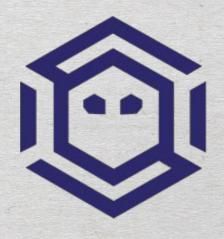




whoami

Jeff Dimmock (@bluscreenofjeff)

- Adversary Simulation Lead at SpecterOps
 - Adaptive Threat Division alumni
 - Avid blogger (<u>https://bluescreenofjeff.com/</u>)
 - Writes some Aggressor scripts
- Speaker at BSides NoVA 2017 and HackMiami
- Participated in Pacific Rim CCDC since 2014
- Maintains the Red Team Infrastructure Wiki w/ @424f424f
 (http://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki)



it was the description with the second of th

bsoj.co/ArcticCon2017

I Take Haralbush la ye another while a middle lake when in the resort is he folds

Agenda

- Introduction
- Design Considerations
 - General
 - Domains
 - Payloads
 - C2
 - SMTP
- Example Infrastructure Designs

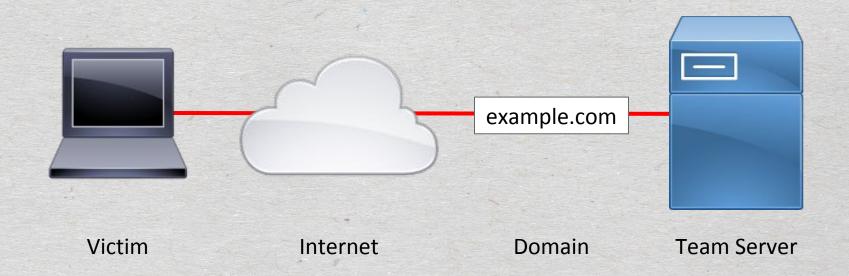
It was the way of the way the will me to be the way the was to be with a

Key Takeaways

Phat is a Covert Red Ceam Attack Infrastructure?

it had Hard bush to you make with me with the what is in a good to he fold a

Standard Pentest Setup



went the 1 well broken to be a consider while on the better better to the to he to h

Covert Red Team Attack Infrastructure domain1.com domain2.com domain3.com domain4.com Redirectors Victim **Domains** Internet **Team Servers**

with the Hand bush to be and condition with the extent in the reserve to he with a

Benefits of a Covert Infrastructure

- Blends in with non-malicious infrastructure
- Builds in defenses against Blue team
- Resilience when an asset is blocked
- Flexibility to adapt as the test progresses

it here I will be in the to you will consider a the bull a be a Very in to see to her to

Pesign Considerations

mit six i mallow the recomble when substituted where into resort hurches

Design Considerations - General

- Segregate all assets based on function
- Place a redirector in front of every asset
- Blend in with normal traffic for the target
- Configure assets in a way that individual pieces can be rolled

it like Handlen skie va andle gellen buddelet ale sig letter see to be

Keep the length of the test in mind when designing

Design Considerations - General

- Don't go overboard for your target
- Tailor the design for anticipated or encountered obstacles

it was I was bush to a world and the middle who be to when you

- Evaluate infrastructure primitives before choosing one
- Be fluid as the test goes; redesign as needed

(Sidenote: document EVERYTHING)

Design Considerations - Domains

- Always use categorized domains*
- Pre-categorized vs. home-grown
- Matching the target's domain categorization can help blend in

is the Hard bush to you make rubble on the which where

 Alternatively, organizations often have domain category whitelists (try Healthcare/Finance!)

