include: Overt, Covert, and Clandestine

Why Infrastructure Tho?

Roll early, roll often

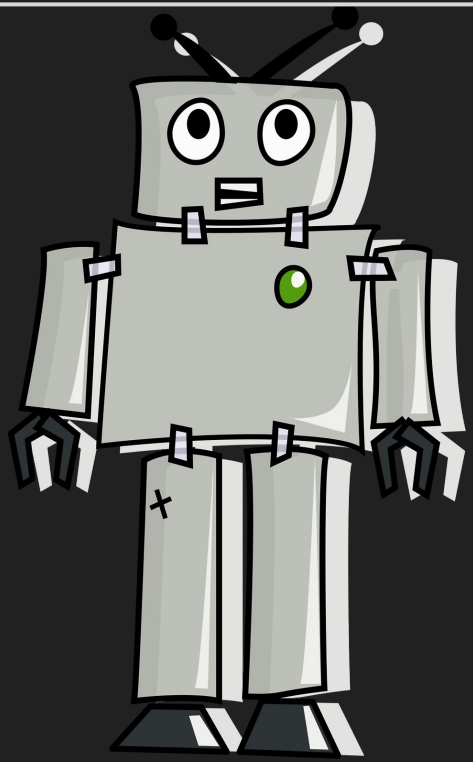
DFIU

#OPSEC

https://commons.wikimedia.org/wiki/File:M3_Stuart_Light_Tank_bogged_down_on_Makin_Island.jpg

