SPOTLIGHT

Sponsored by: Group-IB

This IDC Spotlight examines why email security is often the weakest link in an organization's cyberdefense strategy. It will discuss the common threats posed by email-based attacks, such as phishing and malware. The report will also provide actionable strategies for enhancing email security to prevent attackers from gaining a foothold in corporate networks.

"The Weakest Link" — Email Security Should Be Your Top Cyberdefense Priority

November 2024

Written by: Shilpi Handa, Associate Research Director, Cybersecurity, IDC

Navigating the Evolving Email Threat Landscape

Every business today relies on email communication daily, making it an indispensable channel for corporate interactions. Owing in part to its ubiquity, email remains a prime target for cybercriminals, exploited through various sophisticated methods. Since the widespread adoption of email in the mid-to-late 1990s, numerous technological advancements have been made to secure email communications. However, it consistently ranks as a leading threat vector in annual studies. According to the Federal Bureau of Investigation's 2023 Internet Crime Report, phishing and spoofing were the most reported internet crimes, with nearly 300,000 complaints and losses exceeding $18.7 million.[1] Business email compromise (BEC) incidents resulted in the second-highest financial losses, at over $2.9 billion.

Historically, BEC and phishing attacks have led to substantial financial damage worldwide. Noteworthy incidents include the 2021 Crelan Bank BEC scam, where fraudsters masqueraded as executives to embezzle €70 million, and the 2020 Twitter breach, where social engineering facilitated a cryptocurrency scam using high-profile accounts.[2] Other significant breaches, such as those affecting Ubiquiti Networks, Facebook, Google, and FACC, underscore the urgent need for stringent email security protocols and comprehensive employee training to mitigate such risks. In 2022, the U.S. city of Lexington, Kentucky, fell victim to a phishing scam, losing over $4 million. More recently, in 2024, Orion, a chemical manufacturing company, disclosed a $60 million loss due to a BEC scam.[3]

Given the significant impact of these scams, the importance of preventing email security compromises cannot be overstated, as they often serve as gateways to broader security breaches, leading to substantial data and financial losses. According to IDC's *Future Enterprise Resiliency and Spending (FERS) Survey, 2023,*[4] approximately one-third of all ransomware attacks begin with phishing emails, while nearly 40% of supply chain attacks in Asia/Pacific and 25% in North America were linked to phishing. The survey also highlighted that within large organizations (those with over 10,000 employees), phishing attacks are the most reported incident.

A staggering one-third of all ransomware attacks start with just a simple click on a phishing email!

The advent of AI has introduced an effective new tool for cybercriminals, making phishing and spoofing attacks more sophisticated. The potential of generative AI (GenAI) to enhance phishing campaigns has been recognized for some time, with OpenAI's ChatGPT notably increasing the sophistication and effectiveness of phishing emails and greatly reducing attack times. This has even been documented in a white paper titled "Turing in a Box."[5] GenAI tools facilitate the creation of highly personalized, grammatically correct content that is adaptable to various languages and contexts. These tools also streamline the collection of open-source intelligence (OSINT), gathering detailed information about targets, including personal preferences and company data.

The ongoing challenge of email security is exacerbated by the continued use of insufficiently advanced security methods and the difficulty in training individuals to recognize and resist sophisticated phishing and social engineering tactics. As email is the primary access point to sensitive information and critical systems, maintaining robust email security is crucial in safeguarding against data breaches, malware infections, and other cyberthreats.

