



COMMAND & CONQUER: RED ALERT

C2 TRADECRAFT AND DESIGN CONCEPTS



IN THIS TALK

- **About me**
- **Quick intro to C2's**
- **Pentest, red team and adversary differences**
- **Some famous C2's in the wild**
- **Design Considerations**
- **Examples**
- **Demo (pre-recorded)**

ABOUT ME

- **Lee Kagan**
- **@InvokeThreatGuy**
- **RedBlack Security –Toronto**
- **Adversary systems, MS stuff, threat intel, heavy metal \m/**
- **Blog - invokethreat.actor**



QUICK INTRO TO C2 – A definition

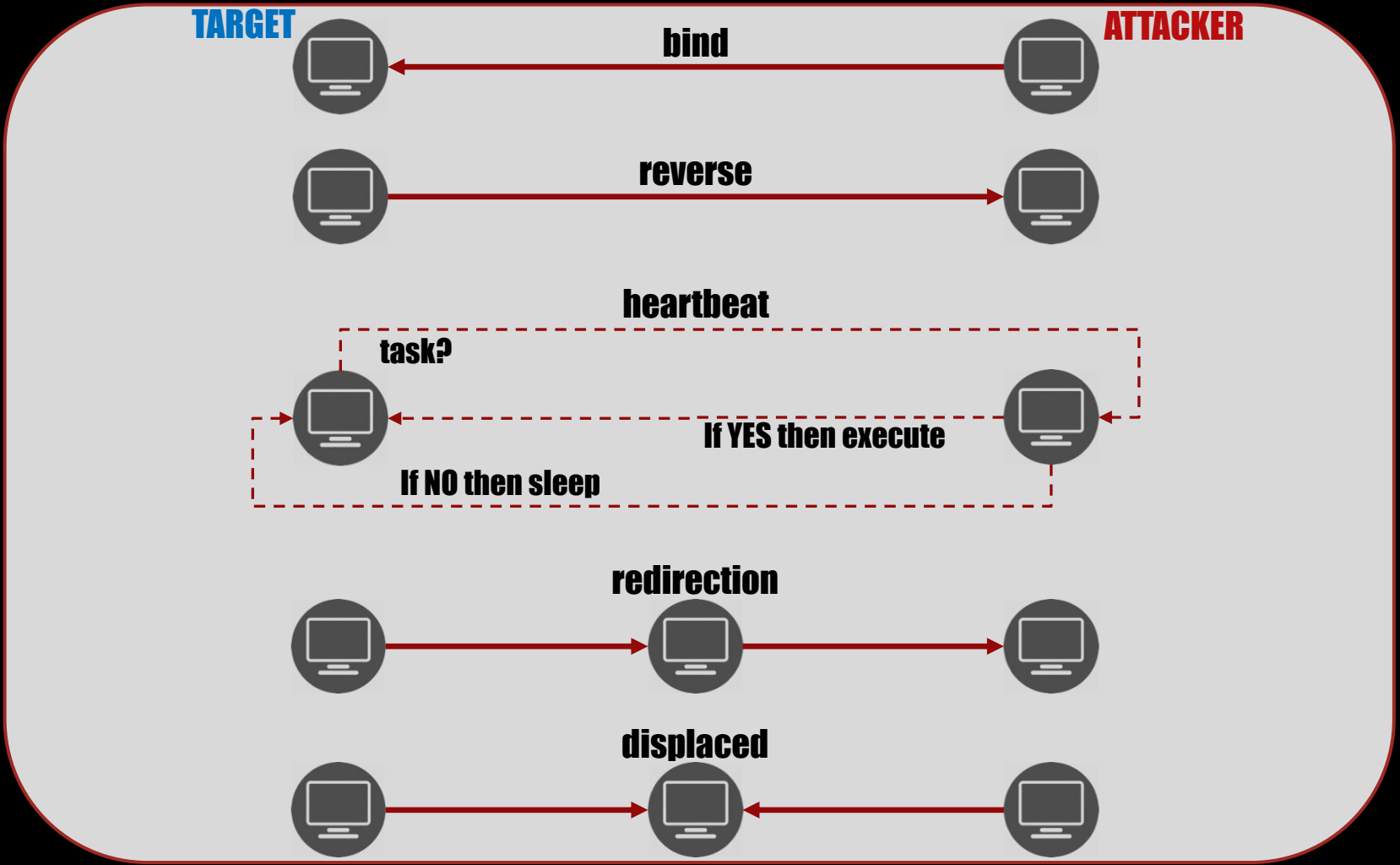
“The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Also called C2”

