Adversary Emulation

CrossCountry Consulting

Going far beyond a traditional penetration test or even a red team engagement, adversary emulation is recreating the tactics, techniques, and procedures of **modern**, **sophisticated adversaries** against your enterprise. The CrossCountry team has many **key differentiators** that distinguish its adversary emulation offering from the penetration testing and red team offerings of many competitors.

KEY DIFFERENTIATORS

Threat Intelligence-Informed Scenarios

- Our in-house threat intelligence team pinpoints the threat actors most likely to target your organization and their likely objectives
- We help you select the scenario best suited to your goals
- Our team can emulate the tactics, techniques, and procedures of the selected threat actor

Sophisticated Command and Control (C2) Infrastructure

Our infrastructure provides:

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

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

Secure Email Gateway Evasion

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

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

Pursuit of Realistic Attacker Objectives

- We demonstrate the impact of a breach to non-technical stakeholders, which can be used to increase or prioritize security budget
- The objective could be money movement, intellectual property theft, mergers and acquisitions information, identity theft, planting ransomware, and many more

Web Filtering Evasion

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

Sophisticated Physical Security Testing

We offer onsite security tests such as:

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

CASE STUDY

1. Scenario

A Fortune 500 company recently fell victim to a ransomware attack despite regular penetration testing and weekly vulnerability scanning. The attackers not only encrypted sensitive databases, but threatened to publish their contents online. After responding to the ransomware incident, the client was eager to ensure that it would not be repeated in the future. They wanted to discover and eliminate the weak points in its defenses that sophisticated attackers can exploit.

2. Our Approach

CrossCountry created a spear phishing campaign targeting new employees. The email sent to the targeted employees appeared to come from the company's online training provider and said that the employee's required business ethics training was past due. The employee wanted to comply with the training requirement and clicked the link in the email. This downloaded a "media player" to the employee's desktop which gave our team remote access to his workstation.

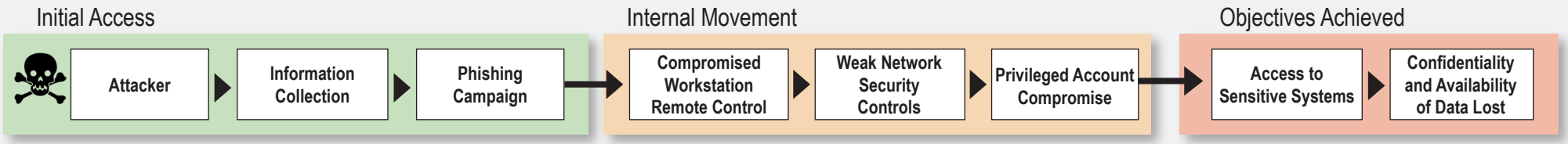
3. Objective

CrossCountry found and exploited multiple vulnerabilities on the company's internal network. These included exposed plain text passwords, a lack of network segmentation, web application vulnerabilities, misconfigured security tools, and insufficient incident response procedures. These vulnerabilities led to CrossCountry gaining privileged access to the client's database servers. We coordinated on a non-disruptive demonstration of access, and CrossCountry planted a "flag" text file in a specific folder on five sensitive database servers.

4. Impact

After demonstrating that an attacker could still obtain sufficient access to execute another ransomware attack, the client's CISO received an increased budget to implement stronger security measures. Based on the results of the adversary emulation exercise, they reprioritized its security spending, focusing on countermeasures for the weaknesses demonstrated during the exercise. The client continues to perform regular adversary emulations to further eliminate vulnerabilities and practice detecting attacks, and has not fallen victim to another ransomware attack.

The following diagram shows CrossCountry's attack path:



MEET OUR TEAM

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

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