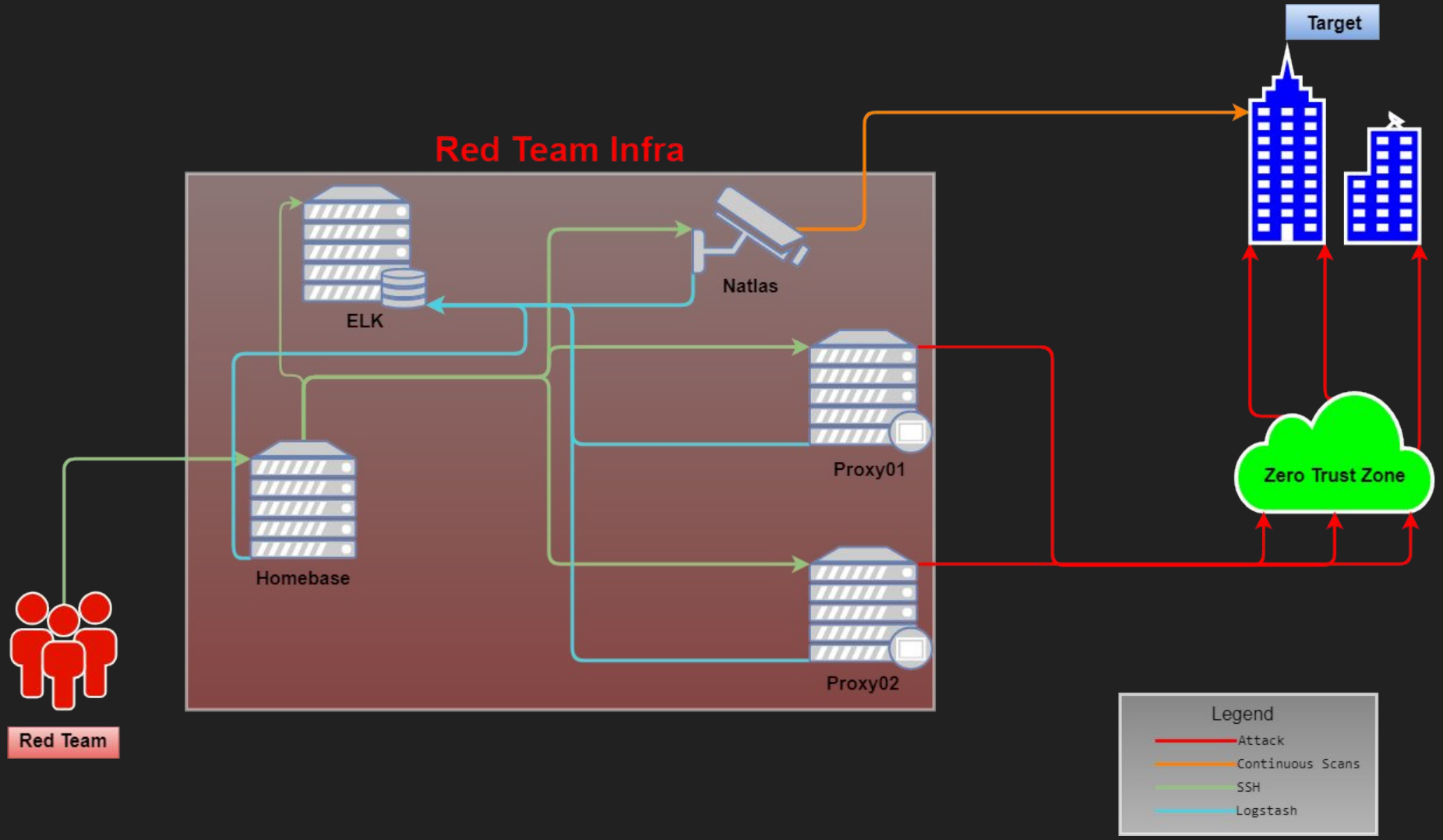
Requirements of Attack Infrastructure

- Secure
- Repeatable
- Self Contained
- Modular
- Flexible
- Automated
- Auditable
- #OPSEC Throughout



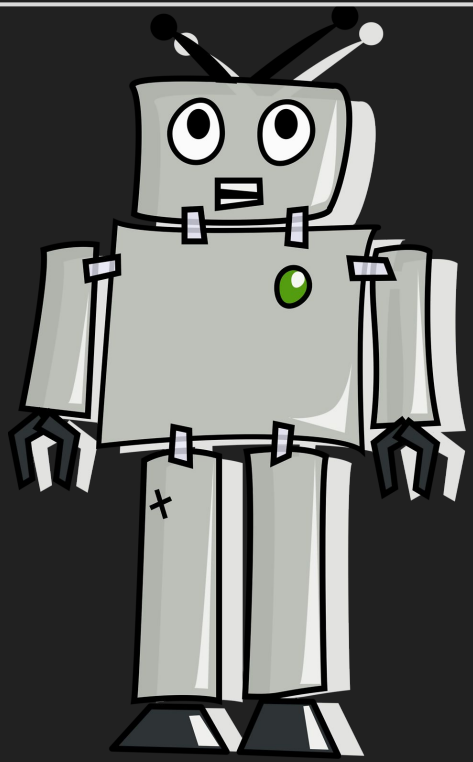
http://res.freestockphotos.biz/pictures/16/16861-illustration-of-a-grey-cartoon-robot-pv.png

Infrastructure Deep Dive


Target
Red Team Infra
ELK
Natlas
Proxy01
Homebase
Proxy02
Zero Trust Zone
Red Team
Legend
Attack
Continuous Scans
SSH
Logstash

Requirements of Attack Infrastructure

- Secure
- Repeatable
- Self Contained
- Modular
- Flexible
- Automated
- Auditable
- #OPSEC Throughout



http://res.freestockphotos.biz/pictures/16/16861-illustration-of-a-grey-cartoon-robot-pv.png

