Regional Bank Defeats Spear-Phishing Campaign with FireEye ETP and NX Essentials

FACTS AT A GLANCE

INDUSTRY	FINANCE

FIREEYE® SOLUTIONS

- FireEye Network Security
- FireEye Email Threat Protection

KEY BENEFITS

- Support for parallel security analysis across multiple virtual operating systems
- In first year, blocked 248 malware-carrying emails that slipped by legacy firewalls
- Able to leverage the latest threat intelligence
- Reduced operational overhead by minimizing duplicate and false-positive alerts from incumbent firewalls

"Nobody in financial services is immune: We are continually coming under attack by coordinated spear-phishing campaigns. ETP has caught every last malware attachment our web filter missed – and NX Essentials is monitoring the other major attack vector."

— **Chief Information Officer**, a Regional Bank

Putting Members First

Since its founding this regional bank has been serving residents with a mantra of 'community first.' It is deeply vested in its customers; they are friends, family, and neighbors. Daily, the bank strives to help its members reach their financial goals and is often more effective in doing so than national banks headquartered elsewhere.

As with all financial institutions, this regional bank is always under cyber attack. Its chief information officer (CIO) revealed, "In the 21st century a community focus is not enough; a regional bank must also offer cutting-edge security, on par with national financial service providers, if it is to remain competitive and responsibly serve its customers."

The CIO knew security must be addressed holistically so the bank first undertook safeguarding the most common threat vector: email. With traditional signature-based security the bank was working overtime to stay ahead of aggressive spear-phishing campaigns; continually being bombarded with emails carrying malware in links or attachments. Simply keeping the infrastructure safe required constant modifications to the legacy protection to manually block known malware.

FireEye

"ETP and NX Essentials have gone beyond our wildest expectations by identifying the threats that are trying to sneak past our legacy security solutions. FireEye gives us visibility into the threat landscape, which is critical for our future security decisions; and as attacks evolve we know we have the backing of FireEye and Mandiant experts."

— **IT Systems Specialist**, a Regional Bank

Cloud-based Excellence

While seeking a best-in-class solution, the bank investigated eight vendors. The IT systems specialist stated, "We set out by researching available materials from industry analysts and FireEye was so favorably reviewed we had to reach out to its team. In the past, we have not sought cloud services but when I saw what FireEye Email Threat Prevention (ETP) was capable of, it blew me out of the water!

"ETP offered better security and more functionality than the hardware-based products at the same price point. For example, we asked several other vendors about parallel analysis using multiple virtual operating systems and they tried to mumble their way out of addressing the question. FireEye, however, analyzes email attachments against a wide range of browser, applications, and operating system environments."

The CIO was impressed by the stability of FireEye being a security-only company, and reflected, "The FireEye employees were forthright with us, FireEye obviously puts its customers' satisfaction first. ETP was one of the first cloud-based solutions in our infrastructure. The point-to-point connections between our web filter, ETP, and our Microsoft Exchange servers are all encrypted. We configured ETP inline and immediately saw results."

Successfully Blocking Attacks

The bank found the implementation process painless and just 12 hours after going live, ETP caught its first malicious email attachment. During its first year of deployment, ETP stopped 248 malware-carrying emails – across the multi-operating system infrastructure – that had slipped by the legacy protection.

The ETP solution easily handles the thousands of emails the bank receives on a daily basis, and it no longer needs to spend large amounts of time manually updating signatures. The IT systems specialist confirmed that managing ETP is straightforward and commented, "ETP's graphical user interface is clean and easy-to-use. It is constantly updated with the latest threat intelligence gleaned from FireEye's worldwide network to keep us one step ahead of the latest threats."

The CIO noted, "In my opinion ETP is a genius solution. Zero-day attacks are slicing through signature-based security and ransomware is becoming such a growing concern that possessing a solution that actually detonates malicious code in an isolated environment – the FireEye MVX engine -- is an order of magnitude improvement. It's become a necessity."

Backed by FireEye Expertise

When ETP detects an email with a suspicious link it notifies the bank and sends the information to FireEye for diagnosis. The bank also utilizes Mandiant, a FireEye company renowned in helping organizations respond to and proactively protect against advanced cyber security threats. In the unlikely event that malware is received and released, this team can advise on the potential impact to the bank, and provide counseling for how best to contain the threat and mitigate any ensuing damage.

The IT systems specialist stated, "In the world of response and protection, the names FireEye and Mandiant are synonymous with the best. We feel much more secure knowing that Mandiant experts are familiar with our environment, and ready to assist us."

FireEye

"To serve a relatively small population, yet be on the cutting-edge of security is a very unique position afforded us by FireEye, and one that grants us the privilege of truly putting our member community first."

— **IT Systems Specialist**, a Regional Bank

Essential Security

Being highly satisfied with its ETP solution, the bank sought to fully secure other possible attack vectors and selected FireEye Network Security (NX) Essentials to detect and prevent malicious activity occurring outside of email-based traffic. NX uses a dual approach of detecting advanced, zero-day attacks using the FireEye MVX engine and identifying known attacks with signature-based IPS technologies. Also configured inline, NX reduced operational overhead by minimizing the duplicate and false-positive alerts seen in some of the legacy defenses.

A Strong Partnership

The IT systems specialist observed, "ETP and NX Essentials have gone beyond our wildest expectations by identifying the threats that are trying to sneak past our legacy security solutions. FireEye gives us visibility into the threat landscape, which is critical for our future security decisions; and as attacks evolve we know we have the backing of FireEye and Mandiant experts."

The CIO concluded, "To serve a relatively small population, yet be on the cutting-edge of security is a very unique position afforded us by FireEye, and one that grants us the privilege of truly putting our member community first."

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.

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

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye