CUSTOMER STORY

FireEye

How One Bank is Winning the Cyber Security War with FireEye

FACTS AT A GLANCE

INDUSTRY

Finance

CUSTOMER PROFILE
One of the oldest and most profitable financial services providers in Asia — offering a wide range of banking and financial products that serve both retail and corporate clients — was recently the latest in a long line of high profile corporations to be breached.

Challenge
On "D" Day — discovery day — the bank's staff was unable to access a domain controller — a server that responds to security authentication requests within a Windows Server domain. An internal investigation discovered that a suspicious login account with domain administrator privileges had been created, enabling unrestricted access to thousands of Windows systems — both servers and clients — across the enterprise. The bank quickly realized that they were looking at the potential for many host systems to have been compromised.

> "It was the Mandiant Incident Response services from FireEye that enabled us to understand the extent of the breach, reverse engineer all of the malware, and block further attempts."
>
> — **Spokesperson for Financial Services Provider**

Solution

Based on its global reputation for dealing with advanced threat actors from around the world, the bank immediately retained Mandiant Incident Response services from FireEye to assist with an enterprise-wide investigation of the intrusion. The service helps organizations evaluate if they have been compromised by advanced attack groups and to determine if criminals are currently still active within the enterprise environment.

Results

Mandiant experts use experience gained over thousands of investigations together with leading-edge FireEye tools when assessing enterprise infrastructures for the presence of various indicators of targeted attacker activity. Findings revealed that the breach followed a pattern that was very familiar to the Mandiant experts:

Initial compromise: Mandiant concluded that the first intrusion occurred on a specific system within the bank two months prior to initial detection, originating from a remote location within a wholly-owned subsidiary's network.

Establishment of a foothold: The attackers moved laterally within the subsidiary's network and quickly found a system that had trusted access to the bank's enterprise infrastructure. While trust relationships are established for valid business needs, attackers are known to exploit them for unauthorized access. In this case too, the criminals leveraged this weakness to enter the bank undetected and gain a foothold deep within the bank's enterprise systems.

Escalation of privileges: A spokesperson for the bank described, "The Mandiant team showed us evidence that the attackers had established a presence in the Microsoft Windows environment during the first month — across multiple hosts — and obtained Domain Admin access." While the evidence was irrefutable, obtaining it was not an easy task. The attackers leveraged genuine enterprise management tools used by the bank's IT staff, enabling them to blend into the bank's environment, and making it difficult to detect their presence or differentiate malicious behaviours from the team's legitimate activities. However, the Mandiant experts were experienced in investigating such attacker activities and able to quickly gather the necessary evidence.

Internal reconnaissance: The Mandiant experts noticed that a legitimate remote management application had been configured to record sessions and their review of these files found evidence of the deployment of malware and monitoring of enterprise e-mail / messaging servers. During the second month of the breach, there was almost daily activity from the attackers within the bank's environment.

Completion of mission: Fortunately, the multi-month campaign mounted by the perpetrators was discovered before they managed to accomplish their final goal. However, the Mandiant team confirmed the presence of breach artifacts on 96 systems — 26 servers and 70 workstations — and 30 systems were found to have active malware running at the time of investigation.

The Mandiant team recovered numerous advanced malware samples that were named to blend in with commonly installed utilities on the bank's systems, such as hkcmd.exe and winmail.exe. The malware families identified included WHITEOUT, SLIMDOWN and NESTEGG.

The spokesperson recounted, "Mandiant uncovered evidence indicating that after planting backdoor and data loading programs, the attackers utilized screen grabbing and key logging capabilities to capture passwords from authenticated users.

"Specifically, 30 hosts were identified with screen grabber malware artefacts and over 50 user profiles were infiltrated by key logging software. The attackers had access to credentials and information that included Enterprise Mail Systems, the decoding of National Payment Message Standard (NPMS) format files, Funds Transfer/ Remmittance Systems and directory systems."

Analysis of the backdoors by the Mandiant team revealed that they contained hardcoded IP addresses for the bank's web proxy devices, along with compromised credentials from valid Windows Login IDs that permitted the attackers to establish communications with the Command and Control (C2) infrastructure. "20 IP addresses and 5 fully qualified domain names (FQDNs) were found to be associated with the attackers' C2 infrastructure" stated the spokesperson. Such level of customized malware left no doubt that this was a targeted attack and the bank was an explicitly chosen victim.

> "The Mandiant team showed us evidence that the attackers had established a presence in the Microsoft Windows environment during the first month."
>
> — **Spokesperson for Financial Services Provider**

The Mandiant team's analysis of the remaining malware samples showed that the attackers had utilized encryption, anti-forensics, and sophisticated techniques to permit their malware to operate in a manner that evaded detection by the bank's security infrastructure.

Battle by battle

Within a couple of days of the Mandiant Incident Response service starting, the bank followed the team's advice by deploying measures that resulted in the successful blocking of the attackers' C2 infrastructure access. In addition, communication between the subsidiary and the bank was halted to mitigate any further lateral movement attempts by the perpetrators.

However, two weeks later, during its forensic deep-dive research, the Mandiant experts identified renewed attacker activity and another of the bank's trusted providers pursued the line of investigation to find that Access Control Lists (ACLs) had been implemented between the subsidiary and the bank in a way that enabled the attackers to regain access to the environment. The issue with the ACLs was immediately corrected and access re-blocked.

Winning the war

The attackers already appeared to have retreated from the environment once they realized that the bank was committed to tracking their activity, uncovering their backdoors and that it would be relentless in eradicating the threat. The Mandiant team worked with the bank to construct an aggressive remediation plan — covering short-term, medium-term and long-term timeframes — as well as providing guidance and supervision to several external vendors involved in executing the detailed action plan.

The capabilities exhibited by the threat actors — including the unique malware customization, attack sophistication, and the C2 infrastructure infiltration — indicated that they are a well-funded, highly organized group and that the attack was structured and specifically targeted against the bank. The multi-month timeline gave further evidence of the patience and strategic planning that preceded each individual compromise. The Mandiant team found no evidence to suggest that any element of the attack had involved bank personnel or its extended staff.

"We work with two of the most recognized names in the computer industry and they deployed their own investigation teams but it was the Mandiant Incident Response services from FireEye that enabled us to understand the extent of the breach, reverse engineer all of the malware, and block further attempts," concluded the spokesperson.

Profiles and characteristics for each of the tactics and techniques used by the attackers were uploaded to Mandiant Advanced Threat Response Centers around the world to further enhance the global threat intelligence of the industry leader in helping organizations respond to and proactively protect against advanced cyber security attacks.

To learn more about FireEye, visit: **www.FireEye.com**

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 has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®