*unless emulating an actor who doesn't

Design Considerations - Domains

- Domains should match planned pretext
- Good choices:
 - Impersonate target company
 - Similar to popular companies/services (Google, Microsoft, etc.)*

it was I was bush to a world and the middle who be to when you

Generalized domains that match industry

*There are precedents for companies coming after squatters

Design Considerations - Payloads

- Payload type
 - HTA, LNK, PowerShell download cradle, etc
- Delivery method (attached, web-based)
 - Attachment
 - Download link (server vs. cloud storage)

it was transfer the recommended and the with the way in the second to her to

- Access control options
 - IP/fingerprint-based restrictions
 - Expiring payload links

Design Considerations - Payload Redirection

- "Dumb pipe"
 - socat/iptables
 - Forwards all connections
 - No monitoring of requests
- Filtering
 - Apache mod_rewrite, nginx
 - Perform conditional processing on requests

it had found bush to ve an after whiten the ball at the price is good to her to

Modify rulesets on the fly

it had blood bush to be and when the believe you with a sea to he will

- Longhaul
 - Used to regain access
 - Persistence
 - Slow check-ins
- Shorthaul
 - Used for primary operating
 - Burned frequently
 - Faster check-ins
- Number of servers

it isk imal bush to be an all withing with the exercise to be 16 hours

- Popular protocol choices:
 - HTTP(S)
 - DNS
 - Domain Fronting (over HTTPS)
 - Third-party

Attribute	HTTP(S)	DNS	Domain Fronting	Third-Party
Latency	Low	High	Medium	Medium
Likelihood to Work	Average	High	High	High
Detectability	Average	High	Low	Low
Ease of Blocking	Average	Low	Low	Low
Ease of Setup	Easiest	Easy	Medium	Medium/Hard

it are made where we will will me middle where in to do to he yet

- Traffic shaping:
 - Custom network footprint
 - Emulate a specific application or threat actor
 - Modify potential signatures (URIs, user agents, etc.)
 - Modify any host implant attributes as much as possible

Broke Hard bush to be a contitue addition the ball a Vale

Use custom profiles for each server

- Choose an appropriate protocol and redirection method per server
 - Validate latency before launching the test
- Keep servers separate
 - Shorthaul and longhaul servers fulfill different roles
 - Be disciplined with each server type
 - Never cross the streams!
- Don't be afraid to roll new infrastructure

Design Considerations - C2 Redirection

- "Dumb pipe"
 - Easiest setup, no filtering protections
- Filtering
 - Longer setup, higher resilience
- Domain Fronting/Third-Party C2
 - Requires setup or development

is note I made in the war and condition with the way with sent to he 10 h

- Blends in well
- Very hard to block

Design Considerations - SMTP

- Self-setup
 - Set up yourself
 - DKIM, SPF, PTR records needed
 - Can be time-intensive
- Third-party
 - Automatic reputation
 - Anti-spam controls
- Open Relay
 - Can use target's own server against them
 - Anti-spam controls could get you flagged

it was translation the war and condition with the war with a sand to he 11th

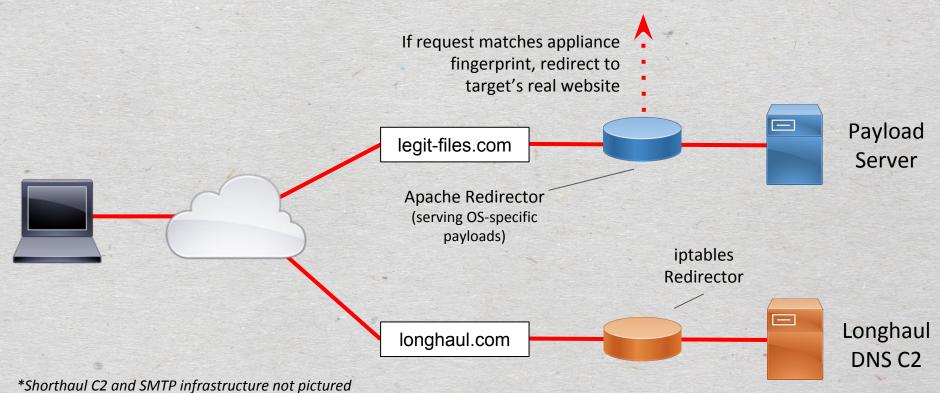
Example Infrastructure Pesigns

it is the Hand bush to we an after able on the both a very so to do to he peta.