– <https://fas.org/irp/doddir/dod/jp1.pdf>

QUICK INTRO TO C2 - Purpose

- **Operator(s) behind the infrastructure**
- **Means to command the target**
- **Means to receive information from the target**
- **Means to distance the operator(s) from the target**
- **Means to evade, hide and thwart investigation**
- **Means to simulate and test**
- **Means to be in full control**

QUICK INTRO TO C2 – Example Connection Types



C2 Differences – Penetration Testing

- **Very low complexity**
- **Can be 1-to-1**
 - **Kali laptop attacking target directly**
- **Maybe a cloud VM or two**
 - **Kali on Digital Ocean, Burp collaborator, payload host or phishing instance**
- **Often not trying to 'appear' as anything specific**
- **Can be a single penetration tester**

C2 Differences – Threat Actors

- **Doesn't need to be fancy**
 - **More concerned with 'get the job done'**
- **Black market access**
 - **Why build when you can rent**
- **Compromise hosts all over the place**
 - **Why rent when you can pwn**
 - **Weaponize the newest exploits and vulnerabilities**
- **Size and scale**
 - **Great force multiplier**

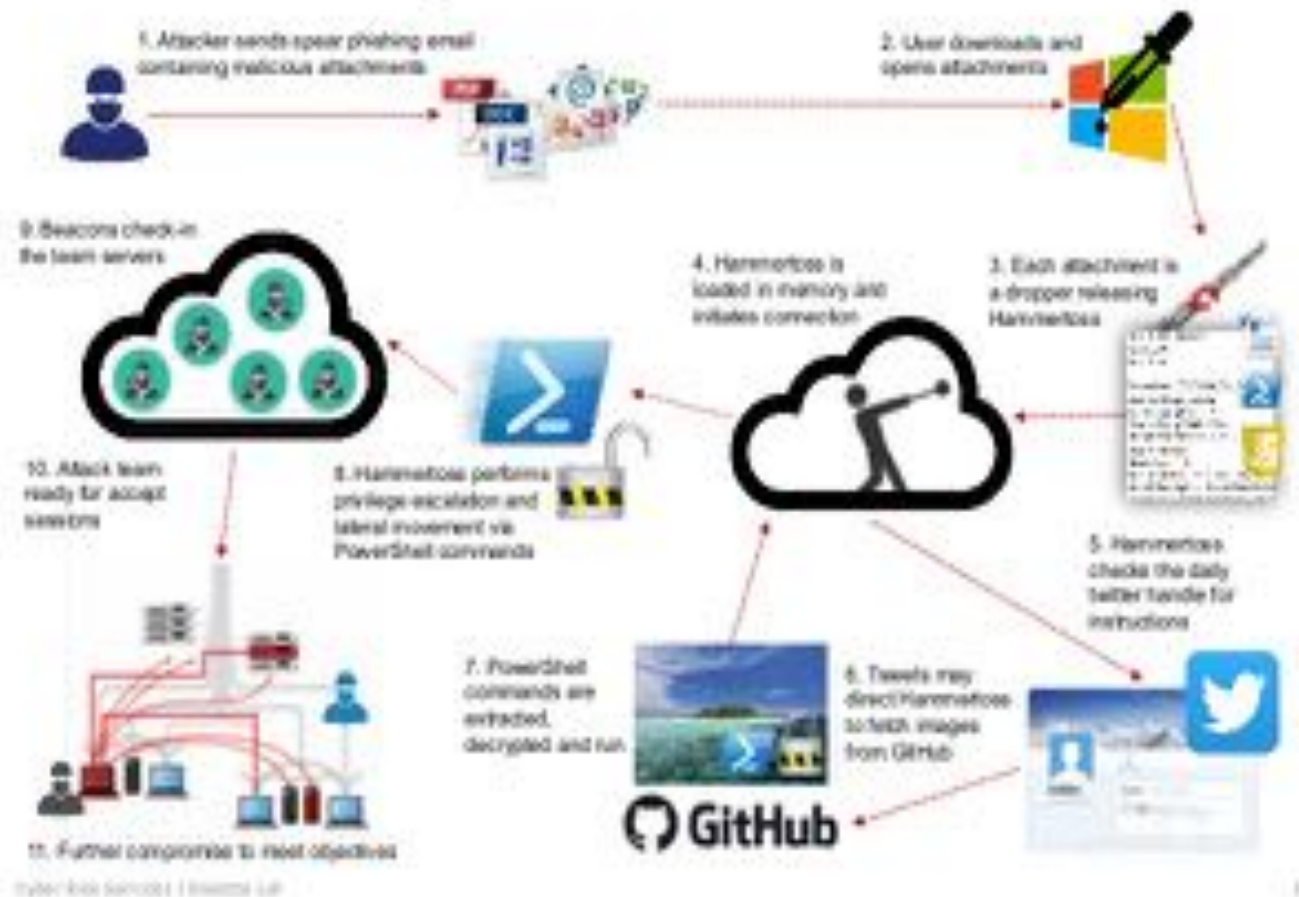
C2 Differences – Red Team

- **Can be the most complex of all**
- **Many operators using the infrastructure**
 - **Often broken down into teams or 'cells'**
- **Defensive controls and security**
 - **There's a blue team trying to knock you down**
- **Logging of everything is critical**
- **Simulating 'something'**

FAMOUS C2 – The Dukes / APT29

- Starts with good ol' phishing
- Attachment drops HAMMERTOSS
- HAMMERTOSS loads in memory
- Leverages 3rd party services
 - Twitter
 - Github
- Daily tweet containing next stage instructions
- Get a picture from Github (stego)
- Decrypt the payload in the picture
- Leverage PowerShell to privesc and move laterally
- Operators have their access