Ingredients of a Powerful Email Security Solution

Redefining Email Security

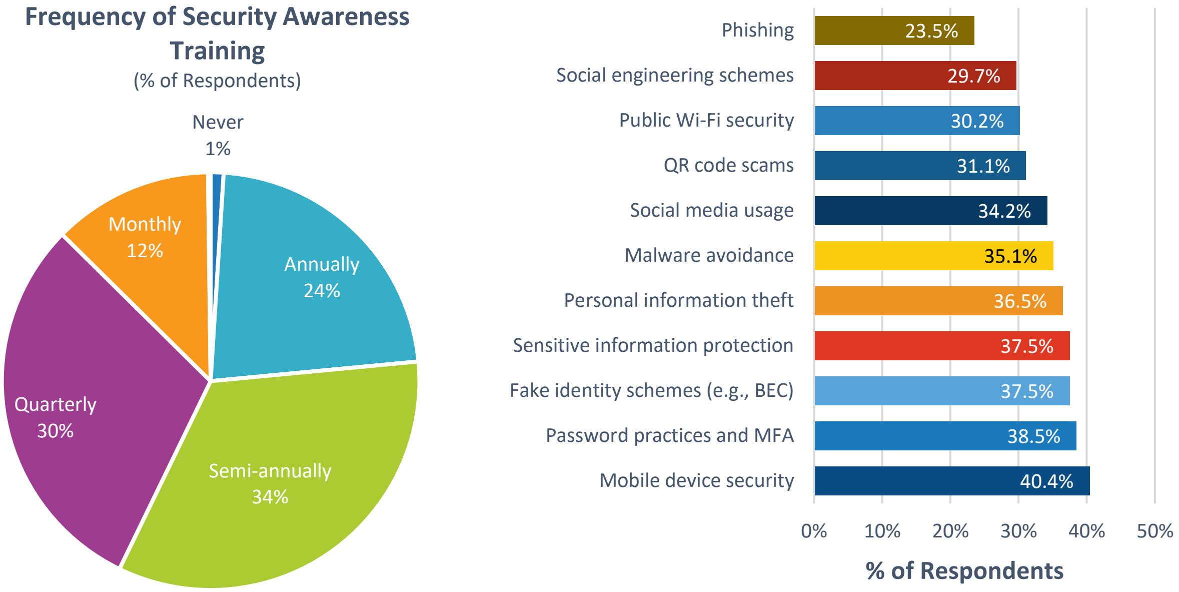
In the evolving landscape of cyberthreats, traditional email security solutions often fall short in effectively countering "weaponized" email attacks, such as those involving data stealers within advanced persistent threat (APT) campaigns. These insidious attacks, which cleverly deliver malicious beacons, links, and files through emails, account for approximately 20% of all email-based threats.[6] Conventional email security protocols typically lack the advanced detection capabilities required to identify and neutralize these complex threats, leaving organizations vulnerable to significant data breaches and espionage activities. In 2024, Microsoft disclosed a significant breach of its corporate systems by a nation-state attack using advanced email tactics, leading to the unauthorized access and theft of emails and attachments from high-ranking executives, as well as personnel within the company's cybersecurity and legal teams.[7] This incident underscores the sophisticated nature of APTs, which continue to challenge even the most robust security infrastructures.

Another area where traditional email security often falls short is encrypted archives sent via email. Security administrators frequently underestimate the threat posed by these archives. Conventional security protocols tend to block these encrypted files, dismissing them as false positives. This leads to a precarious situation where users assume the legitimacy of these emails and petition administrators to whitelist them, inadvertently circumventing established security measures and opening the doors to potential cyberthreats. In March 2024, a phishing campaign was uncovered that was designed to mimic a bank payment notification.[8] This deceptive email was aimed at enticing recipients to open an attached archive file, exemplifying the tactics employed in email archive attacks.

In such cases, the use of dynamic execution and sandboxing technology is essential for ensuring the meticulous examination of encrypted archives in a secure, isolated virtual setting. This method ensures a comprehensive analysis and the safe delivery of files, effectively countering the risks posed by malicious encrypted archives. The threat posed by APTs and email archives is multiplied by human error and inadequate training. An IDC endpoint security study revealed that only 42% of organizations conduct frequent security training, indicating a gap in consistent training.[9] Moreover, the prioritization of BEC and phishing training often falls behind due to the multitude of campaigns organizations must run annually. Despite the efforts made around security training, its effectiveness remains hard to quantify, underscoring the indispensable role of advanced email security solutions.

Together these challenges and incidents highlight the pervasive threat posed by APTs and email archive attacks, underscoring the need for heightened vigilance and advanced security measures to protect sensitive information against these sophisticated cyberthreats. As such, it is imperative for organizations to adopt an advanced email security solution that is effective at identifying, analyzing, and neutralizing the APTs that conventional email security solutions often overlook, including the intricate behaviors of data stealers and other advanced malware types.

