Businesses often deploy individualized security solutions for their email defenses, causing visibility gaps and incomplete risk management. How XDR Tackles The Challenge of Email Security Risks

First, the attacker gains access to a senior leader’s email account, typically a C-suite or member of the Board, and uses it to arrange virtual meetings with employees. During the meeting, the scammer displays a static image of the senior leader or uses deep fake audio to claim legitimacy.

The Nigerian Prince Scam

The Nigerian Prince scam began as early as the 1980s through postal mail but transitioned to email in the early 2000s. Scammers claimed to be Nigerian royalty and would be operating with less-than-usual staff. Given the high concentration of employees being away on vacation, attackers could increase their fraud. As their scheme became more elaborate, they solicited money with the promise of a large inheritance.

There are two variations of BEC scams involving cryptocurrency: direct transfers to a crypto exchange (CE) that is similar to traditional BEC schemes and a threshold to a wider spectrum of cybercriminals. Such spin-off AI tools are making BEC attacks more accessible by lowering the entry threshold to a wider spectrum of cybercriminals.

Attacks like these feature a complex combination of both AiTM and BEC tactics. In one scenario, attackers leverage the popularity of generative AI solutions like ChatGPT to create improved phishing emails that look like they come from legitimate sources. Such emails are crafted to look authentic and easy to believe, making them a formidable threat.

Executive Impersonation

– In these attacks, scammers posed as potential customers or clients and contacted businesses regarding overpayment scams or lottery and inheritance scams. The scammer might claim to be a supplier who needs to pay a purchase order or to be a lottery winner whose prize requires a small fee. They might also pose as the CEO of a company and ask employees to transfer funds, posing as legitimate requests.

– Early instances of executive impersonation involved scammers pretending to be high-ranking executives or directors to request personal financial information. They might ask for sensitive information, under the guise of confidentiality or urgency.

The IC3 has also classified the threat of BEC as one of the leading categories of cybercrime by financial losses. In 2022, the IC3 saw a rise in email-based attacks, where scammers compromised personal, financial, or professional information.

As technology evolves, so do the tactics employed by cybercriminals. While phishing became more sophisticated, the risk to businesses has remained high. This has prompted businesses to explore multi-technology solutions like XDR (Xtreme Defense Realm), which combines multiple security tools and can provide a more comprehensive approach to email security.

Conclusion

SentinelOne has invested to fulfill the potential of comprehensive threat detection and response. It doesn’t merely focus on endpoint activity but delves into the context of activities and first seen circulating in darknet forums. Such spin-off AI tools are making BEC attacks more accessible by lowering the entry threshold to a wider spectrum of cybercriminals.

Requirement for XDR

XDR solutions, when coupled with email security, offer an additional layer of protection beyond the limitations of isolated solutions. By leveraging multiple technologies and integration points, XDR can provide a more effective and streamlined approach to detecting and responding to threats. It is particularly useful in email security, where threats can be more subtle and difficult to detect.

Understanding The Evolution of Modern Business Email Compromise Attacks

Current Top Trends In Business Email Compromise Attacks

In the early 2000s, the world saw some of the earliest phases of BEC scams take form. While the term “BEC” might not have been coined until later, the concept of business email compromise had already begun to emerge. At that time, traditional phishing scams, involving emails that trick users into clicking on malicious links or attachments, were the primary method of attack.

With the advent of new technologies and changes in how businesses operate, BEC attacks have evolved. More sophisticated tactics, such as the use of advanced social engineering and AI tools, have become commonplace. These developments have made BEC attacks more difficult for businesses to detect and respond to.

The fusion of XDR technologies with email security offers a more effective approach to detecting and responding to threats. By leveraging multiple security tools and integration points, XDR can provide a more comprehensive approach to email security.