SYGNIA

FEBRUARY 2024

SYGNIA'S ANNUAL FIELD REPORT:

THE ATTACKER'S PERSPECTIVE

The Attacker's Perspective

During the past year, Sygnia's Adversarial Tactics team participated in numerous engagements, tasked with bringing the "Attacker's Perspective" to the table. The team simulated various techniques, tactics, and procedures (TTPs) across the cyber kill chain for clients from diverse industries with identified vulnerabilities, misconfigurations, and other gaps in their defense strategies.

The Sygnia Annual Field Report: Attacker's Perspective discusses our takeaways from a year of adversarial engagements, identifies the most common and effective TTPs utilized by our teams within clients' environments, includes predictions for the coming months, and provides recommended mitigation strategies for the common contemporary techniques and systemic misconfigurations that are most often exploited today.

Sygnia notes that while the emphasis on cybersecurity has heightened due to the widespread adoption of Zero Trust principles and technologies as well as improvements in endpoint, OS and browser security, the expanding attack surface continues to introduce new opportunities for attackers.

KEY FINDINGS FROM THE FIELD INCLUDE:

The bar has been raised:

The era of ‘quick wins’ for threat actors may be over as the widespread adoption Web Application Firewalls (WAF) and Cloud Access Security Brokers (CASB) has made gaining a network foothold increasingly challenging for attackers.

Impactful improvements in endpoint and OS security:

Detection and prevention capabilities have improved due to the implementation of advanced machine learning mechanisms. Furthermore, significant improvements in operating system (OS) security, particularly in Microsoft 11, set a higher standard for operating system protection and indicate that the bar may soon go up another level. Today’s adversaries must be more creative as defenders are upping their game.

Complex and expanding attack surface creates challenges:

Attackers regularly utilize Command and Control (C2) tactics to overcome network security challenges, exploit vulnerabilities related to the integration of on-premise infrastructure and cloud environments, and make use of kernel driver vulnerabilities to disarm security solutions.

There’s more to come:

As advancements in endpoint and browser security, coupled with the widespread adoption of Zero Trust principles and technology, create significant barriers for attackers, adversaries will shift their focus towards prioritizing supply chain attacks and leveraging AI for malicious purposes. The continuously expanding and intricate attack surface also consistently presents new opportunities for adversaries, who persist in exploiting vulnerabilities in CI/CD pipelines and are poised to target AI systems with tailored cyberattacks, such as data poisoning or input attacks.

2023 TRENDS IN ADVERSARIAL TACTICS

Technological Challenges for Threat Actors – “No More ‘Quick Wins’?”

As we progress into 2024, the cybersecurity threat landscape is undergoing a notable evolution in adversarial tactics. Threat actors are grappling with heightened technological barriers, marking a departure from the era of ‘quick wins’ in cyber-attacks, where threat actors could effortlessly compromise entire environments with tools like the infamous “Mimikatz” and “Responder.”

Sygnia’s Adversarial Tactics team has encountered these significant security enhancements consistently throughout engagements. These advancements directly impact threat actors’ maneuvers within organizational ecosystems, occasionally thwarting their next steps entirely.

Infiltration Challenges

In recent years, efforts to secure organizational perimeters have escalated, with the implementation of Single Sign-On (SSO) and Multi-Factor Authentication (MFA) creating significant barriers for threat actors. Despite these measures, until early 2023, infiltration attempts were still a concern, as attackers regularly find ways to bypass controls using platforms like Evilginx (AiTM) and techniques like HTML smuggling, smishing and vishing.

However, in 2023, there was a noticeable shift in defense strategies. Security enhancements around email infrastructures and web applications, including the deployment of advanced Web Application Firewalls (WAF) and Cloud Access Security Brokers (CASB), have made initial access increasingly challenging for attackers. These advancements, coupled with the robustness of SSO and MFA, have significantly raised the difficulty for unauthorized access, thereby reducing the effectiveness and motivation of threat actors.

Endpoint Security Developments

Endpoint Detection and Response (EDR) Solutions: Detection and prevention capabilities have been enhanced through the implementation of advanced machine learning mechanisms. Nonetheless, achieving comprehensive coverage remains critical, as any security gaps can provide malicious actors with opportunities to plan their lateral movements through these unaddressed blind spots.

Microsoft Windows 11 Hardening: Windows 11, while not yet widely adopted, has enhanced its security framework, incorporating robust features like advanced application and driver control, passwordless authentication, and improved phishing defenses. These advancements significantly increase the difficulty for unauthorized access and credential harvesting, thereby fortifying the security of endpoints. Due to these enhanced security measures, attackers are likely to shift their focus towards older operating systems, which may lack these robust security features. As Windows 11 continues to evolve, its comprehensive security enhancements set a higher standard for operating system protection, though its full potential remains to be seen until it achieves broader usage.