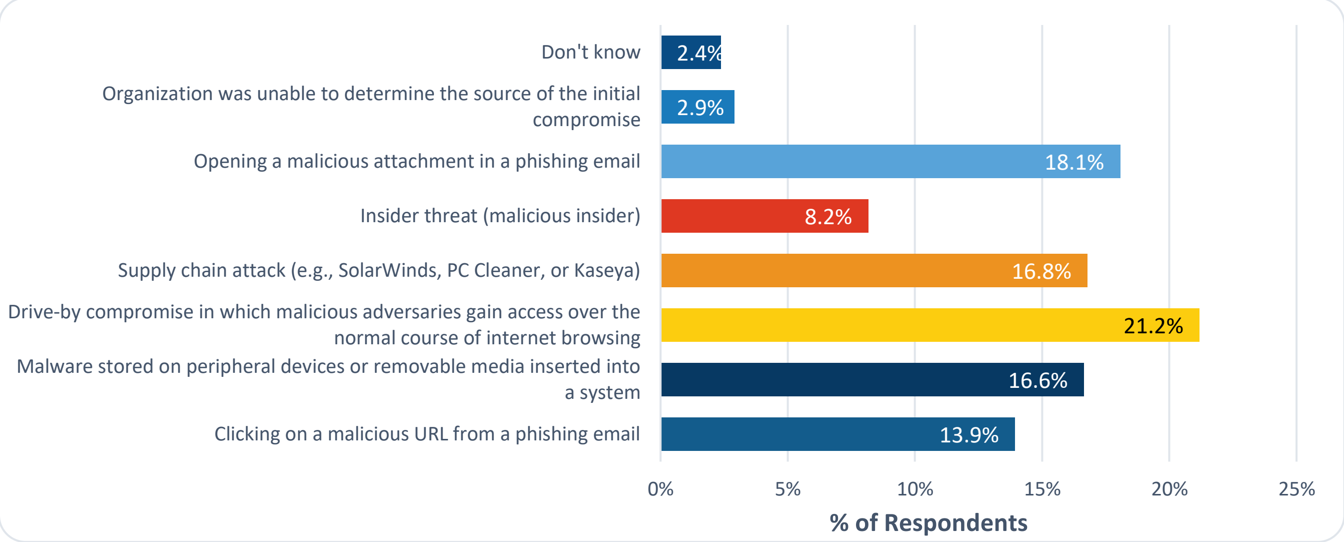
Figure 1: Frequency and Topics of Security Awareness Training Among Global Organizations



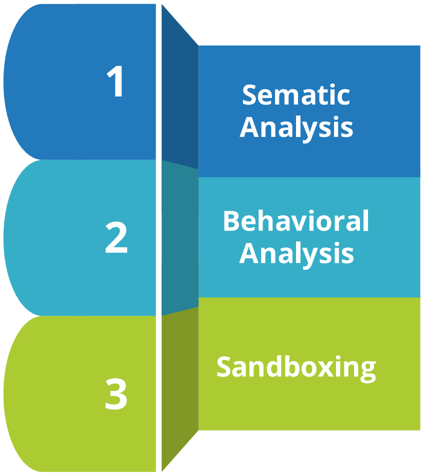
Source: IDC's *Endpoint Security Survey*, December 2022 (n = 1,015)

Though email security solutions are available in numerous flavors, focusing on some advanced techniques can provide better protection against BEC attacks. One critical technique is semantic analysis, which delves into the intent behind messages by utilizing a comprehensive understanding of the meanings of words, phrases, and sentences within their specific contexts. Utilizing semantic analysis can fortify defenses against meticulously engineered phishing attacks.