Network Fabric Security

SSH to homebase only through corp OUTBOUND IP

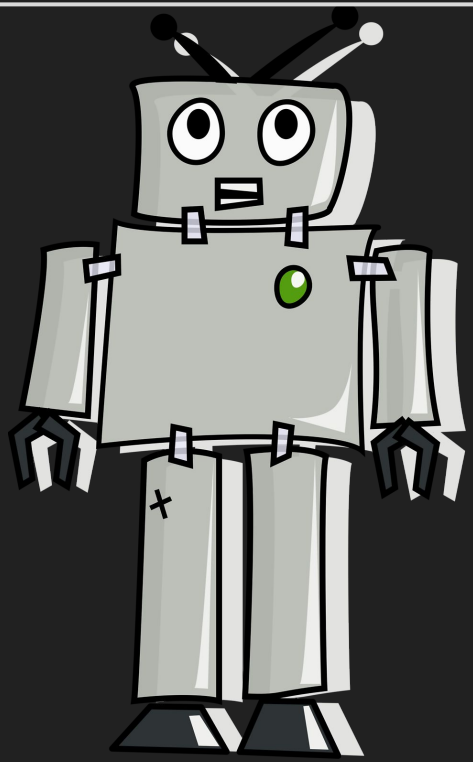
Proxies for inbound C2

- HTTP
- HTTPS
- SSH (if needed, not by default)
- DNS (if needed, not by default)
- 4444 / 2222 (if needed, not by default)

Open Internal fabric routes everything

Requirements of Attack Infrastructure

- Secure
- Repeatable
- Self Contained
- Modular
- Flexible
- Automated
- Auditable
- #OPSEC Throughout



http://res.freestockphotos.biz/pictures/16/16861-illustration-of-a-grey-cartoon-robot-pv.png

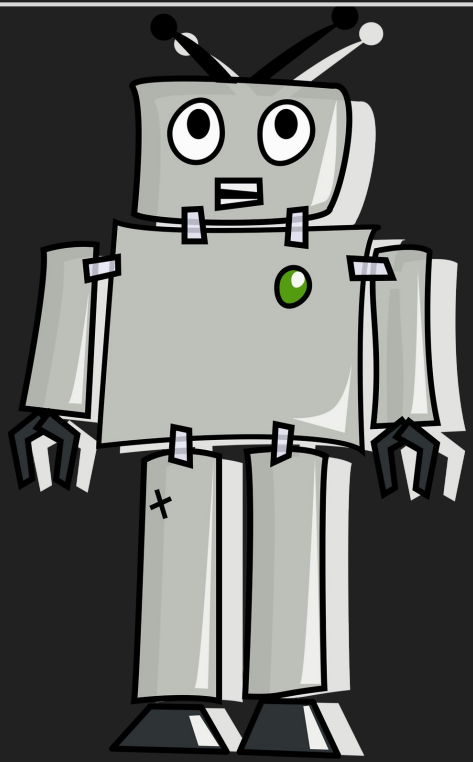
Repeatable

Variety of tooling used

- Terraform
- Vagrant
- Puppet
- Lots of git-fu

Requirements of Attack Infrastructure

- Secure
- Repeatable
- Self Contained
- Modular
- Flexible
- Automated
- Auditable
- #OPSEC Throughout



http://res.freestockphotos.biz/pictures/16/16861-illustration-of-a-grey-cartoon-robot-pv.png

Self-Contained Access Control

Red Team-SSH repo and SSH keypairs

Role based access control via tags

- Redteam
- Infra
- Core
- Volunteer

Example json

```
{
    "users" : [
        {
            "uid" : 6001,
            "name" : "Some Name 1",
            "username" : "somename1",
            "authorized_keys" : "BASE64 GARBAGE",
                "shell" : "/bin/bash",
                "tags" : [
            "volunteer" ,
            "redteam"
        ],
        },
        {
            "uid" : 6002,
            "name" : "Some Name 2",
            "username" : "somename2",
            "authorized_keys" : "BASE64 GARBAGE"
                "shell" : "/bin/bash",
                "tags" : [
            "core",
            "redteam"
       ]
        }
}
```

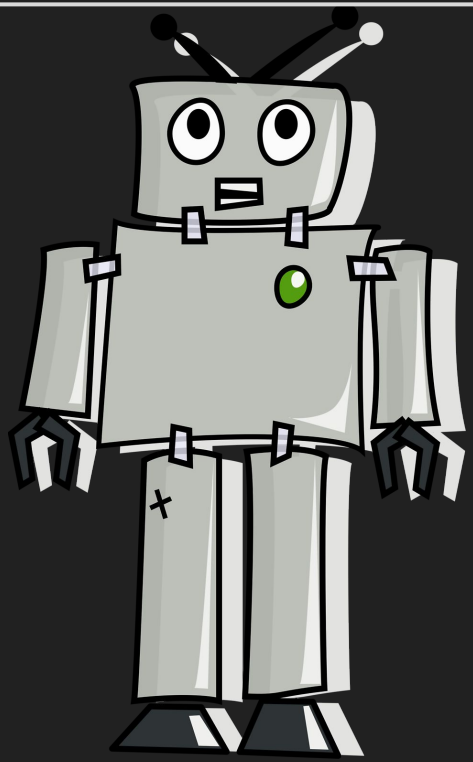
https://github.com/redteaminfra/redteam-ssh

