SYGNIA

FEBRUARY 2024

ANNUAL FIELD REPORT

Executive Summary

The Sygnia annual field report is a compilation of unique insights derived from hundreds of projects spanning incident response, posture assessments, and simulated attacks carried out during 2023. The report includes notable identified trends, strategic insights cultivated through client engagements, and the most prominent tactics, techniques, and procedures employed by various threat actors. The report also includes key preventative strategies that have proven highly effective in combatting emerging threats, offering a comprehensive guide to fortify your cybersecurity defenses.

KEY FINDINGS

The field report is a compilation of findings derived from Sygnia's Incident Response, Adversarial Tactics, Enterprise Security, MXDR, Engagement Managers and Legal teams, each to be published individually in the coming weeks. Key findings include:

1. The Threat Landscape Perspective:

Sygnia's Incident Response teams identify impactful changes in ransomware strategies during the past year. Ransomware groups transitioned from encryption-oriented attacks to data exfiltration and extortion strategies, employing tactics that yield faster monetization and refining new ways to cripple organizations and pressure them into. In addition, bypassing MFA has become a common tactic as a high percentage of organizations already enforce this best-practice policy, and identity and cloud-based breaches are on the rise with new techniques used to exploit and deliver severe blows to networks globally.

2. The Attacker’s Perspective:

Sygnia’s Adversarial Tactics team shares last year’s key improvements and developments that affect threat actors’ operations and identifies the most common TTPs they have utilized within clients’ environments, noting a marked increase in the number of exploited systemic misconfigurations, and a need for innovative and effective mitigation strategies.

3. The Defender’s Perspective – Preparedness:

Sygnia’s Enterprise Security team notes a return to basics in the cybercrime community, as evidenced by the simplicity of some of 2023’s major cyberattacks. The dual challenge of SEC compliance and CISO accountability is complicating matters for organizations as new regulations are already having an impact in major incidents. The rise of AI in cybersecurity may mark a turning point in attack strategies – a reduction in the time required to execute attacks, along with an increase in their targeted capabilities.

4. The Defender’s Perspective - Detection:

Sygnia’s MXDR department notes the impact of major technological advancements, market dynamics, and user adoption in the MXDR, which will have a profound impact on the 2024 landscape as trends combine with emerging technologies that will to propel the XDR market forward.

5. The Executive Perspective:

After conducting countless tabletop exercises in 2023 Sygnia’s Engagement Managers bring their collective intelligence of the most common challenges, alleys and items that are underestimated by customers globally. They also advise executives on how to build a security team, prioritize security budget and measure the effectiveness of a cybersecurity program.

Sygnia’s Legal team identifies the three most notable emerging major topics of 2023; the CISO’s expanding role and increased liability, the SEC’s new disclosure requirements and their implications on regulatory landscape and global collaboration, and emerging trends in 3rd party-based attacks and their impact on risk management.

The annual Sygnia field report goes beyond theoretical recommendations, including practical approaches to achieving robust defense without additional technology investments. Learn how to leverage your existing security estate and assets effectively, ensuring a powerful defense against cyber threats.

Stay ahead of the curve and download this week’s report: Threat Landscape Perspective.

Annual Field Report: The Threat Landscape Perspective

Sygnia's Incident Response teams dealt with hundreds of incidents in 2023, from small-scale intrusions through complex ransom incidents to large-scale APT campaigns. Reflecting on the previous year, Sygnia concludes that the driving force of criminal cyber groups remains maximizing monetization in the face of the increasing capabilities of the average security stack, which pushes threat actors towards new capabilities and techniques to overcome the new obstacles.

SYGNIA'S KEY INSIGHTS FROM THE FIELD INCLUDE:

Changes in ransomware strategies and campaigns as ransomware groups prioritize data exfiltration in pursuit of faster monetization and using aggressive negotiation methods to pressure victim organizations into paying ransom demands.

Bypassing MFA has become a common tactic as a high percentage of organizations already enforce MFA as a best-practice – creating a layered security approach is crucial for when the MFA obstacle fails.

Identity and Cloud-Based breaches are on the rise, threat actors seizing the opportunities of unmonitored IT areas to move laterally between organizational applications and gain access to sensitive data – under the main enabler that these systems are accessible from anywhere in the world in contrast to on-premises network appliances.

WHAT WERE THE MAJOR TRENDS OF 2023?

Rise in Data-Theft Extortion Attacks

2023 saw a significant shift in the ransomware landscape as some ransomware groups shifted away from encryption in favor of data exfiltration and extortion. Non-sophisticated threat actors can carry out these data-theft attacks even if they don't have access to high quality ransomware encryptors, and traditional threat actors often opt for these low-cost intrusions rather than full blown double-extortion attacks as they require less effort and are often just as lucrative.

This shift emphasizes the need for substantial adjustments in ransomware readiness strategies. Organizing the company's sensitive data ahead of time allows for better detections if and when the data is exfiltrated and knowing what data was actually stolen enables a more informed response to ransom demands.

Aggressive Ransom Negotiation Targeting Client Trust

Threat actor ransom negotiation tactics have changed massively over the past few years. In 2023 Sygnia observed a shift in extortion tactics as threat actors repeatedly tried to exploit the trust between the business and its clients. In these cases, threat actors deliberately contact clients or publish the breach via public channels to pressure the victim into meeting the ransom demand.

This tactic is highly effective as the client is generally left wondering if the company cares enough about them to pay the threat actor and protect their information, and the victim company risks burning the trust between them and their clients, potentially losing clients if they do not respond quickly and effectively.

