How IRONSCALES Would Eliminate a Phishing Attack Targeting a Major Healthcare System

Since the beginning of 2015, healthcare has been the industry most targeted by cyber attack, according to IBM's Cybersecurity Intelligence Index. This is largely because, for financially motivated cyber criminals, illegally obtaining medical records can sell for significant profit on the dark web. Medical records can't simply be canceled like a stolen credit card, after all.

To gain unauthorized access to patient medical records and administrative networks, skilled adversaries are deploying highly targeted phishing and spear-phishing campaigns that even the most aware of employees are susceptible. In fact, phishing attacks in Q2 2016 "shattered" previous records, according to the Anti-Phishing Working Group (APWG), and recorded attacks were up by more than 61 percent from the previous quarter.

Around the world, the cybersecurity risks to the healthcare industry have proliferated in conjunction with the increase in electronic healthcare records (EHRs) and the increased adoption of Internet of Things (IoT) and mobile devices. Today, financially motivated cyber criminals use phishing and spear-phishing techniques to inject ransomware or crypto-ransomware into corporate networks. Once completed, the adversary can exfiltrate or lock down medical systems until the organization agrees to pay a ransom fee that can range from hundreds of thousands to millions of dollars.

The Scenario

A major healthcare system oversees a vast network of more than 50 primary care hospitals, specialty hospitals, emergency rooms and outpatient facilities across North America that all share patient information electronically. The system's administrators must stringently comply with HIPPA and FDA regulations, as well as embrace technical standards to ensure the integrity, confidentiality and availability of patient records and business critical applications, tools and machines. In fact U.S. law now requires all medical records be stored electronically as a means to enhance safety of patient privacy and make it easier for doctors to access and share medical images, records and reports.

But while HIPPA's Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information, the sheer volume and sophistication of attacks makes this mandate almost impossible to comply with.

Taking both compliance and the cyber threats facing the healthcare industry seriously, the company's board of directors approved investment in traditional defenses, including employee training, firewalls, anti-virus and an intrusion prevention system (IPS), which is operated by a Managed Security Services Provider (MSSP). Unfortunately, these safeguards alone were not enough to proactively defend against the onslaught of phishing attacks that now target employees on a regular basis.

The Attack

Recently, a highly realistic spear-phishing campaign targeted more than 100 employees across all 50 locations. The attack, which was positioned as an email update from the organization's human resources (HR) department, compelled readers to open a malicious .docx file that would inject crypto-ransomware code upon download. The email was titled, Important Updates to Your Account, and contained an almost perfect mockup of the email template commonly used by HR. Once the email was opened and the file was downloaded, the attackers had the opportunity to lockup important information, preventing physicians from accessing critical patient records and delaying surgery and medicine distribution, until a ransom would be paid for its release.

The attackers also took several steps to reduce suspicions from phishing-aware employees, including impersonating a familiar sender, incorporating disclaimers in the email, juggling malicious and non-malicious links in the same email, and using non-latin based text characters to disguise suspicious words.

The Response

As an IRONSCALES customer, within five minutes of the first email's arrival, an employee reported the attack as suspicious through IRONSCALES active protection Microsoft Outlook button, a one-click process to the IRONSCALES system. At this point, 67 mailboxes were affected.

Immediately, IRONSCALES automatic mitigation process was triggered, and IronTraps automatically deleted the suspicious email from all affected mailboxes and prevented the spread of the phishing attack to any other mailboxes. During the seven minutes between detection and completion of mitigation, IronTraps secured ALL mailboxes and protected ALL of the company's employees from unintentionally sharing credentials with the hackers. Ultimately, IRONSCALES completely removed the threat from all mailboxes in 12 minutes and prevented significant financial and reputational damages to the company.

The average cost of a cyber attack in the healthcare industry is $363 per medical record, more than twice the national average, according to IBM. Most importantly, remediating the attack within minutes could have also prevented a loss of life.

Here is a step by step response to the attack with and without IRONSCALES phishing mitigation solution

Without IRONSCALES

1. An employee reports s phishing attack to the SOC team, sending it to the bottom of an exhaustive list of tickets already submitted – regardless of priority.

2. Once the SOC team gets the report, they must manually perform forensic analysis and reverse engineering.

3. The SOC team attempts to pinpoint the origin and nature of the attack to figure out the best way to contain it.

4. The SOC team compiles all reported alerts in order to analyze the situation.

5. After the attack has been realized, the SOC team sends an email to all employees about the phishing event.

6. The SOC team quarantines and deletes suspected phishing emails.

7. Without machine intelligence, there are no preventative measures to ensure the same attack won't happen again.

Projected Timeline: Days to weeks

With IRONSCALES

1. Every email that arrives or that is clicked on is inspected by IronTraps.

2. With one click, an employee reports a phishing attack to the IRONSCALES system.

3. IRONSCALES' servers automatically execute to analyze the number and skill ranking of responders, Multi AV, Sandbox Scan and other proprietary analytics to determine the most appropriate response.

4. Automatic remediation is issued at the gateway and endpoints, consisting of an enterprise-wide quarantine, disabling links and attachments and remove of email, as preconfigured by the SOC team.

5. Each attack generates an intrusion signature to both the endpoints and the SIEM, ensuring a similar attack will be detected and prevented.

Projected Timeline: Minutes

IRONSCALES Automation and Awareness

Globally, phishing attacks have evolved from an occasional annoyance into a persistent epidemic. In fact, increasingly sophisticated and highly targeted phishing schemes have essentially transformed every enterprise employee into a primary threat vector. Most enterprises today are cognizant of the financial, reputational and even physical risks of phishing, however, few have modified their defenses to meet the complexity of the modern threat landscape.

IRONSCALES is the first and only automated email phishing response solution to combine human intelligence with machine learning. Our technology automatically protects enterprises in real-time from the financial, reputational and physical damages of targeted phishing attacks.

IRONSCALES ensures that employees are prepared to take an active role in protecting the integrity of their organizations, while reinforcing their efforts with machine learning technology that can automatically defend enterprises from attacks in real-time.