SSH Configuration #OPSEC

```
Host homebase-#{vpcname}
     #{hostname}
     #{proxycommand}
     User <SSH_USER>
     IdentityFile ~/.ssh/id_rsa
     #Uncomment AddressFamily if you have WSL errors to force ipv4
     #AddressFamily inet
     LocalForward 50050 127.0.0.1:50050
     LocalForward 5000 #{subnet}.14:80
     LocalForward 9001 127.0.0.1:9001
     ##Change 59xx to your VNC Port and uncomment this forward. Your UID is found in sshKeys users.json
     #Your port number is (5900 + (UID - 6000) + 1)
     #LocalForward 5901 127.0.0.1:59xx

Host proxy01-#{vpcname}
     Proxycommand ssh homebase-#{vpcname} nc -q0 %h.infra.us %p
     User <SSH_USER>

Host proxy02-#{vpcname}
     Proxycommand ssh homebase-#{vpcname} nc -q0 %h.infra.us %p
     User <SSH_USER>

Host elk-#{vpcname}
     Proxycommand ssh homebase-#{vpcname} nc -q0 %h.infra.us %p
     User <SSH_USER>
     LocalForward 5601 #{subnet}.13:5601
```

Requirements of Attack Infrastructure

- Secure
- Repeatable
- Self Contained
- Modular
- Flexible
- Automated
- Auditable
- #OPSEC Throughout



http://res.freestockphotos.biz/pictures/16/16861-illustration-of-a-grey-cartoon-robot-pv.png

