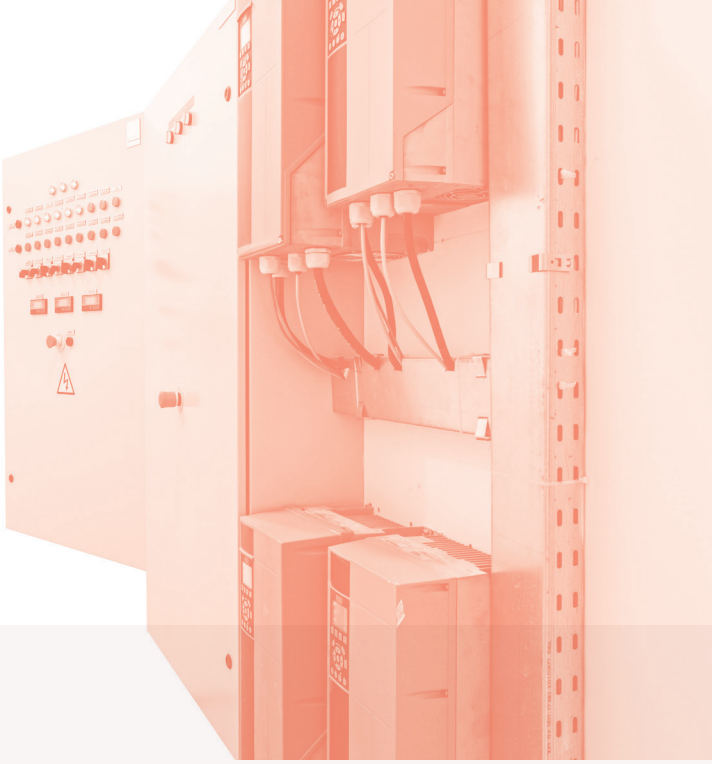
HOW AUTOMATED PHISHING RESPONSE **CAN REMEDIATE A SOPHISTICATED EMAIL PHISHING ATTACK** ON A POWER COMPANY



The increase in cyberattacks targeting critical infrastructure is gaining the world's attention. While many organizations are hesitant to report any attempted or successful breach, the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) in the United States reported a 20% uptick in attacks between 2015 and 2016. Other studies, such as the SANS 2016 State of ICS Cybersecurity report, have similar findings. Looking ahead into 2017, cybersecurity will certainly remain one of the biggest threats facing critical infrastructure.

The most popular form of cyberattack, including those targeting critical infrastructure, originate from phishing, or "the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers." This tactic is so popular, in fact, that 95% of all successful cyberattacks derive from a successful phishing campaign, according to the recent IBM Security Officer Assessment.

> Spear phishing, an advanced type of phishing in which an email or text appears to be from a colleague or business, is used in almost 40% of all attacks and is opened 70% of the time.

While spear phishing was first identified as a threat to critical infrastructure as far back as 2013, the technique has improved in sophistication and frequency in recent years - with the power industry becoming a primary target.

First discovered in 2010, Stuxnet is considered the world's first digital weapon used to target a foreign government's critical infrastructure with physician destruction as its motive. Specifically, it was designed to target ICS and as responsible for substantial damage to Iran's nuclear program. Though never confirmed, the malicious computer worm is believed to be a jointly built American- Israeli cyberweapon.

The first known time a cyberattack was successfully used against a country's power grid happened in December 2015, when a Ukrainian power company was a victim of a spear-phishing campaign - leaving 230,000 people without power for up to 6 hours. In January 2016, a successful phishing attack containing ransomware hit Israel's Electric Authority. While the damages in both cases were minimal, the events reinforce the viability of the phishing threat and just how problematic it is to an industry that remains on high alert.

Though no organization can decrease the prevalence of phishing, reducing the effectiveness of phishing is proven to minimize risk. With an automated phishing mitigation response powered by machine learning, coupled with employee awareness and training already in place, power companies have the opportunity to detect, remediate and respond to even the most sophisticated email phishing attacks in real time.

HYPOTHETICAL
USE CASE

IRONSCALES' AUTOMATED EMAIL PHISHING RESPONSE **SOLUTION** PREVENTS A NATION-WIDE POWER OUTAGE

THE SCENARIO

In the United States, a collection of electric utilities is responsible for the generation, transmission and distribution of power across the entire western part of the country. While once isolated from each other, theutilities began to interconnect over the last few decades to increase efficiencies and reduce costs. Further, with the introduction of the smart grid, the once-analog Supervisory Control and Data Acquisition (SCADA) systems and industrial control systems (ICS) have become increasingly digitally connected.

