Microsoft

OPCDE: Red Team Handcuffs

Caleb McGary
Kyle Bachmann

Agenda

- What is this
- Who we are
- Handcuffs
- Conclusion

What this is

How a Red Team (us) deals with real world constraints that:

- Impact our day to day job
- Force us to change tactics
- Require additional actions

Who we are

One of several Microsoft Red Teams

- 8 Members (6 FTE + 1 intern + 1 manager)
- Responsible for CDG
  - COSINE (think Windows)
  - Devices
  - Gaming

Caleb McGary – https://www.linkedin.com/in/calebmcgary

Kyle Bachman - https://www.linkedin.com/in/kyle-bachmann/

Definitions

Handcuffs

verb (used with object)

- to put handcuffs on.
- to restrain or thwart (someone) by or as if by handcuffing:
- Ex: The amendments **handcuffed** the committee and prevented further action.

Handcuffs

Limitation: Using External Resources

- Attackers host and use resources that they may not fully control.

- Example:
- Stuxnet used c2 servers out of US, Canada, France, and Thailand:
  - smartclick.org
  - Best-advertising.net
  - Internetadvertising4u.com
  - Ad-marketing.net

Limitation: Using External Resources

Why this matters:

- We cannot tolerate potentially leaking data by using external, public, or untrusted resources
- Attacking from only resources we control or own makes it much easier to detect, deconflict, and respond to us
- May not fully test the incident response process as short cuts will be taken
- Adds additional overhead as we must log all actions, data, traffic, etc.

SOLUTION: EXTERNAL RESOURCES

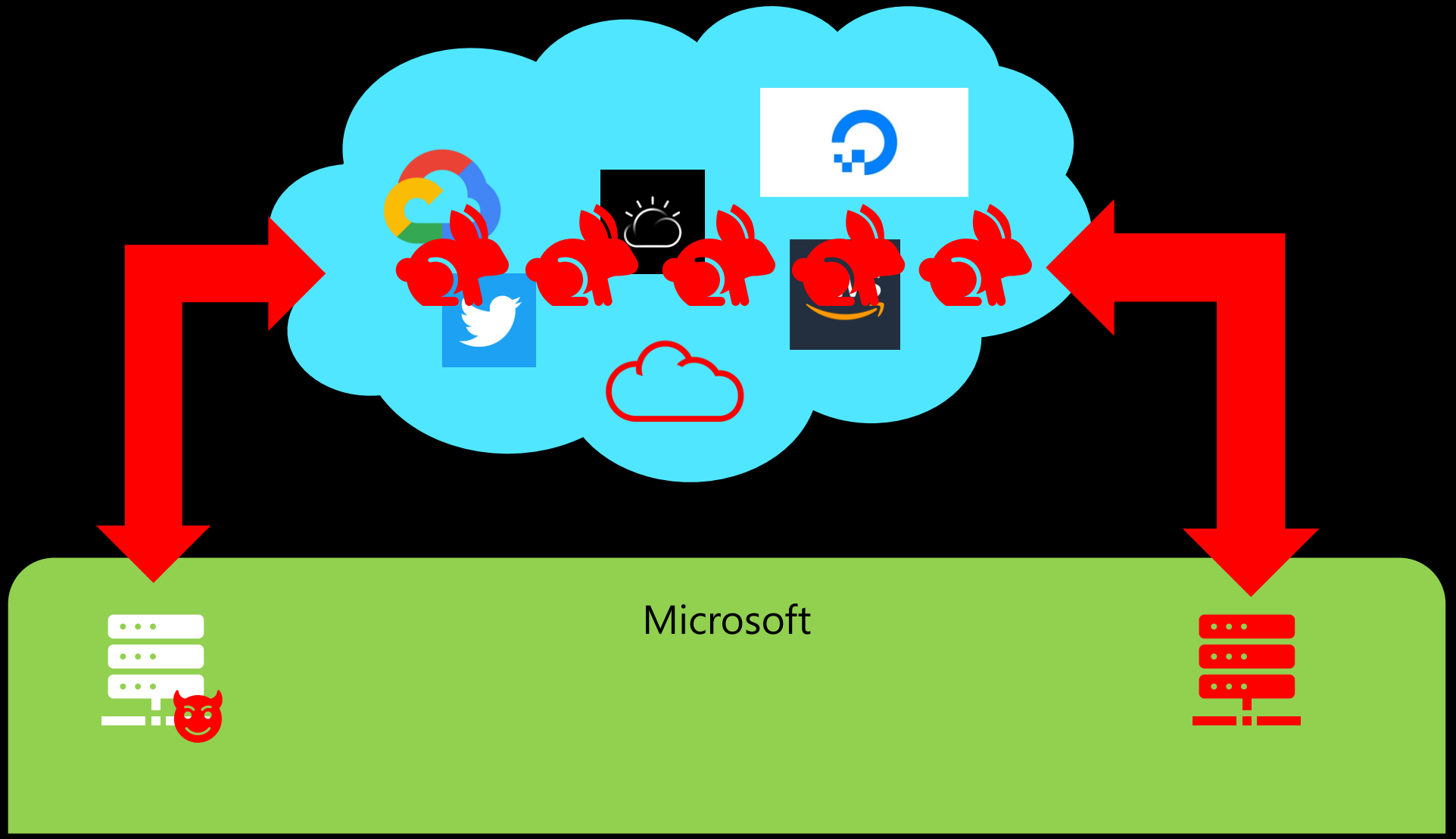
It's **often** just traffic

- Use hosted infrastructure from legitimate resources like AWS, Digital Ocean, etc
- Assume the infrastructure will be compromised; only use pass through proxies and custom payload (data) encryption
- Ideally tooling should generate payloads (data) that is protocol agnostic (chunking and tracking)

