New IRONSCALES Research Finds Microsoft ATP Takes Up to 250 Days to Create Phishing Attack Signatures

Office 365 Advanced Threat Protection not keeping up with speed of email phishing threats; Study also concludes that half of all email phishing attacks worldwide now impact more than 25 organizations

TEL AVIV, Israel and ATLANTA (PRWEB) September 17, 2019 -- IRONSCALES, the world’s first automated phishing prevention, detection and response platform, today revealed that Microsoft Office 365 Advanced Threat Protection (ATP), the primary email security filtering service for Office 365 users, can take up to 250 days to create an email phishing attack signature and make it available to enterprise technical staff. Over the course of three months, a representative sample size of 1000 malicious emails containing links or attachments found that ATP took between 6 and 250 days from the time an email phishing attack was first reported until the time that a signature was deployed.

Additionally, within this same 250-day time period, identical phishing emails were resent up to 77 times to various recipients within the same organization. This delay in signature creation leaves Office 365’s 60 million monthly users at severe risk of malicious email phishing messages impacting business continuity - as it now takes less than 82 seconds for a phishing email to lure a click.

“It’s frustrating to learn that ATP seems to lack the sense of urgency that phishing mitigation requires in today’s email threat landscape,” said Eyal Benishti, Founder & CEO of IRONSCALES. “As the main cybersecurity safeguard for millions of people, ATP must prioritize phishing attack signatures to limit risk or be more transparent with their users about the need for additional email security to serve as an additional line of defense. When combining this slow response time with the fact that ATP cannot stop business email compromise and the onslaught of fake O365 login pages harvesting users’ credentials, users must begin to ask tough questions about just how much ATP is actually reducing their risk.”

IRONSCALES’ research also found that attackers are gaining unprecedented leverage over their organizational targets. Currently, for every uniquely identified email phishing attack:

- 50% now affect more than 25 organizations worldwide
- 20% now affect more than 40 organizations worldwide
- 10% now affect more than 55 organizations worldwide
- 5% now affect more than 65 organizations worldwide
- 2% now affect more than 100 organizations worldwide

In addition, attackers now target between two and 40 mailboxes per company impacted by an email phishing attack, IRONSCALES research concluded. Earlier this year, IRONSCALES research also determined that 42% of all phishing attacks are polymorphic.

How IRONSCALES mailbox-level security “sees” attacks post ATP

Unlike other anti-phishing technologies, IRONSCALES is installed post gateway, inside of the mailbox. This mailbox-level view provides unprecedented visibility into the emails that bypass secure email gateways (SEG) such as ATP, including insight into the sender’s true identity and the data and metadata extracted from
previously trusted communications. As such, IRONSCALES can identify which attacks bypass ATP and how long it takes to create a new signature for each new threat.

Once attacks are verified, IRONSCALES can automatically make remediation decisions in real-time based on threat intelligence and the considerations of human security members within its virtual analyst community. Using advanced AI incident response to purge emails that bypass ATP, IRONSCALES automatically remediates 70% of all phishing attacks within just 82 seconds. This unprecedented speed from threat identification to enterprise wide remediation not only reduces the risk of employees clicking on malicious messages, but also enables SOC and security teams to better predict how the next phishing attack will look.

For more information, download our eBook: Office 365 ATP is Not Built to Defend Against Modern Real-World Email Threats, visit www.ironscales.com and follow @IRONSCALES.

About IRONSCALES

IRONSCALES is the leader in anti-email phishing technologies. Using a multi-layered and automated approach starting at the mailbox-level to prevent, detect and respond to today’s sophisticated email phishing attacks, IRONSCALES expedites the time from phishing attack discovery to enterprise-wide remediation, reducing the time from detection to response from hours or days to just seconds or minutes, by significantly reducing the workload on incident responders. 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 phishing epidemic that today costs companies millions of dollars annually. It was incubated at the 8200 EISP, the top program for cyber security ventures, founded by alumni of the Israel Defense Forces’ elite Intelligence Technology unit.
Contact Information
Evan Goldberg
ARPR
8553008209

Online Web 2.0 Version
You can read the online version of this press release here.