Figure 2: Most Prevalent Threat Types Among Global Organizations



Source: IDC's *FERS Survey, 2023, Wave 3* (n = 952)



Additionally, behavioral analytics plays a crucial role in identifying potential security threats by monitoring anomalous activities. This involves analyzing a wide array of data, including sender and recipient details, email headers, embedded images, URLs, and attachments, to detect unusual patterns or inconsistencies. Email attachments represent a popular vector for cyber intrusions and must be rigorously scrutinized for threats. In IDC's *FERS Survey, 2023* "opening a malicious attachment in a phishing email" was identified as the second-most prevalent method of compromise among global organizations.[8]

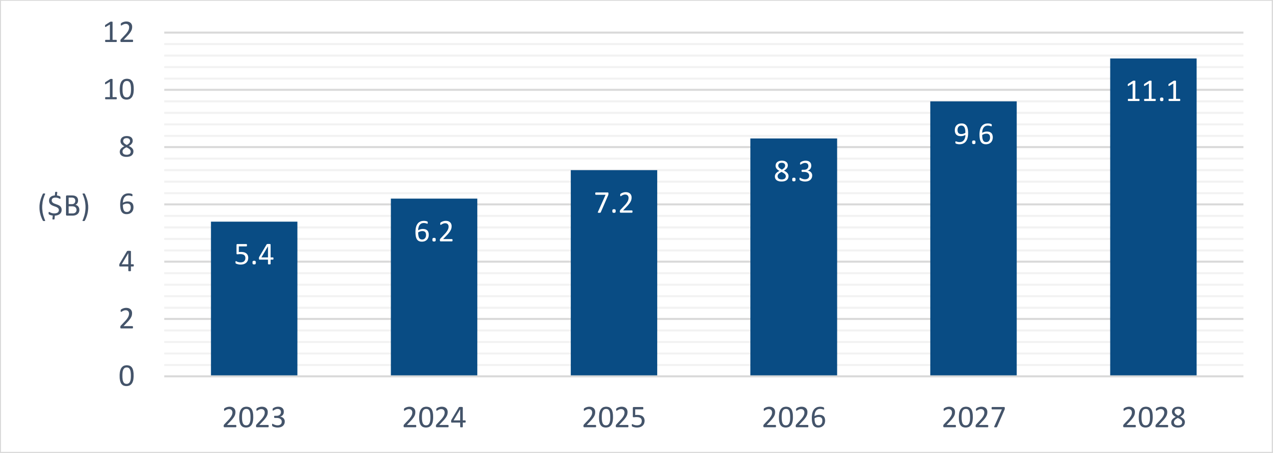
To mitigate these risks, the implementation of email sandboxing is essential, especially for defending against zero-day threats and unverified senders, as it quarantines and neutralizes threats within a secure environment before they can cause harm. Sandboxing, a cornerstone of advanced threat protection, offers an additional security layer by isolating and analyzing emails that bypass initial filters yet contain suspicious elements, such as unknown URLs or file types from unknown sources, meticulously testing them to identify potential threats prior to them being delivered to users' inboxes. This process ensures that potentially harmful emails are scrutinized before they can impact your network or mail server, thereby enhancing your organization's overall email security posture. Moreover, it contributes significantly to data breach prevention by mitigating the risks associated with phishing attacks, where employees might inadvertently compromise their account credentials.

Importance of "Right Selection"

Current Email Security Maturity

Email security has been a critical component of technology infrastructure for many years, and IDC forecasts that worldwide spending on messaging security software will increase at a compound annual growth rate (CAGR) of 15.6% over the 2023–2028 period to reach $11.1 billion in 2028.[9]

