Red Team

CrossCountry
CONSULTING

In a red team assessment, the CrossCountry team attempts to gain access to your internal network (usually via **spear phishing** or **physical entry**), obtain a persistent foothold, stealthily move laterally through the network, and escalate privileges to the highest level (e.g., “Domain Admin” or similar). In a red team exercise, the Security Operations Center and/ or Incident Response teams are not informed, which evaluates their ability to detect and prevent a sophisticated attacker.

KEY DIFFERENTIATORS

Sophisticated Command and Control (C2) Infrastructure

Our infrastructure provides:

- Multiple C2 channels to persist in case of detection
- The C2 channels can use HTTPS, HTTP, and/ or DNS
- Malleable profiles that make C2 traffic appear benign even if SSL is inspected
- Automated C2 server creation and reconfiguration with Terraform scripting

Spear Phishing with Fully Functional Payloads

- We not only measure the “click rate” on a spear phishing campaign, but also demonstrate the compromise of the phishing victim’s workstation
- Our payloads evade EDR/ antivirus detection and provide a beachhead on the phishing victim’s workstation for our team to pivot to the target’s internal network

EDR/ Antivirus Evasion

- We stay abreast of which tools and techniques are likely to be detected by EDR and/ or antivirus, constantly updating your tools and techniques to remain stealthy

Web Filtering Evasion

- We provide categorized, aged domains and/ or domain fronting to evade web filter controls for disallowing suspicious or uncategorized domains

Secure Email Gateway Evasion

- Our team provides execution delays and various sandbox detection techniques that allow phishing payloads to bypass email gateway sandboxes

Sophisticated Physical Security Testing

We offer onsite security tests such as:

- RFID Badge cloning
- “Drop Box” device that connects out via cellular modem
- Social engineering, lockpicking, and burglary tools

CASE STUDY

1. Scenario

A Fortune 500 financial institution was developing an internal incident response capability. The client wished to test this new capability against the techniques of real attackers and find areas for improvement.

2. Our Approach

CrossCountry created a spear phishing campaign targeting their hiring process. The email sent to recruiters contained a resume with malicious code. We also performed a physical entry/ social engineering attack in parallel with the spear phishing attack by performing RFID badge cloning in the parking lot of the client's corporate headquarters, used the cloned badges to enter the building, and connected a rogue device to the network in a conference room.

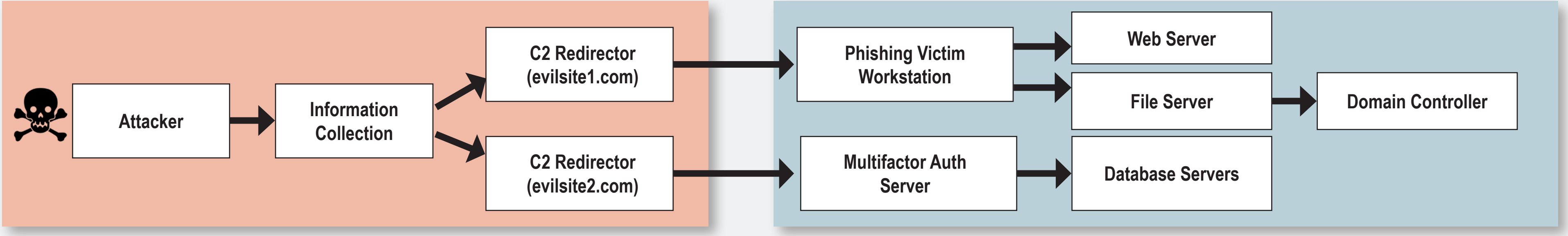
3. Objective

CrossCountry moved laterally from its initial foothold and escalated privileges, evading detection by EDR, antivirus, email sandboxing, and other security tools. CrossCountry compromised the domain controller, downloaded all employee hashes and cracked them offline, demonstrating full control of the client's network.

4. Impact

The client made multiple improvements to its incident response procedures and fine tuned its alerts based on the results of the test. They are now better prepared to detect and respond to a real incident in the future.

The following diagram shows CrossCountry's attack path:



Attacker

Information Collection

C2 Redirector (evilsite1.com)

C2 Redirector (evilsite2.com)

Phishing Victim Workstation

Multifactor Auth Server

Web Server

File Server

Database Servers

Domain Controller

MEET OUR TEAM

CAMERON OVER
Cyber & Privacy Partner Lead
cover@crosscountry–consulting.com

ERIC EAMES
Advanced Cyber Risk Lead
eeames@crosscountry–consulting.com