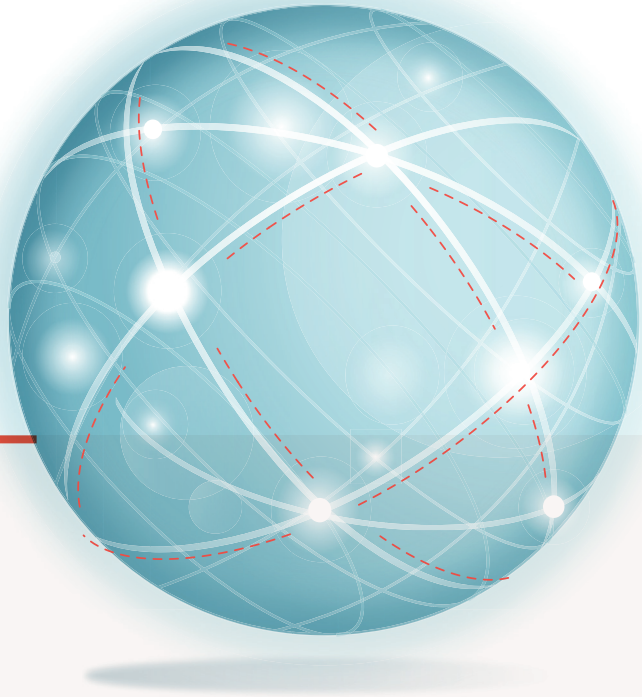
IRONSCALES' FEDERATION COMBINES HUMAN INTELLIGENCE WITH MACHINE LEARNING TO DISCOVER & STOP SPEAR-PHISHING ATTACKS



FEDERATION™

Phishing attacks have evolved in sophistication and frequency since they first originated in the 1990s when the internet reached mass-market adoption – and there's no sign of slowing down. In fact, in just the past 12 months, millions of high profile organizations, spanning all industries and sizes, and the people they employ, became targets of cyber attack.

According to a recent report, there were 400,000-phishing sites detected per month in 2016 and the Anti-Phishing Working Group concluded that phishing attacks reached an "all-time high" in Q2 2016. The phishing epidemic has become so widespread, in fact, that it recently prompted the U.S. Secretary of Homeland Security Jeh Johnson to proclaim phishing a primary threat to national security.

More effective than traditional phishing scams, spear-phishing attacks are carefully targeted with emails crafted to appear to be from a colleague at the recipient's company. The attackers are most often professional criminals that study the companies and their current projects, in addition to the technical savviness of its employees.

According to the InfoSec Institute, spear phishing emails are opened 70 percent of the time and provide ten times the return on investment (ROI). As such, spear phishing has become increasingly popular for professional cybercriminals. In fact, through extensive R&D, IRONSCALES' team of security researchers, IT and product experts, and interactive training specialists have discovered significantly more spear-phishing attempts in 2016 than traditional phishing.

To address the challenges of spear-phishing, IRONSCALES developed the first and only multi-layered automatic phishing mitigation solution to combine human intelligence with machine learning. Since 2013, IRONSCALES has been detecting and blocking advanced phishing attacks against companies worldwide. By assigning signatures to each attack and continuously learning from new phishing attempts, IRONSCALES has the ability to successfully identify and mitigate spear-phishing attacks and accurately predict targets.

The following case study is just one example of the complexity of spear-phishing email design and attack technique, how swiftly phishers move from attack to attack, and how IRONSCALES' can automatically remediate phishing and prevent repeat attacks across its clients' networks.

DISCLAIMER
To protect the integrity and privacy of all involved, company names have been removed.

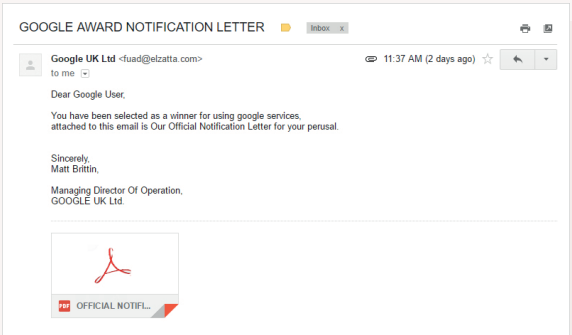
FEDERATION™

THE ATTACKS

ON MAY 16, 2016

A manufacturing company was the target of a sophisticated spearphishing attack. The email used in the attack included a malicious pdf-attachment, whose signature was not yet known to the company's anti-virus software, and impersonated Matt Brittin, president of EMEA business and operations at Google.

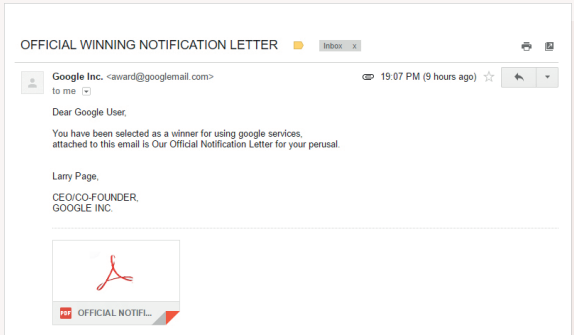
The suspicious email was reported the same day that employees received it, and IRONSCALES immediately took action in stopping the attack and removing the email from all inboxes. Attackers attempted the spear-phishing campaign again on September 18 and November 6, though IRONSCALES automatically remediated the attacks without employee intervention, at that point the attachment was still passing AV engines and other behavioral tests.



ON SEPTEMBER 22, 2016

a second wave of spear-phishing attacks reached a food processing company. Unlike the first attack, however, the email significantly changed. This particular email was designed to impersonate Larry Page, co-founder of Google and Alphabet Inc., from the address googlemail.com – which is not the domain Google uses to send official emails.

In addition, the email contained links not yet detectable by the company's existing link scanning solutions. Despite these differences, through the discovery of some common patterns, Federation, IRONSCALES' phishing intelligence sharing platform, was able to determine that the variety of spear-phishing emails were from a single source and, ultimately, the same attacker. As a result, the attack response was automatically triggered and Federation mitigated the phishing emails without any manual intervention. Just four days later, the same attack reached a company in the shipping industry and was remediated for three users.



IRONSCALES' FEDERATION COMBINES HUMAN INTELLIGENCE WITH MACHINE LEARNING TO DISCOVER & STOP SPEAR-PHISHING ATTACKS

In total, IRONSCALES remediated four spear-phishing attacks at the manufacturing company, 12 attacks at the food processing company and three attacks at the shipping company as a result of its automatic phishing remediation solution and its email phishing intelligence.

To learn more about how IRONSCALES users can gain unprecedented email phishing intelligence in real-time on dangerous and destructive phishing attacks, **request a demo** of Federation today.

IRONSCALES is the world's first and only anti-email phishing technology to combine human intelligence with machine learning. Our suite of technologies work together to prevent, detect and respond automatically to today's sophisticated email phishing attacks using a multi-layered and automated approach.

Headquartered in Tel Aviv, Israel, IRONSCALES was founded by a team of security researchers, IT and penetration testing experts, as well as specialists in the field of effective interactive training, in response to the increasing phishing epidemic that today costs companies millions of dollars annually. It was incubated in the 8200 EISP, the top program for cyber security ventures, founded by alumni of the Israel Defense Forces' elite Intelligence Technology unit.