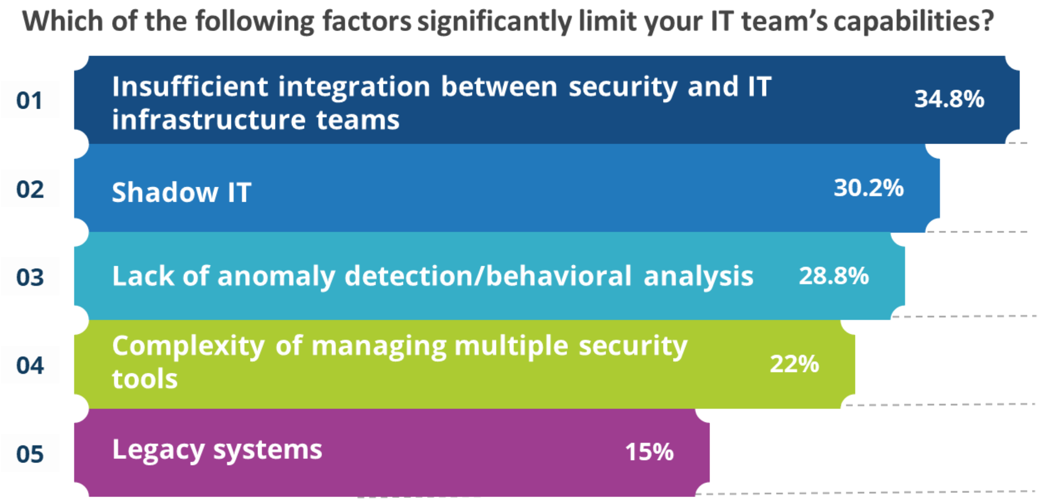
Figure 3: Messaging Security Software Market Size ($B)



Source: IDC's *Security Spending Guide*, August 2024

This data underscores the existence of a robust market for email security solutions. Nevertheless, many organizations still lack advanced email security technologies, contributing to the surge in sophisticated BEC and phishing attacks. The absence of cutting-edge security measures significantly hampers an organization's ability to bolster its IT capabilities, as highlighted in a 2024 IDC study where a "lack of anomaly detection and behavioral analysis" was cited by almost one-third of the respondents.[10]

Figure 4: IT Team Difficulties



Source: IDC's *Worldwide Security Survey, 2023* (n = 900)

Selecting the Right Tool

In today's market, organizations have access to three primary types of email security solutions, each catering to different security needs and operational frameworks. The first category is the secure email gateway (SEG), which monitors both inbound and outbound emails. SEGs are versatile, available as on-premises appliances, virtual appliances, or cloud services. They operate by processing and filtering Simple Mail Transfer Protocol (SMTP) traffic, necessitating organizations to redirect their mail exchange (MX) record toward the SEG for comprehensive email traffic management.

The second category encompasses secure cloud email gateway solutions, which boast integrated cloud capabilities. Unlike traditional SEGs, these solutions leverage application programming interface (API) access to cloud email providers, allowing for the analysis of email content without altering the MX record. Initially designed to complement existing gateway solutions, secure cloud email gateways are swiftly gaining traction as the primary choice for email security due to their seamless integration and enhanced flexibility.

Lastly, email data protection services offer an additional layer of security by encrypting emails to track and safeguard against unauthorized access, both before and after emails are dispatched. This capability is crucial for organizations looking to protect sensitive information and ensure compliance with data protection regulations.

Selecting among these solutions largely depends on the specific use case, operational requirements, and security objectives of an organization. Each type offers unique advantages; however, advanced capabilities must be evaluated when selecting an email security solution, as these can significantly reduce the threat of BEC or phishing attacks succeeding.

- **Advanced Analysis Techniques:** Utilizing behavioral analysis through sandboxing technology allows email security solutions to examine attachments and links in a secure, isolated setting. This real-time monitoring of behavior identifies and neutralizes malicious content, ensuring proactive threat management. Additionally, the capacity for retrospective analysis enables the tracing of threat origins and evolutions by re-evaluating emails when initial malware neutralization efforts falter. This ensures the ability to issue alerts and eliminate harmful emails from inboxes even after delivery.
- **Enhanced Threat Detection:** An ideal email security solution furnishes security teams with transparent, modifiable rules, facilitating the refinement of the threat detection process for improved precision and relevance. Moreover, the flexibility to craft and enforce bespoke security policies allows administrators to tailor controls and responses to meet the unique security demands of customers.
- **Flexible Deployment Options:** A multitenant architecture is important for managed service providers and large enterprises, supporting the segregated operation for various customers or departments on a single platform to uphold data integrity and security. The availability of both cloud-based and on-premises deployment alternatives ensures scalability and flexibility, supporting diverse infrastructure and security needs. Effortless integration with major cloud services, such as Microsoft and Google, via robust APIs, is crucial for a seamless security management experience.
- **Robust Threat Intelligence:** The integration of continuously updated threat intelligence feeds significantly bolsters the solution, providing immediate insights into emerging threats, vulnerabilities, and attack vectors to enhance detection and response efforts.
- **Comprehensive Additional Capabilities:** Implementing advanced filtering mechanisms to intercept and block spam emails is essential, reducing the influx of unwanted messages and diminishing the risk of email-based threats. The deployment of sophisticated techniques to identify and counteract phishing attempts is likewise imperative. The solution must shield users from deceptive emails and websites by pinpointing and blocking dubious content and links, thereby protecting sensitive information.