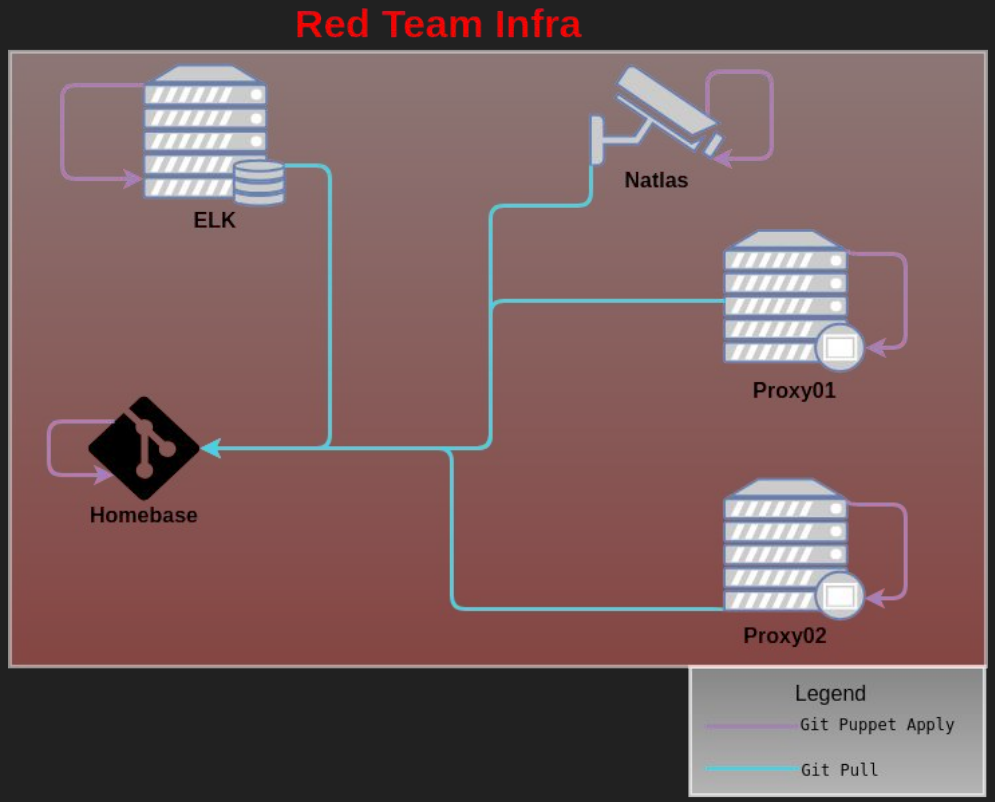
Modular, Flexible, Buzzwordable

A suite of Puppet Modules are provided that you can plug-and-play in your instance deployments!

```
{ modules } master > ls
backflips      gitpuppet           hostsexternal    loot          natlasserver  tinyproxy
cobaltstrike   gitserver           hostsinternal    modrewrite    nmap          touch
dante          homebasetools       hostsinternalhb  mollyguard    opsec         unattendedupgrades
elk            homebasetoolsubuntu irc              monitoring    proxytools    volunteerssh
etherpad       hosts               logstashconfig   natlasagent   ssh           yama
```

https://github.com/redteaminfra/redteam-infra/tree/master/puppet

Replicated Masterless Puppet #OPSEC



Cobalt Strike

Windows shop heavy, but provisions everything you need to host a teamserver!

Supported by proxies with the mod_rewrite module, you can quickly spin up engagements and testing playgrounds!

Cobalt Strike with mod_rewrite

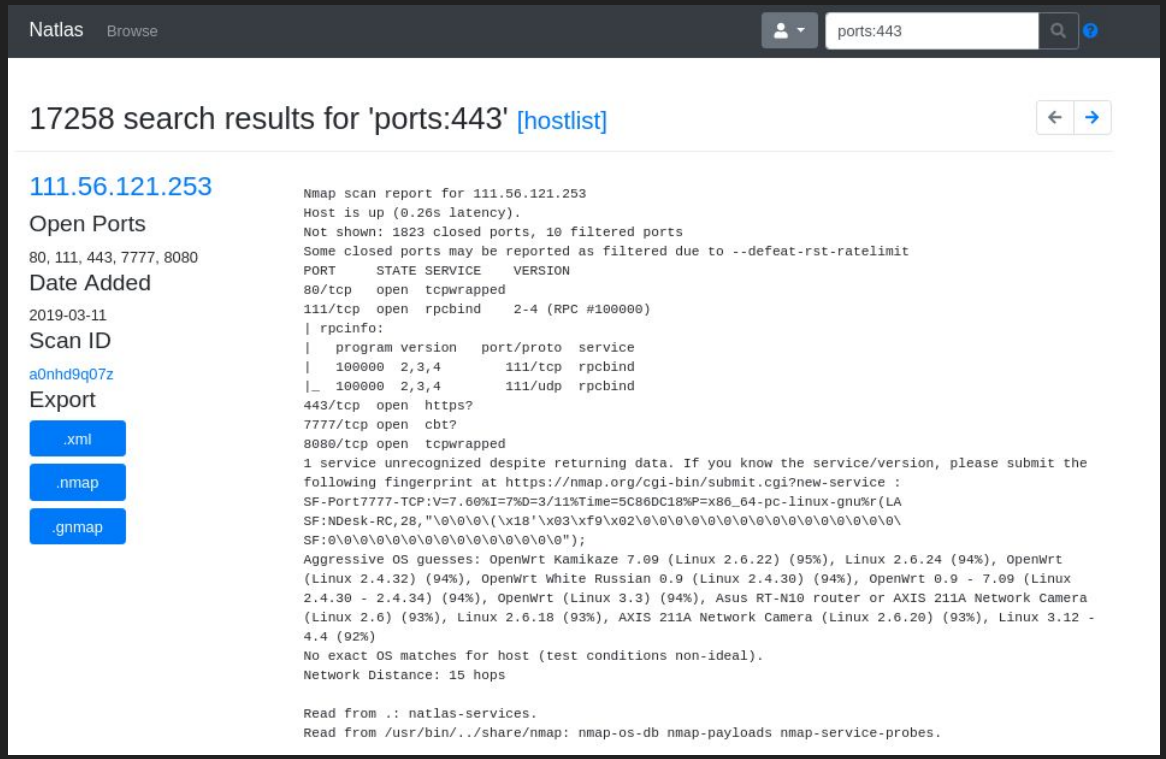
```
RewriteEngine On

# Stageless
RewriteCond %{HTTP_USER_AGENT} Mozilla\/5\.0\ \(Windows\ NT\ 6\.1\;\ WOW64\;\ Trident\/7\.0\;\ rv\:11\.0\)\ like\ Gecko [NC]
RewriteCond %{REQUEST_URI} (/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=book|/N4215/adj/amzn.us.sr.ap) [NC]
RewriteRule ^.*$ %{REQUEST_SCHEME}://192.168.1.10%{REQUEST_URI} [P]

# Staged
RewriteCond %{REQUEST_URI} (/get32.gif|/get64.gif) [NC]
RewriteCond %{HTTP_COOKIE}     !its=me; [NC]
RewriteRule ^.*$ %{REQUEST_SCHEME}://192.168.1.10%{REQUEST_URI} [P]

RewriteRule / /index.html [L,R=302]
```