Anatomy of an advanced persistent threat Hammertoss lifecycle

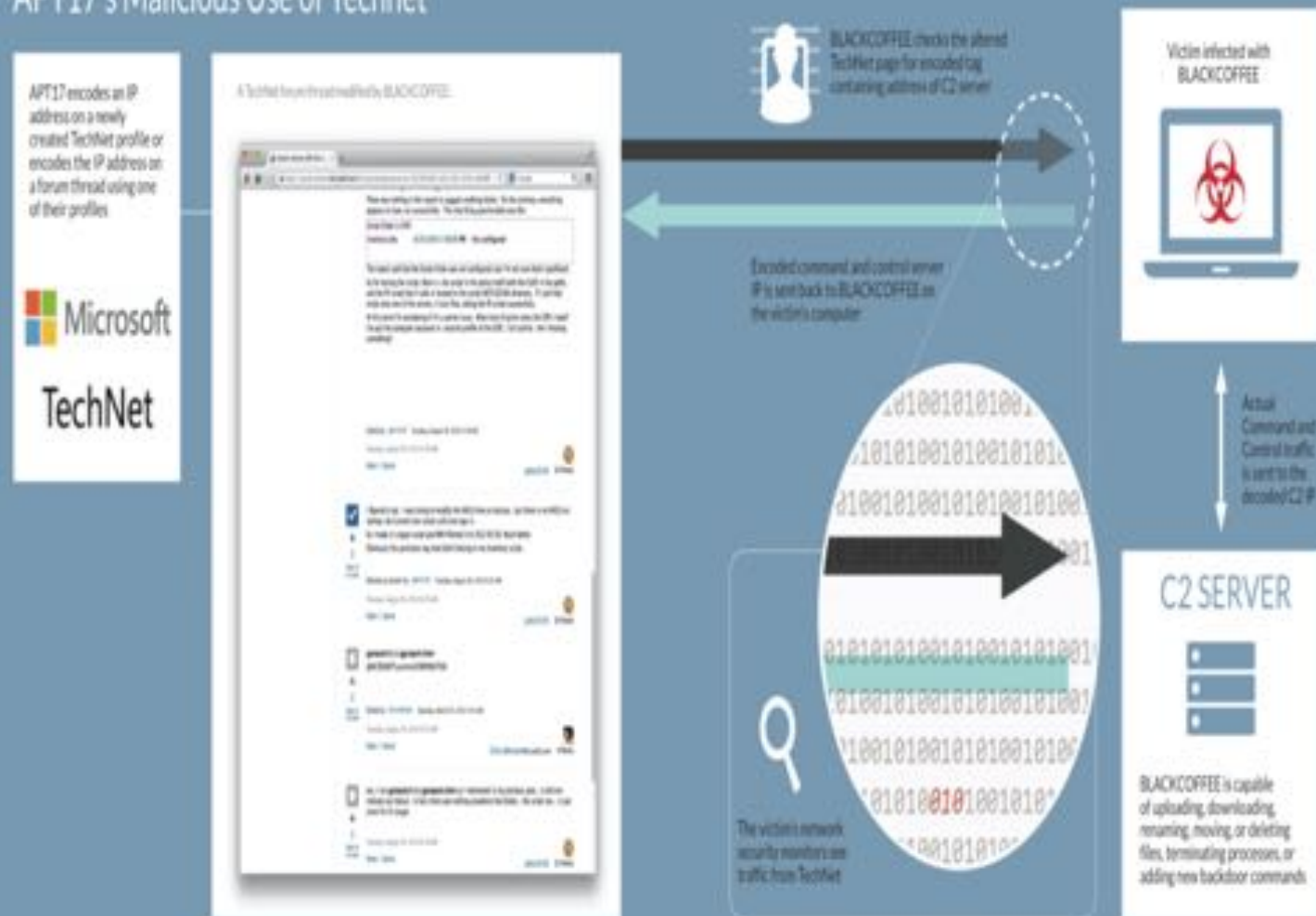


<https://www.slideshare.net/qmatheson/security-breach-its-not-if-its-not-when-its-will-you-know>

FAMOUS C2 – Deputy Dog / APT17

- **BLACKCOFFEE malware**
- **Leverages 3rd party services**
 - **MS TechNet!!!**
- **Didn't compromise TechNet**
 - **C2 encoded tags in profiles and forum posts!!**
- **C2 IP sent back to infected hosts**
- **Operators have their access**

APT17's Malicious Use of TechNet



https://www.fireeye.com/blog/threat-research/2015/05/hiding_in_plain_sight.html

DESIGN CONSIDERATIONS – Ground up approach

- **What do I want on the target?**
 - Remote access
- **What does it do once it runs on the target?**
 - Escalates privilege and persists
- **What kind of file/payload is it?**
 - MS Office doc with macro to run PowerShell
- **How do I get it to my target?**
 - Obstacles of email, network and endpoint defences
- **How does it communicate?**
 - Heartbeat over HTTP every 15 minutes
 - Domain array

DESIGN CONSIDERATIONS – OPSEC and Security

- **Domains**
 - **Good rep and history, frontable**
- **Cloud VMs**
 - **Multiple providers**
- **Monitoring**
 - **Email, slack, SMS alerting, log all the things**
- **Encryption along the way**
 - **How you connect, how targets receive/send data**
- **Harden like you would anything on the internet!**