Figure 5: Components of an Advanced Email Security Solution

Advanced Analysis Techniques

Enhanced Threat Detection

Flexible Deployment Options

Robust Threat Intelligence

Comprehensive Additional Capabilities

Source: IDC Analyst Opinion

Email Security Best Practices

A comprehensive approach to email security requires more than just implementing a robust email security solution. Several additional components play a pivotal role in fortifying your organization's defenses:

- **Strong Password Policy:** Instituting a policy that mandates the use of long, complex, and unique passwords or passphrases, which are regularly updated, is fundamental. This simple step ensures that access to email accounts is tightly controlled.
- **Multifactor Authentication (MFA):** Implementing MFA adds an essential layer of security, particularly in instances where passwords may be compromised. This practice significantly reduces the risk of account breaches, helping to safeguard sensitive information.
- **Employee Security Awareness Training:** Recognizing that employees are both the primary defense mechanism and the most significant vulnerability is key. Providing continuous**,** relevant**,** and personalized security awareness training empowers employees to recognize and mitigate potential threats, thereby reducing the likelihood of successful phishing attacks and overall security risks.
- **Public Wi-Fi Policy:** Establishing guidelines that either restrict the use of public Wi-Fi or mandate the use of VPN connections when accessing corporate resources can drastically reduce exposure to cyberthreats prevalent on public networks.
- **Email Encryption:** Adopting end-to-end encryption ensures that email messages remain confidential and secure, both in transit and in storage. This practice is vital for protecting sensitive communications from unauthorized access.
- **Access-Level Management:** Applying principles such as "least privilege" and "need to know" in access policies helps minimize potential internal threats. Careful management of administrative email permissions and prompt deactivation of email accounts upon employee departure are critical measures to prevent unauthorized data access.
- **Patching Software and Applications:** Maintaining up-to-date software and applications through regular patching is essential. Outdated technology lacks the latest cybersecurity defenses, leaving systems vulnerable to attacks. Ensuring that email-related software and plug-ins are current is particularly important to prevent security breaches.

By integrating these and many other standard practices into your organization's email security strategy can significantly enhance its defense against a wide array of cyberthreats, ensuring a more secure and resilient digital environment.

Considering Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies designed to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its capabilities to protect people and businesses and to support law enforcement operations.

At the core of Group-IB's success lies its commitment to technological innovation. The company's next-generation Unified Risk Platform offers a holistic cybersecurity framework that combines cyberthreat intelligence, digital risk protection, threat detection and response, attack surface management, and fraud prevention. The platform allows businesses to proactively defend their critical infrastructure from cyberattacks while continuously monitoring for suspicious activity.

Furthermore, Group-IB's full-cycle incident response and investigation capabilities have consistently elevated industry standards. The company's track record includes over 77,000+ hours of cybersecurity incident response completed by its DFIR Laboratory, more than 1,550 investigation cases solved by its High-Tech Crime Investigations Department, and CERT-GIB's round-the-clock efforts.

Group-IB Business Email Protection

Business Email Protection (BEP) by Group-IB is a cutting-edge solution designed to safeguard organizations from email-borne threats such as spam, phishing, business email compromise, and sophisticated malware attacks. As email continues to be a primary attack vector, BEP offers advanced protection by using AI-driven threat detection, behavioral analytics, and threat intelligence to block email threats in real time and safeguard critical business operations.