https://github.com/redteaminfra/redteam-infra/tree/master/puppet/modules/modrewrite

Others C2s?

Easy to add via Pull Request!

Natlas



https://github.com/natlas/natlas

Natlas Deployment

Automated as two puppet modules

- Natlasagent
- Natlasserver

#OPSEC Throughout

No C2 on the internet freely available!

Strong OUTBOUND and INBOUND restrictions on homebase

No TLS termination in Zero Trust Zones

#OPSEC

No team server on the internet

Code | Pull requests 0 | Insights

Branch: master ▾ **cobaltstrike-extraneous-space / cobaltstrike-servers.csv** Find file | Copy path

fox-srt Update list with http dataset from 2014 830ace8 7 days ago

1 contributor

9370 lines (9369 sloc) | 373 KB Raw | Blame | History

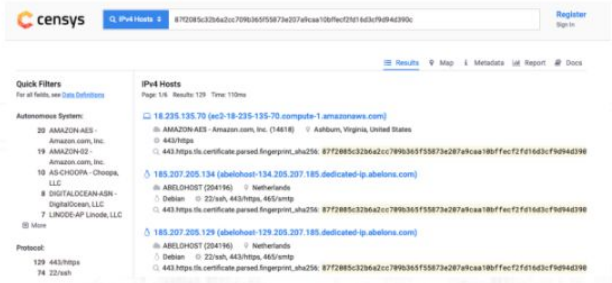
Search this file…

	ip	port	first_seen	last_seen
2	1.122.234.70	443	2017-06-20	2017-06-20
3	1.122.64.110	443	2017-01-17	2017-01-17
4	100.2.202.125	80	2016-04-26	2016-05-10
5	100.25.185.145	443	2019-02-12	2019-02-12
6	100.25.217.29	443	2018-11-20	2019-01-01
7	100.3.129.148	80	2016-03-29	2017-06-05
8	100.7.3.44	80	2016-12-20	2016-12-20
9	100.7.3.45	443	2016-11-29	2016-12-27

How did you find these team servers?

Here are the common techniques to identify Cobalt Strike team servers on the internet:

1) The Cobalt Strike product ships with a default SSL certificate for HTTPS communication. This self-signed certificate has no place in a live operation, but it's still used in many Cobalt Strike deployments. One technique to find Cobalt Strike Beacon controllers is to search for the SHA-256 hash of Cobalt Strike's default certificates:



2) Cobalt Strike's DNS server (when it's enabled) will respond to any request it receives with the bogon IP 0.0.0.0. A search for DNS servers that respond to an arbitrary DNS request with this answer will find Cobalt Strike systems. It will also find non-Cobalt Strike systems as well. It's a noisy indicator.

3) Search for systems with port 50050 open. This is the controller for Cobalt Strike's team server.