- Email attachments blocked
- Pre-phish revealed email appliances
- Appliances crawl all links in emails
- No intel about web browsing restrictions

it here I will built to be an after while a to be the starte with the here

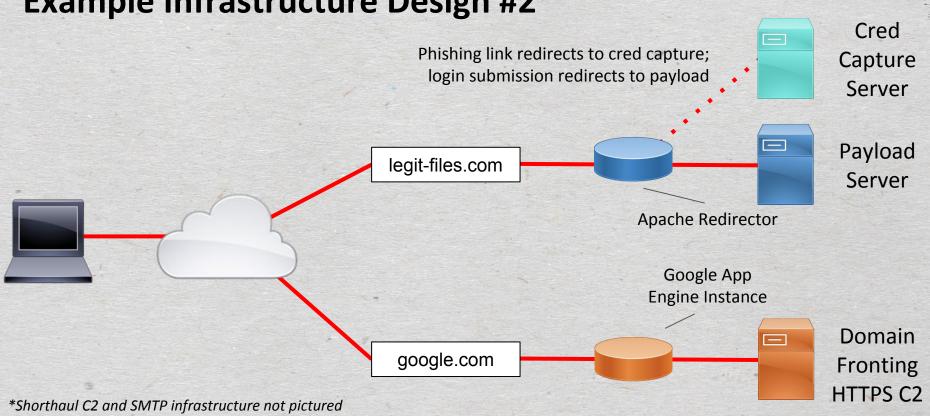
Mixed OS environment



unit tide Hardburkluss ander when with the extern in to resert he felt a

- About half of users don't have internet access
- Those with internet access are heavily restricted
- Publicly-accessible OWA and remote access logins

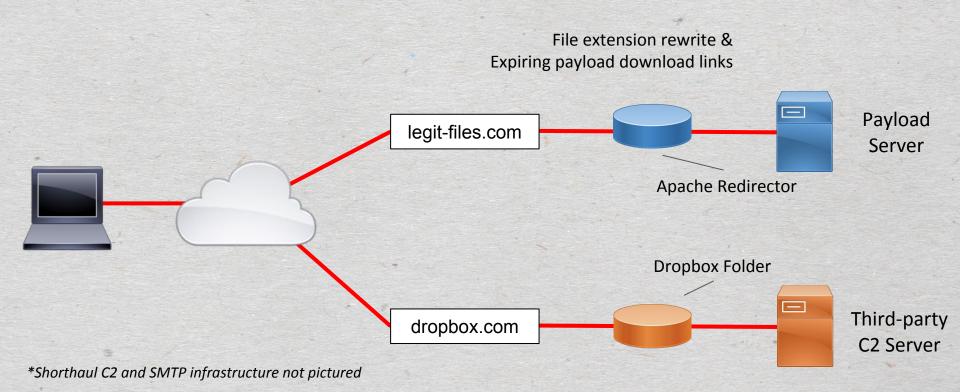
it less 11 millow the war and the relation the bath as being into ano to held



mit her I was bush to a condition with white way with sea to he with

- Email attachments blocked
- Email appliance reviews all links and blocks wide range of file extensions
 - docx allowed
- Pre-phishing was manually acted on quickly
- Found case study for the target's deployment of a popular online storage service

it was I was bush to be an afternable in the batch as being



with the Hand bush to be and condition with the extent in the reserve to he with a

Key Takeaways

- Segregate assets
- Use redirectors, ideally with filtering
- Stress test assets for operational latency
- Document EVERYTHING
- Don't go overboard achieve your objectives

it was I was been between the wilder with the ask of which was to be 16h

bsoj.co/ArcticCon2017 bit.ly/RedTeamInfrastructure



it had I mad be still you and the when me had all a very later to be to be 1/2 ha