CASE STUDY

MANDIANT®
A FireEye® Company

International Retailer Bolsters Security Operations

Use case for Red Team Assessment

SITUATION

A popular global clothing retailer suffered a harmful cyber breach involving theft of its customers' personal data. After remediation efforts were concluded, the organization's security leaders committed to revamping their program infrastructure. They quickly recognized the need to assess the effectiveness of their cyber security posture and existing operational controls in the event of another targeted attack against their critical assets, which they identified as customer credentials, employee data, payment information and point-of-sale (POS) systems.

The retail industry is a primary target for cyber criminals around the world, who pursue a variety of financial and identity-related theft motives. Financially motivated threat actors commonly exploit retailers through POS compromise, which enables them to collect customer credentials and monetize and launder stolen financial funds. Despite mindful measures organizations have taken to secure themselves against these threats, the sophistication of retail attack groups continues to heighten, and their presence continues to grow.

Former cyber breach initiates assessment

Proactive preparation is key to getting ahead of targeted adversary attacks, including periodic independent evaluation of the organization's current prevention, detection and response capabilities. Virtually all breached organizations think their security program is effective — until they find out the hard way that it isn't.

FireEye Mandiant has a world-class reputation responding to the most complex breaches worldwide. Knowing this, the retailer engaged a Mandiant Red Team Assessment to objectively evaluate their detection and response capabilities against targeted attacks. A no-holds-barred simulated attack scenario was conducted in the client's environment, emulating current, real-world threats. The red team consultants worked with the retailer's senior leaders to identify a set of jointly agreed upon objectives that focused on high-risk areas of the business.

Meeting assessment objectives

Over the course of an eight-week engagement, Mandiant experts evaluated the organization's prevention, detection and incident response capabilities by simulating a determined attacker. This evaluation went far beyond compliance checklists — it examined the client's ability to detect malicious activity and respond to the detected events by observing the processes, tools and staffing deployed in response to threat activity.

FireEye

The red team simulated a full attack lifecycle—from initial reconnaissance to mission completion (Fig. 1).

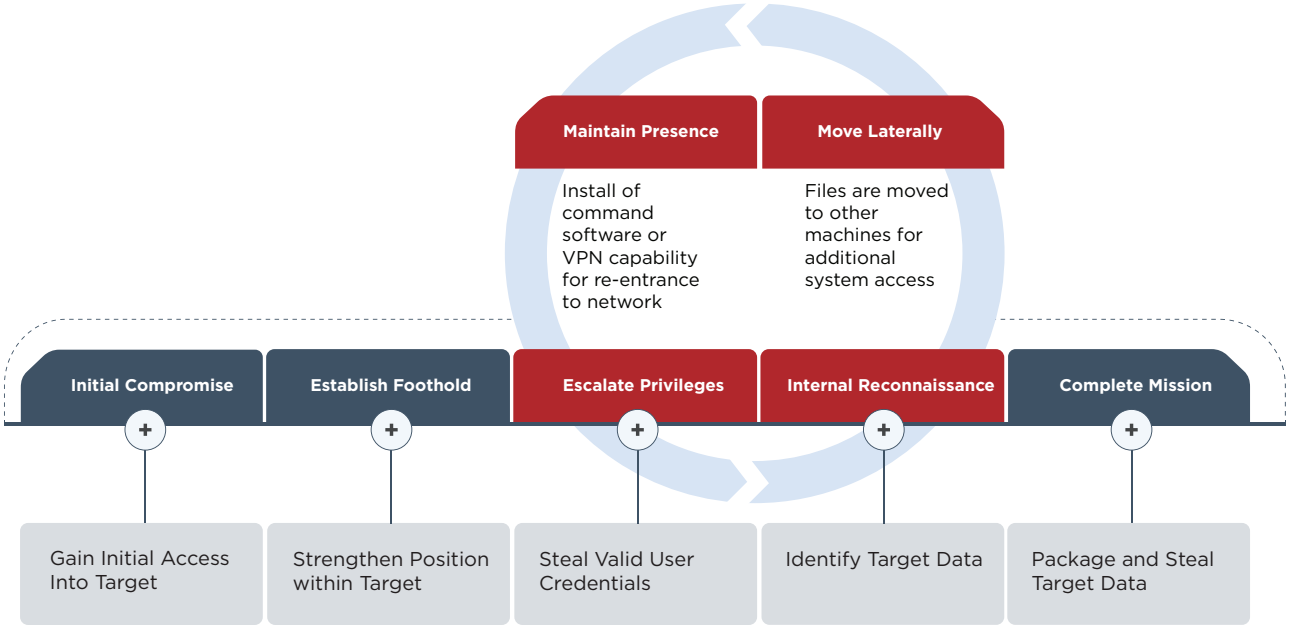

Figure 1. Cyber attack lifecycle.

Mandiant consultants challenged the organization's security team to respond to the following simulated scenarios for each attack lifecycle phase (Table 1).

Table 1. Red team attack lifecycle simulation activity.

Lifecycle Phase	Duration	Scenario Tactics
Initial compromise	3 days	• Recon-based phishing • Domain fronting • Obfuscated payload
Establish foothold	1 day	• Registry persistence
Lateral movement	Ongoing over 7 weeks	• WMI and Powershell frameworks • 2-Factor bypass using SMB sessions • Segmentation bypass through pivoting
Escalate privileges		• Kerberoasting – 1 day • Credential dumping – Ongoing over 7 weeks
Internal reconnaissance	Ongoing over 7 weeks	• Interrogation of network hosts
Maintain presence	Ongoing over 7 weeks	• Expanding network positions
Complete mission	2 weeks	• Enabling admin logon using API interface • Exfiltration using HTTPS

Mandiant consultants tested the detection and response capabilities of the retailer's current security function by performing the following tactics.