 - **Logwatch, fail2ban, go nuts**

DESIGN CONSIDERATIONS – Technical Management

- **Size and scale**
 - How 'big' you need it to be
- **Automation**
 - Script out common builds and features
 - Terraform, C2K ;)
- **Adaptable**
 - Extending capabilities, rolling new machines and domains
- **Access and permissions**
 - Controlling access for the red team operators
 - Controlling traffic to and from the infrastructure

DESIGN CONSIDERATIONS – Role based

- **Phishing instances**
 - Servers and email accounts dedicated to phishing operations
- **Staging and payload instances**
 - Dedicated to hosting initial files/exploits/scripts
- **Short-term instances**
 - Dedicated to initial foothold or quick access tasks
- **Long-term instances**
 - Dedicated to stealth, persistence, way back in
- **Redirectors**
 - Place in front of everything
 - Proxy features is better than true redirection

DESIGN CONSIDERATIONS – Role based (cont.)

- **3rd party services**
 - **Social Media – Twitter, Telegram, Instagram**
 - **Email – Gmail, domain-based**
 - **Cloud Storage – OneDrive, Dropbox, Google Drive**
 - **Cloud VM – AWS, Digital Ocean**
 - ***aaS – GCP/GAE, Azure, AWS, Digital Ocean**
 - **Comms – Slack, Teamspeak, A/V Conference**

RED TEAM TREASURE TROVE

- Design considerations
- Domains
- Phishing
- Redirection
- C2 traffic profiles
- 3rd party comms
- Obscuring infra
- Securing infra
- Automation
- Tips