4) Another technique is to look for 404 Not Found root page with empty content and a text/plain Content-Type. This is the default response of Cobalt Strike without a redirector or content explicitly hosted at /.

- https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild/
- https://blog.cobaltstrike.com/2019/02/19/cobalt-strike-team-server-population-study/
- https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967

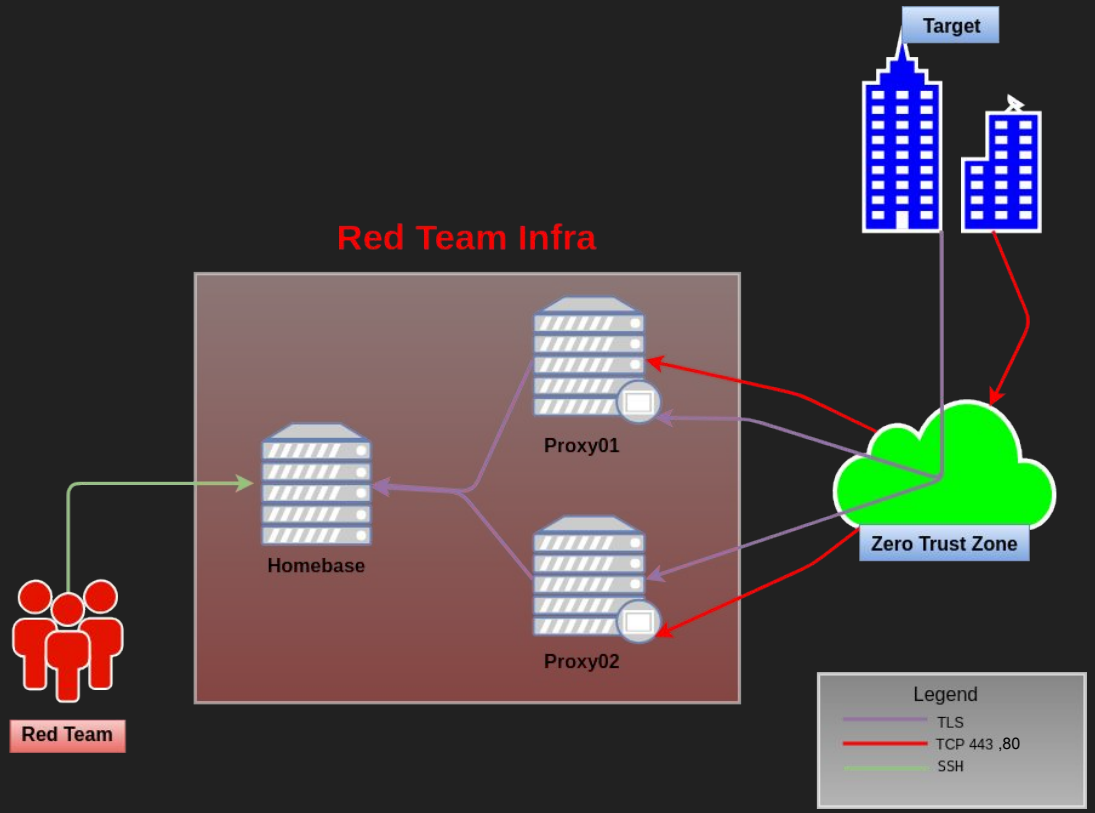
Zero Trust Zones

Assume breach of all hosts used outside of Red Team Infra

External/sketch provides a very simple set of provision scripts for zero-trust reflector proxies.