Through these exercises, Mandiant experts revealed the true impact a sophisticated attacker can have on the organization's cyber environment.

Initial compromise

Recon-based phishing: The red team performed targeted phishing attacks on employees identified by the organization and executed lures based on reconnaissance findings.

Domain fronting: The domain name of a reputable site was used for initial connection. While this well-known domain was exposed to the gateways in clear-text, the domain name of the actual target server was only communicated after the establishment of an encrypted HTTPS connection. This information was hidden from the organization's security technology deployed at the gateway.

Obfuscated payload: The red team constructed an implant and disguised it using the Veil Evasion tool. This created a Windows executable file that served as a means to obtain an initial foothold into the retailer's network. Use of the tool's Python Packer prevented detection by most common antivirus applications.

Establish foothold

Registry persistence: The red team established a foothold by installing a persistent backdoor to the retail manufacturer's host systems, which became accessible after initial compromise.

Escalate privileges

Domain access: The red team obtained domain privileges by using a technique called Kerberoasting. This technique targeted accounts used to run services (such as MSSQL, J2EE, SCCM, Citrix) within the domain and other trusted domains. These service accounts were registered as service principal names (SPNs) on the domain controller.

Kerberoasting took advantage of the fact that, by design, any domain user could request a Kerberos ticket for any domain service, regardless of whether the user was granted access to the service. Each ticket contained a hashed form of the service account password which was then attacked offline.

Credential dumping: Local administrator logins were used to dump credentials in memory for pass the hash attacks or password cracking of over 30 passwords.

Internal reconnaissance

Interrogation: Using the initially acquired list of client domain computers, the red team began interrogating the network's reachable hosts by inspecting the activity of users who had active sessions on hosts to which the red team had gained access.

This process was repeated as new network perspectives were gained through lateral movement. This information was then used to dump credentials on hosts of interest after lateral movement was achieved.

Lateral movement

WMI and Powershell: The red team used WMI and Powershell frameworks to execute the in-memory payload across hosts to achieve lateral movement.

2-Factor bypass: The red team bypassed 2-factor controls on remote desktop protocol (RDP) interfaces by using server message block (SMB) sessions to infiltrate such restricted systems including production and infrastructure administration servers.

Segmentation bypass: The red team used dual-homed hosts to pivot from accessible segments where the red team gained an initial foothold to restricted segments, such as the production and administration servers.

Maintain presence

Expanding presence: The red team continued to establish backdoors and alternate callbacks from restricted segments that allowed navigation to additional areas with increased network accessibility.

Complete mission

Administrator login: The red team bypassed 2-factor controls that were set on the retailer's POS devices being used to restrict administrator access. This was accomplished by disabling the 2nd factor from the POS API interface and logging in as an administrator.

Accessing PII: The red team proved they were able to access personal customer data (such as email addresses, phone numbers, home addresses, usage history) by using a cloud hosted API interface with API keys from developer emails.

Domain fronting is a communication technique using different domain names across various layers of communication.

Kerberos is a network protocol that uses secret-key cryptography to authenticate client-server applications.

Kerberoasting takes advantage of how service accounts use Kerberos authentication with service principal names (SPNs) and allows password cracking for those accounts.

	Initial Reconnaissance	Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
Detect	—	✓	✗	✗	✓	✓	✗	✗
Inhibit	✗	✗	✗	✗	✗	✗	✗	✗
Respond	✗	✗	✗	✗	✗	✗	✗	✗

Figure 2. Evaluation of client's capabilities.

Taking action

After the assessment was completed, the customer received tactical and strategic recommendations for immediate and long-term improvements. Because multiple ineffective controls were discovered and business risks continued to accumulate, the CISO worked closely with Mandiant experts to strengthen the organization's detection capabilities and ultimately reduce overall incident response time.

Based on these recommendations, the retail manufacturer reprioritized its security investments:

- Implementation of endpoint and detection response (EDR) products and egress monitoring systems
- Adoption of an augmented IR plan
- Mandate for routine use of prescriptive playbooks addressing:
  - Phishing
  - Data theft
  - Compromised credentials
  - Malware
  - Denial of service
  - Ransomware
  - Compromised system
  - Security violations
  - Unlawful activity
  - Vulnerability exploitation
  - Other criminal activity

Red teams raise critical vulnerability awareness

The customer deployed a Mandiant Red Team Assessment to test the detection and response capabilities of its current security function. Their security team gained first-hand experience responding to a real-world target attack — without actual risk to the business.

Through these exercises, Mandiant experts revealed the true impact a sophisticated attacker has on an organization's cyber environment. This assessment uncovered significant gaps in the retailer's security posture and the effectiveness of their existing processes, increasing the organization's awareness of current vulnerabilities that attackers could use in a future attack.

The red team engagement succeeded in helping the organization learn from their incident response shortfalls and build a roadmap for immediate and long-term improvements. Ultimately, the results of this assessment helped justify additional security budget and the need for periodic maturity evaluations to maintain the retailer's ability to outmaneuver advanced attackers.

For more information, visit: **https://www.fireeye.com/services/red-team-assessments.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FireEye