The screenshot shows the GitHub interface for the repository 'bluscreenofjeff / Red-Team-Infrastructure-Wiki'. At the top, it displays repository statistics: 102 watches, 840 stars, 180 forks, and 180 issues. Below this, there are tabs for 'Code', 'Issues (1)', 'Pull requests (0)', 'Projects (0)', and 'Insights'. The repository description is 'Wiki to collect Red Team infrastructure hardening resources'. There are tags for 'infrastructure', 'redirector', 'cobalt-strike', 'empire', 'red-team', and 'pentesting'. The repository has 81 commits, 1 branch, 0 releases, 5 contributors, and is licensed under BSD-3-Clause. A commit history table shows three commits: 'Added Cobalt Strike External C2 resources' (latest, 13 days ago), 'Added more to the phishing section' (6 months ago), and 'Initial commit' (11 months ago). The 'README.md' file is selected, showing a description of the wiki's purpose, a call to action for pull requests, and a 'Table of Contents' with links to sections like 'Design Considerations', 'Domains', 'Phishing', 'Redirection', 'C2 traffic profiles', '3rd party comms', 'Obscuring infra', 'Securing infra', 'Automation', and 'Tips'.

bluscreenofjeff / Red-Team-Infrastructure-Wiki

Watch 102 Star 840 Fork 180

Code Issues (1) Pull requests (0) Projects (0) Insights

Wiki to collect Red Team infrastructure hardening resources

infrastructure redirector cobalt-strike empire red-team pentesting

81 commits 1 branch 0 releases 5 contributors BSD-3-Clause

Branch: master New pull request Create new file Upload files Find file Clone or download

Commit	Message	Time
bluscreenofjeff	Added Cobalt Strike External C2 resources	Latest commit a62878e 13 days ago
	Added more to the phishing section	6 months ago
	Initial commit	11 months ago
	Added Cobalt Strike External C2 resources	13 days ago

README.md

This wiki is intended to provide a resources for setting up a resilient Red Team infrastructure. It was made to complement Steve Borosh (@424f424f) and Jeff Dimmock's (@bluscreenofjeff) BSides NoVa 2017 talk "Doomsday Preppers: Fortifying Your Red Team Infrastructure" (slides)

If you have an addition you'd like to make, please submit a Pull Request or file an issue on the repo.

THANK YOU to all of the authors of the content referenced in this wiki and to all who contributed!

Table of Contents

- Design Considerations
 - Functional Segregation
 - Using Redirectors
 - Sample Design
 - Further Resources
- Domains
 - Categorization and Blacklist Checking Resources
- Phishing
 - Easy Web-Based Phishing
 - Cobalt Strike Phishing
 - Phishing Frameworks

<https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki>

Automating C2 Builds

- **C2K – Command and Control Kit**
- **Version 1 (working on v2)**
- **Deploys Digital Ocean droplets**
- **Sets up Iterm for logging**
- **Installs Cobalt Strike**
- **Sets up a firewall**
- **Custom SSH config**
- **Adds HTTPS support from Let's Encrypt (thanks Alex 😊)**

 **BLACK HILLS** Information Security  [About](#) [Contact](#)

24
JUL
2017

HOW-TO BLUE TEAM, BLUE TEAMING, C2, C2 INFRASTRUCTURE, DIGITAL OCEAN, LETS ENCRYPT, PEN-TESTING, PENETRATION TESTING, RED TEAM, RED TEAMING, SSH CONFIGURATION

How to Build a C2 Infrastructure with Digital Ocean – Part 1

Lee Kagan* //



Deploying an offensive infrastructure for red teams and penetration tests can be repetitive and complicated. One of my roles on our team is to build-out and maintain the red team systems and control accesses to and from them. There's an endless variety of what you may wish to deploy but I found I was consistently repeating the same baseline deployment.

<https://www.blackhillsinfosec.com/build-c2-infrastructure-digital-ocean-part-1/>
<https://github.com/invokethreatguy/C2K>

C2K v2

Preview

LINKS AND SHOUTOUTS

- <https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki>
- <https://github.com/invokethreatguy/C2K>
- <https://cobaltstrike.com/>
- <https://fas.org/irp/doddir/dod/jp1.pdf>

Special thanks to:

- @bluscreenofjeff
- @itsreallynick
- @malcomveter
- @sixdub
- @Killswitch_GUI
- @armitagehacker
- @424f424f

THANK YOU