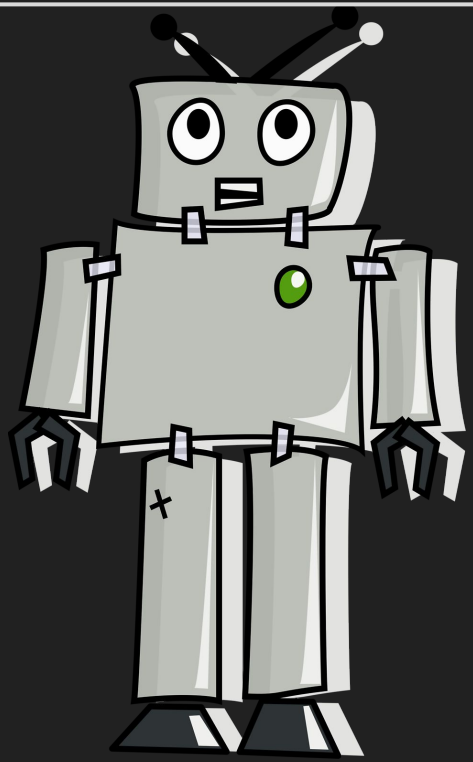
```
ssh user@sketch bash -c “echo <BASE64 GARBAGE>|base64 -d|bash”
```

TLS Termination



Requirements of Attack Infrastructure

- Secure
- Repeatable
- Self Contained
- Modular
- Flexible
- Automated
- Auditable
- #OPSEC Throughout



http://res.freestockphotos.biz/pictures/16/16861-illustration-of-a-grey-cartoon-robot-pv.png

Auditable via Telemetry

All done via the ELK instance

- All boxes send telemetry data to it via logstash

Several opsec safe alerts are present in the monitoring module

- C2Dead
- C2Compromised

Agility

> be me

> blueteam finds C2 domain

> oh$#!!.gif

> need to roll to new C2

> go go go

MFW tested in staging and rolled to prod in 15m

This My Life Now

1. Terraform apply
2. hack; hack; hack
3. git add; git commit
4. git push homebase-xxx:/var/lib/git/infra
5. ????
6. git push origin master
7. Profit!!


Demo
TIME

Open Source

https://github.com/redteaminfra

https://github.com/redteaminfra/redteam-infra

https://github.com/redteaminfra/redteam-ssh

https://github.com/redteaminfra/redteam-infra/issues

https://github.com/redteaminfra

Training and How To ! ? ! ?

There are training docs in the repo and hopefully enough README.md's!

https://github.com/redteaminfra/redteam-infra/tree/master/documentation

Future Work

We want to support all the Clouds!

Closing some issues with puppet deployment

Closing more issues

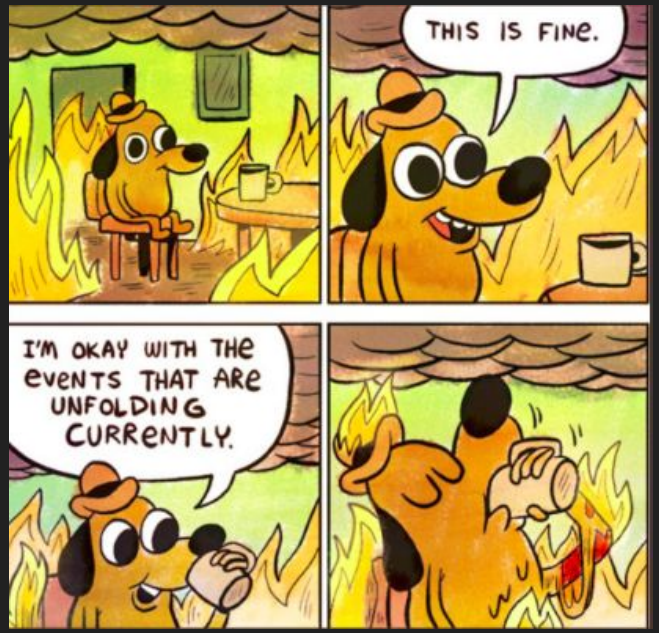
And more issues

Issues

Blog Post incoming ! ! ! !

Closing Remarks

Learn it, love it, live it.



Thank Yous and References

dade for supporting https://github.com/natlas/natlas

Toby Kohlenberg for helping us to define original architecture goals and Red Teaming

- Red teaming probably isn't for you - https://www.youtube.com/watch?v=P4zIUQQo6Hg

Adam Luvshis for the Aggressor scripts

Chris Hawke for monitoring with elastalert

All the people we asked questions and yap yap'd with about infra

Our staring point - https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki

EOF