A basic implementation of this principle

- NGINX pass-thru proxies

Solution: External Resources



Limitation: Attacking Personal Devices

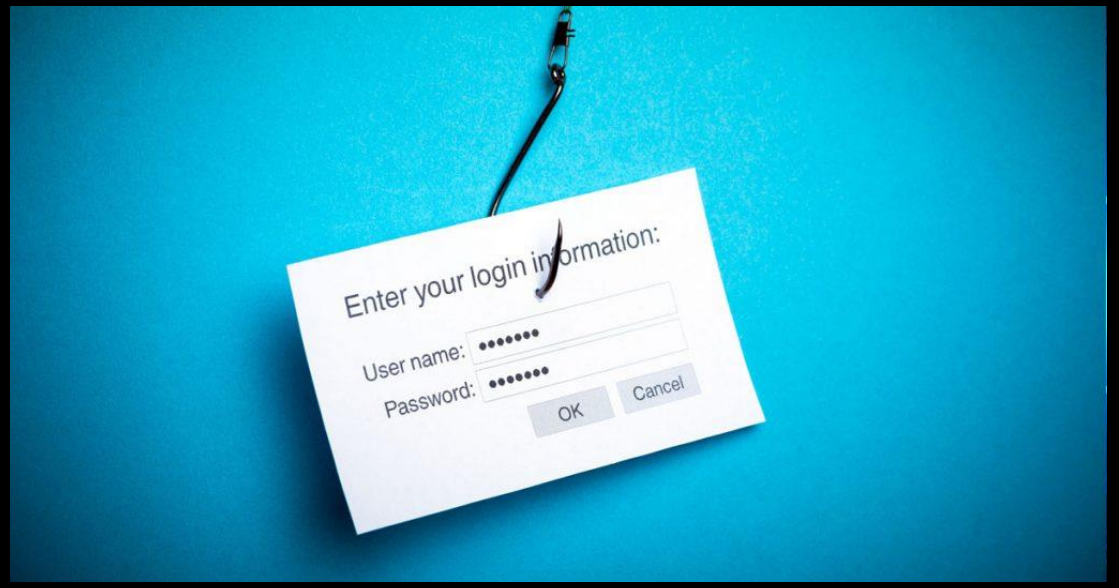
Attackers can (and do) compromise non-corporate devices to look for ways of gaining corpnet access

Example:

Android malware focused on fraud will be used for other purposes if additional access is found

Limitation: Attacking Personal Devices

- Why this matters:
- We cannot break the law and compromise personal devices or do pre-texting (in some cases)
- Personal devices **are** a valid risk to corporate regardless of training or state of device
- Erodes employee trust in team, harms or limits BYOD initiatives



Solution: Attacking Personal Devices

Via **assume breach** mentality, emulate said compromise

- Have a scenario that relies on the compromise of a personal device as a starting point; use same level of access or knowledge as would be obtained from a personal device compromise
  - Example: endpoints that are not otherwise discoverable
- Maintain personas that can be used or burned
- Work with corporate HR to figure out how to fake a user

LIMITATION: TOOLSET DEVELOPMENT

Adversaries routinely build completely new custom targeted toolsets and malware for each campaign.

Examples:

- Stuxtnet
- Duqu
- Flame
- etc

LIMITATION: TOOLSET DEVELOPMENT

Why this matters:

- When we get signatured, the cost to re-tool is high
- Not allowing for tooling to be signatured limits testing of a full response
- Fast paced cadence of work requires flexibility vs customization tradeoffs
- Potentially unable to implement attacks due to architecture choices

Solution: Toolset Development

In coordination with Hunt:

- Agree on what is signatured and how
  - "Silent Alerts"
- Age out tools periodically
- Have a robust development pipeline and skillset
  - We by design hire people that can code
- Manage tool development tightly

LIMITATION: WEAKEN SECURITY

Adversaries can (and often do) weaken the overall state of security of systems they compromise.

Examples:

- Disabling patching
- Leaving less than secure shells on system
- Disabling defensive components on system

Limitation: Weaken Security

Why this matters:

- We cannot introduce additional risk as part of our tests
- We must leave systems and compromised data in the same or greater state of security than how we find them
- We cannot risk a third-party compromise of a system we have compromised resulting in inability to correctly attribute activity

Solution: Weaken Security

Several components:

- All tooling must be reviewed internally for security flaws
- All tooling must perform strong authentication
- All actions must be logged, via automation if possible
- Internal process exists for deconflicting or evaluating potentially compromised devices
  - If compromise is found, terminate test and let Blue Team respond
- Notify Blue Team of any critical vulnerabilities that cross identity boundaries

LIMITATION: TIME BOXED

Adversaries can spend months attacking a single target.