The utilities' IT personnel, responsible for attaching modern technology components to SCADA and ICS, is not tasked to manage the systems. Instead, operations technology (OT) professionals, who are primarily controls engineers and plant managers, hold this responsibility. But as IT and OT converge, it is OT workers, many of whom are on the verge of retirement and lack basic cybersecurity knowledge, who have been tasked with overseeing the digital safety of their networks and facilities.

Recognizing the vulnerabilities of its newfound connectivity, the owners and operators of the power systems implement a stringent security strategy that includes advanced phishing detection; network monitoring and anomaly detection, multi-factor authentication, firewalls and endpoint security. Additionally, all employees-from the lowest level engineer to the C-Suite-are mandated to complete phishing awareness training annually.

HYPOTHETICAL
USE CASE

IRONSCALES' AUTOMATED EMAIL PHISHING RESPONSE **SOLUTION** PREVENTS A NATION-WIDE POWER OUTAGE

THE ATTACK

In 2015, a group of patient, well-funded nation states with a political agenda began planning a strategic and targeted spear-phishing campaign on the U.S. power grid in the northeastern part of the country – with their sights set on causing chaos and disruption through blackout. Knowing that just one successful attack had the potential to shut down the country's most populous region, the motivated cybercriminals spent months developing a sophisticated and persistent attack designed to be delivered straight to the inboxes of the less than cyber-savvy engineers of the interconnected utilities.

With research complete and the targets identified, the attackers were ready to execute. The phishing email used in the attack looked almost identical to the email template used by the utilities and was addressed from the CEO of one of the power plants. The message was positioned as urgent, asking employees to take 5 minutes and visit a webpage - which was hyperlinked - to immediately change personal login controls due to unauthorized attempts at network access.

Once the email was opened and the link was clicked, the attackers would have the opportunity to access the SCADA network and enter a period of stealthy reconnaissance in an effort to find the most appropriate time to begin their attack. As such, once the network is accessed, it's very hard to find the hackers, no less get them out, until they have shown their hand – which could very well not be until an attack against the electric grid is underway. It seemed almost foolproof.

THE RESPONSE

Recognizing that the email was delivered by an unknown sender and the reply address did not match, **IronShield alerted the employee. As a result, the employee reported the attack as suspicious through IRONSCALES active protection Microsoft Outlook button, a one-click process to the IRONSCALES system.** At the time of the reporting, 125 inboxes across 5 states were affected.

In response, IRONSCALES' servers automatically executed a system-wide scan that analyzed the number and skill ranking of the responders; Multi AV and Sandbox Scan results and other proprietary analytics. **Within just 7 minutes, forensics was completed, and an intrusion signature was sent directly to endpoints, email servers and the SIEM, which then triggered an immediate and automatic mitigation response - quarantining inboxes, disabling links and attachments, and permanently removing the phishing email – even for users that were not logged in or online.** In addition, important event information was then automatically and anonymously shared with other users.

In the end, as a result of its automated email phishing response, IRONSCALES successfully remediated the spear-phishing attack targeting the U.S. power grid – preventing the significant financial, reputational and physical damages that would have resulted from shutting down power in 11 states. Further, with Federation, the phishing attack intelligence was automatically and anonymously shared with enterprises and organizations worldwide, preventing unknown and potentially unlimited damages.

IRONSCALES **AUTOMATION AND RESPONSE**

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.

An easily installed email add-on, IronTraps empowers employees to report suspicious emails with one-click on their toolbar in both Outlook and Gmail clients. The automated phishing response technology is intelligent enough to analyze the maliciousness of the threat and remove it from all employee inboxes to prevent it from spreading – all of which alleviates the burden on the SOC team. With IronTraps, each time a malicious event is detected, it remembers it, so that the same type of scam can never successfully infiltrate any other computer within the network again.

When a phishing attack is automatically detected or reported, the following sequence of events is triggered:

1. An automatic notification is sent to both the security team and IRONSCALES' servers.
2. IronTraps then automatically executes a comprehensive phishing forensic examination of the suspicious email using our integrated Multi-AV and Sandbox Scan. Working in conjunction with IRONSCALES's advanced technology, IronTraps analyzes the number and skill ranking of the reporter, in addition to other proprietary analytics, which determines the most appropriate mitigation or remediation response.
3. Once the attack is verified, an automatic remediation response is initiated consisting of an enterprise-wide removal of all malicious emails.

Complementing **IronTraps** is **Federation**, a tool that automatically and anonymously shares phishing attack intelligence with enterprises and organizations worldwide.