Business Email Protection uses machine learning algorithms to analyze attachments, links, and message content for malicious behavior, going beyond what traditional sandboxes can do when it comes to assessing both intent and context. The precise detection effectively blocks all malicious emails and, as an added advantage, maintains an exceptionally low false positives rate.

Business Email Protection is further enhanced with its customizable Malware Detonation Platform. The advanced sandbox environment inspects attachments and links across more than **500 different file formats and extensions** and conducts real-time analysis to detect both mass campaigns and complex targeted attacks. Detailed reports provide security teams with process trees, indicators of compromise, network activity dumps, and in-depth behavioral analysis.

Group-IB Business Email Protection can be integrated quickly and seamlessly within existing security infrastructures — whether in the cloud, on premises, or in a hybrid format. Its flexibility allows organizations of all sizes to tailor the solution to their specific needs.

Key Technological Differentiators

By isolating potentially harmful content before it reaches user inboxes, Business Email Protection by Group-IB proactively neutralizes threats, preventing business communications from being exploited in sophisticated business compromise attacks. Thanks to its many innovative features, the solution can detect highly elusive malware behavior, such as that used by data stealers and APTs.

Advanced Defense: Outsmarting Evasive Threats in Business Email

Business Email Protection uses various anti-evasion techniques to detect and stop malware designed to bypass traditional lines of defense. Unlike conventional solutions that merely block password-protected archives, Group-IB Business Email Protection extracts passwords from email content, attachments, related emails, or even other archives and analyzes the archive contents within a secure virtual environment. Such an approach ensures that only safe files reach users, preventing human error from compromising the organization.

Automated Intelligence: A Built-In Anti-Phishing Expert

Business Email Protection handles advanced URL analysis by simulating real user behavior, opening web pages, rendering them in a browser, and navigating through links to detect hidden malware. If new threats are discovered after an email has been delivered, Business Email Protection can **retrospectively analyze** and remove malicious emails from inboxes, reducing post-delivery risks.

Realistic Virtual Environments: Adaptive Malware Detonation

A distinctive feature of Business Email Protection is its use of realistic virtual machines for malware detonation. Virtual machines closely mimic real computers, making it difficult for malware to detect and evade the sandboxing environment. If the initial analysis lacks sufficient information about a file, Business Email Protection automatically adapts the execution environment until the file reveals its malicious behavior.

Next-Gen Web Interface

Business Email Protection combines advanced detection capabilities with an efficient mechanism for manual investigation through a user-focused interface. Developed with first-hand feedback from cyber investigators and digital forensics experts, the interactive web interface has been recognized with the prestigious Red Dot Design Award for its intuitive and innovative design.

The Power of the Ecosystem

As part of managed extended detection and response (MXDR), Business Email Protection can be easily combined with other Group-IB solutions to provide comprehensive protection across multiple attack vectors. With Group-IB Business Email Protection, organizations can protect their email systems against tailored threats, prevent data breaches, reduce financial risk, and ensure business continuity. The integration with MXDR further strengthens the platform's capabilities, making it a comprehensive and proactive solution for securing the most vulnerable access point — email.

About the Analyst

Shilpi Handa, *Associate Research Director, Cybersecurity, IDC*

Shilpi Handa is an associate research director at IDC, with responsibility for the Middle East, Türkiye, and Africa cybersecurity practice. Her core research coverage revolves around cybersecurity, with a focus on network security, cloud security, application security, and security operations.

Sources:

1. www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
2. abnormalsecurity.com/blog/most-costly-bec-attack-examples
3. www.infosecurity-magazine.com/news/manufacturing-loses-60m-bec/
4. IDC's *Future Enterprise Resiliency and Spending Longitudinal Survey*, 2023
5. i.blackhat.com/USA21/Wednesday-Handouts/US-21-Lim-Turing-in-a-Box-wp.pdf
6. securitytoday.com/articles/2022/07/30/just-why-are-so-many-cyber-breaches-due-to-human-error.aspx
7. IDC's *AP Endpoint Security Survey, 2023*
8. IDC's *Future Enterprise Resiliency and Spending (FERS) Survey, 2023*
9. IDC's *Security Spending Guide*, August 2024
10. IDC's *Worldwide Security Survey, 2023*

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.