Examples:

- Almost any active campaign out there (hence the term campaign)

Why this matters:

- We have 4-12 weeks on average to accomplish our goal
  - Includes breach, action on objective, and report
  - Subject to business rhythm constraints (change freeze, holiday, etc.)

Solution: Time boxed

Maintain persistence

- We have dedicated tooling for this (separate from main toolset)
- Generate an **irregular** signal for Blue Team to hunt on

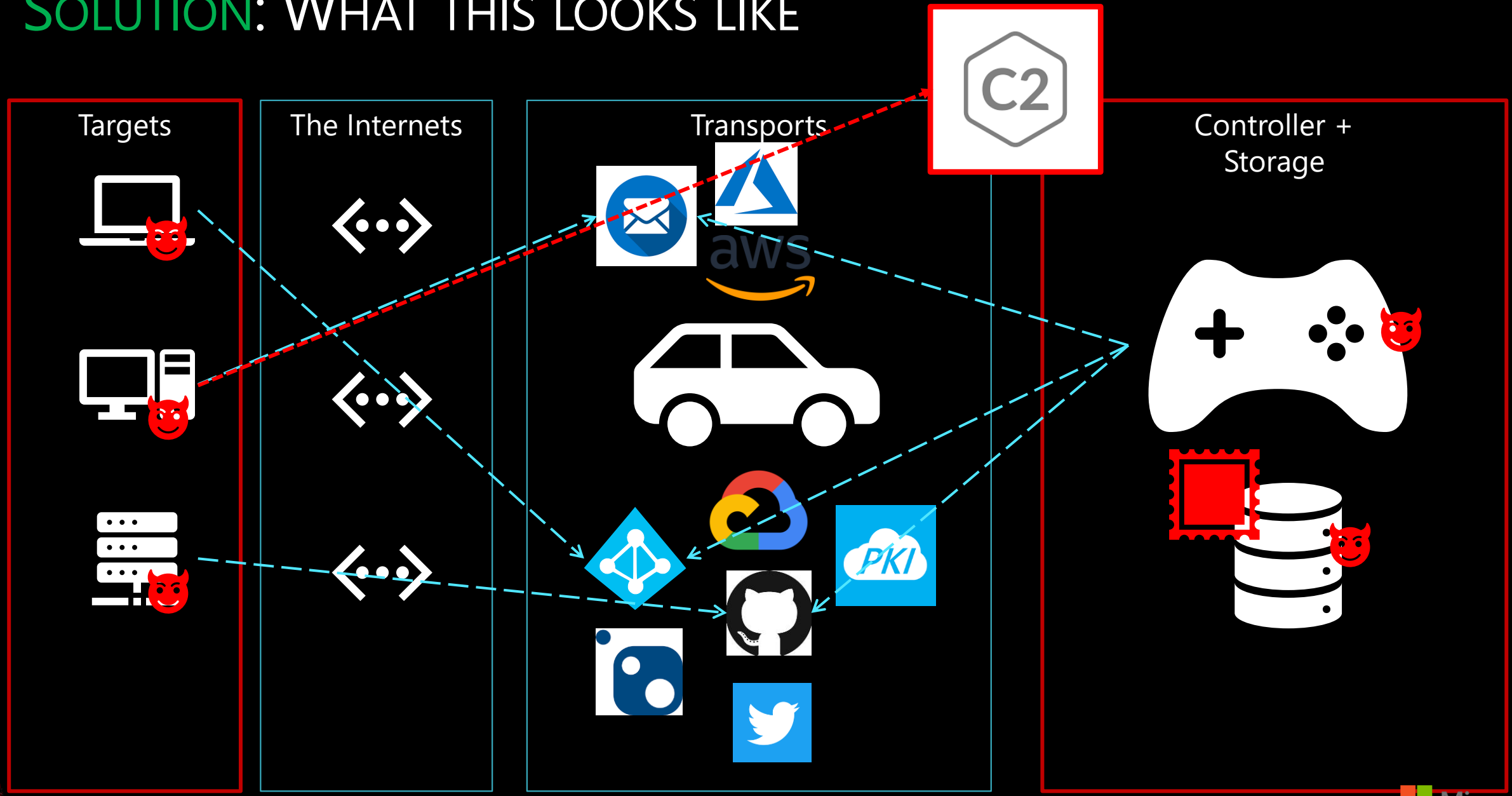
Use automation to track system state and watch for opportunity

- We have dedicated tooling for this (separate from main toolset)

Plan engagements out several cycles in advance

- We can swap or change around if opportunity arises

SOLUTION: WHAT THIS LOOKS LIKE



CONCLUSION

SUMMARY

Coordinate closely with your partners

- Blue Team (IR, Hunt, Forensics)

Use creative thinking to evaluate situations

- Allow for fluidity in your schedule

- Leverage internal knowledge, tooling, and partnerships to be more efficient

Questions