IRONSCALES
SAFER TOGETHER

IRONSCALES THREAT INDEX

Q3 2023 Edition

BEC Attacks Continue to Grow

23% Increase

BEC attempts increased by 23% from Q2 2022 to Q2 2023.

Despite increased awareness, the scourge of BEC continued largely unabated over the past year.

24% Increase

Advanced email attacks increased by 24% in the last year.

The threat of advanced email attacks continues to rise at a dizzying pace, increasing by 24% in the past year, and organizations are struggling to keep up. Threat actors are now adopting new strategies designed to evade traditional defenses.

Novel Strategies Struggle to Avoid Improved Defenses

73%

BEC attacks using **"Senders with Multiple Display Names"** rose by 73% from Q1 to Q3 2023.

What is it?

Attackers use "Senders with Multiple Display Names" to target entire organizations without alerting traditional security tools.

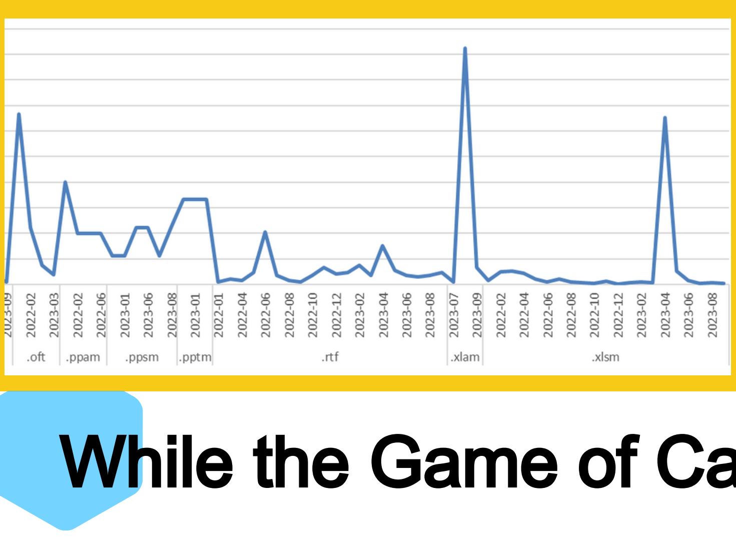
How?

Despite being sent from the same address, malicious emails display different names in the "From" field for different recipients, creating the illusion that they're from different senders.

Malicious Payloads Lose Steam

For decades, malicious attachments and hyperlinks have served as the tip of the spear for email-based cyberattacks. And for just as many years, threat actors and security vendors have been locked in a perpetual game of cat and mouse.

First party data shows a dramatic increase in xlms and xlam file-types this summer, where earlier in the year, the .oft and .odt file types saw more attacks.



This summer, we saw a 37x increase in xlam and xlms file types used as malicious payloads.

But, just earlier this year, **.oft and .odt file types saw the most dramatic growth in malicious use.** Every year, we see novel classes of malicious payloads emerge, surge, then sink into disuse; only for the cycle to start all over again.

While the Game of Cat and Mouse Continues, Fewer Threat Actors are Choosing to Participate.

Over the past two quarters, **the overall volume of attacks containing malicious payloads (i.e. dangerous links or attachments) has begun to decrease precipitously,** more than doubling in its rate of decline from one quarter to the next.

22% Decrease

From Q3 to Q4 2022, malicious payload attacks decreased by 22%.

47% Decrease

From Q1 to Q2 2023, malicious payload attacks decreased by 47%.

AI Ushers in a Golden Age of Social Engineering

Threat actors are turning to cutting-edge tools to better execute a timeless approach.

8 Million Phishing Attempts

The number of phishing attempts IRONSCALES stopped that successfully evaded native defenses in 2022.

88% Classified as Unknown

Of those 8 million messages, nearly 88% were classified as unknown threats — advanced phishing attacks that forego malicious payloads in favor of well-polished social engineering strategies, enabled by AI.

Standard email security tools have gotten better at identifying malicious payloads. Including a malware attachment or a link to a phishing webpage in an email is a surefire way to get swept up by today's standard defenses.

At the same time, generative AI has given hackers the ultimate tool for social engineering at scale. With programs like FraudGPT, they can now create infinitely more polished, sophisticated, and convincing social engineering attacks — in a fraction of the time.

Ready to Experience the Power of Generative AI Email Security with IRONSCALES?

GET A DEMO

Stop Phishing
Dead in its Tracks.

IRONSCALES is the industry's only AI and human insights enterprise email security solution protecting 10,000 global customers.