Handling these ransom negotiations require a robust and mature negotiation approach, avoiding common pitfalls that often result in major damage to client relations. Engaging in disaster event war-games creates a more knowledgeable and informed starting point, establishing a blueprint for handling the business dilemmas that may arise during such events.

Surge in ESXi Encryptions in Ransomware Incidents

The holy-grail of on-premises ransomware incidents, ESXi and virtualization appliances remain a lucrative fast-win target allowing threat actors to control major parts of the infrastructure from a few single locations. This is a multi-year trend as threat actors continue enhancing techniques to maximize impact and destruction with the minimum of effort. Earlier in 2023, the high-profile "ESXiArgs" ransomware campaign showcased the increased interest in virtual infrastructure amongst ransomware groups, with many using tweaked and tailored malware to hit the appliances.

While the average security stack is becoming more robust, ESXi and other virtual appliances are often left unpatched since they are often not seen as part of the network perimeter. Furthermore, visibility into ESXi activity and authentication are often blind spots in the security defense plans. ESXi appliances and other virtual appliances have thus become a great opportunity for threat actors and organizations must begin including them as part of the overall organizational security strategy.

> “MFA is a useful tool, helping prevent and/or reduce cyberattacks and protect organizational identities, however it should never be the sole basis of the organization’s security strategy.”

Overcoming the MFA Obstacles

As organizations raise the security bar by enforcing MFA as a common practice, threat actors are finding new and creative ways to bypass it. Whether it’s SIM-swapping, social engineering, or MiTM phishing-kits, threat actors are creating enhanced methods of bypassing the MFA barrier to gain access to systems and accounts.

MFA is a useful tool, helping prevent and/or reduce cyberattacks and protect organizational identities, however it should never be the sole basis of the organization’s security strategy. With the increased use of SIM-swapping and phishing kits in 2023, organizations should adopt layered approaches to security, under the assumption that a time will come when the MFA barrier will be breached.

Enhanced Targeting of Companies in the Cryptocurrency Industry

The cryptocurrency sector is witnessing a surge in the activity from both nation-state and financially motivated threat actors. Over the past year, Sygnia witnessed a notable increase in the frequency and sophistication of such incidents leading to both the exfiltration of sensitive data and the theft of large amounts of digital funds. The fact that the cryptocurrency industry is largely unregulated and holds significant monetary potential raises concerns as threat actors find it a great opportunity. To top it off, companies in the cryptocurrency sector are relatively young and their overall cybersecurity infrastructures are subsequently less mature than the average corporation.

When applied to the Cryptocurrency context, the common best practices such as enforcing MFA for funds transactions and increased security over wallet secrets in vaults are often successful in deflecting the basic intrusions completely and allow a larger timeframe to respond to the more sophisticated breaches.

Identity-Based Cyber Intrusions

With cloud-based software and SaaS applications available from anywhere in the world, Sygnia observed a subsequent rise of identity-based attacks in 2023. Threat actor strategies and tactics are shifting with the landscape and cybercriminals are increasingly aiming to takeover accounts to not only steal sensitive information but also as a means of moving laterally between applications by leveraging SSO access.

As organizations adapt to and adopt the cloud, they should configure their cloud environments in a way that limits applications and identities as much as possible, preventing unnecessary overlaps of access between them. Gaining visibility into the identities in the organization and implementing least-privilege and zero-trust principals are crucial to combatting identity-based attacks.

WHAT WILL 2024 INTRODUCE TO THE CYBER LANDSCAPE?

As we peer into 2024, we can expect threats to further shift towards the new opportunities that emerge from the advancement of IT and software solutions:

Evolution of Cloud and Identity Based Cyber-Attacks

The past years may have represented the first phase in the evolution of cloud and identity based cyber-attacks. Taking advantage of the fact the cloud is accessible from anywhere, the nature of these attacks is often relatively simple. The next step in the evolution, as we have already started to observe, will include a more sophisticated approach such as leveraging features that allow lateral movement between IaaS accounts or using the built-in encryption procedures of cloud storage resources to hold data hostage.

The role of AI in Cyber Intrusions

With AI becoming increasingly commoditized, in 2024 we will see the application of these capabilities on both the offensive and defensive side of the cyber playing field.

On the offensive side, cybercriminals will further use AI to amplify social engineering attacks, crafting sophisticated phishing emails, SMSs, deep-fakes, and other types of manipulative communication. This should impact the landscape with a rise in successful exploitation of the human factor, in account takeovers (ATO) and business email compromises (BEC), and in enhanced threat actor negotiation capabilities. Furthermore, AI and LLMs present a brand-new attack surface for threat actors to exploit – from prompt injections to the takeover of AI agents and its capabilities.

On the defensive side, we should expect to see the first real applications of AI beyond the threat intel helper applications that exist today. Enhancing day-to-day productivity and capabilities of SoC teams to cope with the number of alerts and triage both faster and in some cases even automatically.

Regulations in Cybersecurity

New cybersecurity and data-breach laws and legislation passed in the United States in the past year are starting to impact companies and organizations. 2024 will test whether and how these regulations will impact cyber-intrusions and ransom operations, forcing organizations to abide by the given set of standards. Specifically, this may affect incident containment methodologies, causing organizations to expedite response measures.

CONTRIBUTORS: Dor Fenigshtein, Noam Lifshitz, and Ori Porag

WANT TO KNOW MORE ABOUT ONE OF OUR SOLUTIONS?

As the trusted advisor and cybersecurity service provider of leading organizations worldwide, Sygnia protects the enterprise through a variety of solutions that are aligned with the current threat landscape. From OT and Cloud Security to Ransomware Readiness, our Enterprise Solutions are borne out of frontline experience and a deep understanding of the threat actor mindset.