PERFORMANTA

Case study

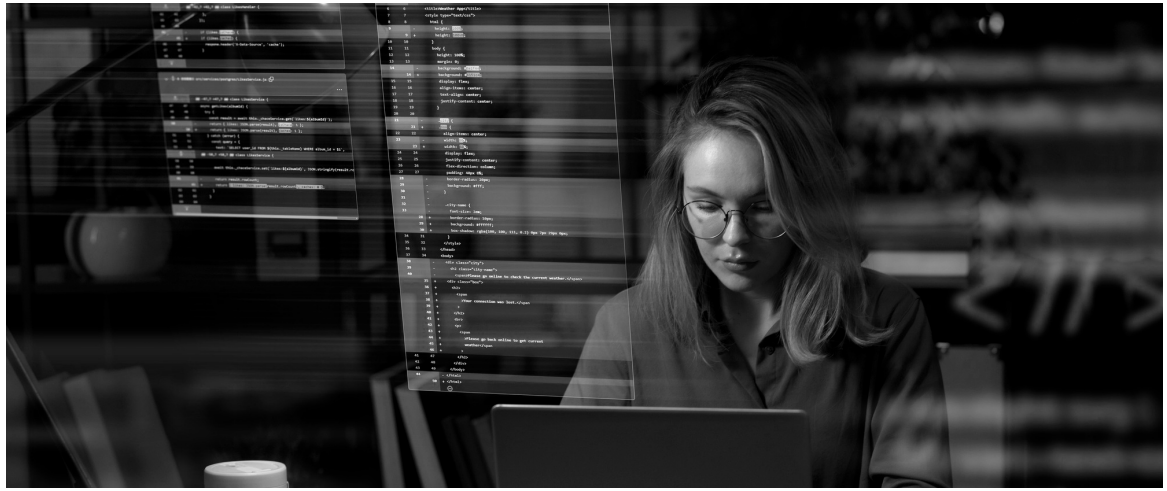
Detecting and stopping a targeted nation-state attack

Leading Global Telecoms Company

Security Information and Event Management (SIEM) & Extended Detection & Response (XDR)

Overview

- A well-resourced attack targeted Performanta's client, a large global telecommunications company.
- Performanta's investigation uncovered an elaborate attack, including web shells and backdoors, custom-written malware, extensive phishing, and many compromised mail accounts.
- We shut down the attack through several actions, including reverse-engineering the malware, creating a DNS blackhole server to stop access to malicious URLs, expanding deployment of endpoint threat detection, and securing domain admin and other privileged accounts.
- It took around 14 months to remove the damage caused by the attackers, but the breach attempt was halted in its tracks.
- Our client gained a 60 percent improvement in the Mean Time to Detect (MTTD) security incidents and a 40 percent increase in network visibility.



Executive Summary

Broadly speaking, there are two types of cyber attacks. One is opportunistic, focusing on random victims. But the other type targets specific organisations and individuals. These latter attacks are well-funded, well-planned, and often have the backing of a nation-state. They are incredibly dangerous and difficult to detect. Performanta's client, a large global telecommunications firm, fell in the crosshairs of what became known as Operation Soft Cell: a sophisticated attack against global telcos by a well-resourced nation-state attacker.

Our client's security information and event management (SIEM) detected a failed login to an Active Directory (AD) administration account—indicating a potential breach attempt. Springing into action, Performanta's XDR team uncovered the attack. Evidence included installed web shells and backdoors, phishing campaigns, custom-written malware, and compromised mailboxes. These are all hallmarks of a high-level attack.

Fortunately, the SIEM caught wind of the attack. Since Performanta and our client had previously created response plans, there was little delay in responding to the breach. Our actions included isolating impacted systems, creating a DNS blackhole server to stop access to malicious URLs, reverse-engineering the malware, expanding deployment of endpoint threat detection, and securing domain admin and other privileged accounts. We also improved the context of the SIEM system's rules to improve its detection.

It took 14 months to remove all traces of multiple state-backed attackers from our client's enterprise systems. That speaks to the stealthy and deliberate nature of the attack. Yet the event also demonstrates how layered and integrated security can hamper even the most determined attacker. While the incident revealed areas for improvement, it also showed how modern cybersecurity can fight back against well-resourced and determined attackers. Without these measures, our client would only have discovered the breach long after it accomplished its goals.

The Challenge

Sophisticated cyber attacks are slow, methodical and clandestine. Once attackers find a way in, they start changing the environment to support their campaign. If these actions go undetected, the attack will only surface once the criminals pull the trigger—by this point, it is often too late to stop the attack. Hence why early detection and removal is critical. In this case, our client's security information and event management (SIEM) system detected a failed suspicious login attempt to an ActiveDirectory (AD) admin account.

Accessing power AD accounts is often one of the first major steps in a breach. Upon closer investigation, our security team uncovered an advanced attack. The perpetrators had started installing web shells and backdoors, modified registry credentials, compromised mailboxes, circulated malicious Excel attachments, and begun stealing data. The extent of the attack was significant, and clearing it would require serious countermeasures.

The Solution

A nation-state group was behind this elaborate and highly-planned attack. Fortunately, the SIEM exposed their activities. Good cybersecurity is not a wall but a series of sandtraps, dead-ends and monitors that impede and detect dangerous activities. Once alerted, we evaluated the situation and locked down key areas, following an established response plan.

Performanta's extended detection & response (XDR) teams took several crucial steps against the breach. We launched proactive 24x7 engagement to detect, contain and remediate the compromise, and reverse-engineered the malware. We deployed endpoint detection (EDR) services across the client's 20 countries of operation and helped our client develop appropriate endpoint rules. Other actions included deploying a DNS blackhole server to prevent access to malicious URLs, secured domain admin and other privileged accounts.

The Results

This attack was eventually identified as Operation Soft Cell, a concerted nation-state attack staged against multiple global telecommunications providers. Soft Cell is a textbook example of a high-level attack: it focused on specific targets (instead of random victims), using tactics such as phishing, zero-day vulnerabilities and custom-built malware. In most cases, companies are woefully underprepared for such an adversary.

Fortunately, our client's SIEM detected anomalies, and our security team and response protocols responded. Our client's security measures worked. There was room for improvement, underscoring the reality that a security environment is never static; it must constantly evolve and improve. Performanta helped prevent the attack from causing extensive damage. We additionally helped our client improve their security based on these lessons, leading to a 60 percent improvement in the Mean Time to Detect (MTTD) security incidents and a 40 percent increase in network visibility.

PERFORMANTA

www.performanta.com