Network Security Evolution

Proxy Solutions: Enhanced proxy categorization for malicious sites and IP addresses makes it harder to initiate unauthorized outbound communications. Despite these advancements, malicious actors are finding ways to circumvent these restrictions by utilizing Command and Control (C2) tactics over third-party applications such as Slack, Jira, GitHub, and Google Drive. These platforms, typically trusted and widely used within organizations for legitimate and essential purposes, can unwittingly serve as channels for malicious activities.

To counter this, organizations must develop a comprehensive allowlist of legitimate third-party applications, tailored to the specific needs of their users. This approach ensures that while essential tools remain accessible, the vectors for potential security breaches are minimized. The adoption and implementation of various Zero Trust solutions like CATO, Zero Networks, Zscaler, and Netskope enable enhanced segmentation and network restrictions. These measures can eliminate the concept of 'trusted' devices and users within the network, thereby minimizing opportunities for attackers to laterally move towards workstations and critical servers.

Techniques and Misconfigurations – "Adversary Perspective from The Trenches"

Throughout the past year, Sygnia's Adversarial Tactics team has encountered several technological vulnerabilities that repeatedly provided opportunities for threat actors to compromise clients' environments. This section presents the most common TTPs utilized by our teams in clients' environments and delves into how contemporary techniques and systemic misconfigurations are increasingly being exploited, necessitating innovative and effective mitigation strategies.

Hybrid Cloud Environment: The increasing adoption and expansion of hybrid setups within organizations present numerous challenges regarding the security of the expanded attack surface in hybrid environments. Moreover, a white paper that highlights several attack vectors leading to a full compromise of the organization by leveraging the AD Connect infrastructure was presented during 2023 by Dirk-jan Mollema, showcases a thorough explanation in relation to this rising risk and its threat to large organizations. While there is a noticeable trend towards securing on-premises infrastructure, Sygnia has observed a rise in vulnerabilities associated with the integration process between on-premises and cloud environments, as well as misconfigurations related to the built-in features of cloud resources. Notably, clients often maintain a default configuration of the AD Connect infrastructure, which facilitates lateral movement from on-premises environments to the cloud. **Our research**, 'Guarding the Bridge: New Attack Vectors in Azure AD Connect' has uncovered several new techniques enabling threat actors to exploit their presence on the AD Connect server to harvest credentials of users and service accounts, subsequently allowing for lateral movement and privilege escalation within cloud infrastructure.

To address this security concern, it is essential to treat related infrastructure as tier 0, adhering to Microsoft's best practices. This approach involves applying the highest level of security measures and monitoring to prevent unauthorized access and ensure the integrity of both on-premises and cloud-based systems.

BYOVD (Bring Your Own Vulnerable Driver): Although not novel, the exploitation of vulnerable drivers from trusted vendors, particularly Kernel Driver exploitation, remains prevalent and effective, particularly in Red Team engagements and by threat actors during attacks on organizations. This tactic is primarily employed to disarm security solutions, posing a significant security challenge due to the inherent trust placed in legitimate vendor drivers.

Sygnia has noted a widespread trend in which both security professionals and threat actors are exploiting these vulnerabilities, signaling a significant demand for BYOVD (Bring Your Own Vulnerability Discovery) solutions within the cybersecurity community. To successfully mask our activities and bypass EDR restrictions, Sygnia has developed a proprietary tool named "Blinding-Lights." This tool has shown high efficiency in operational scenarios, providing an innovative method to disable EDRs (Endpoint Detection and Response systems) by dynamically and statically removing kernel callbacks. The approach of the tool builds on existing repositories, such as wavestone-cdt/EDRSandblast and ch3rn0byl/CVE-2021-21551.

To effectively counteract this ongoing threat, organizations must maintain an up-to-date list of compromised drivers and regularly monitor resources like loldrivers.io for the latest information on drivers with known CVEs (Common Vulnerabilities and Exposures). Staying proactive in this manner is essential to stay ahead of potential exploits and ensure robust security measures against BYOVD challenges.

Certificate Vulnerabilities: Numerous organizations remain exposed to risks stemming from misconfigurations in Active Directory Certificate Services (ADCS), an attack vector first highlighted by SpecterOps in 2021. Despite heightened awareness, ADCS infrastructure remains a substantial attack surface, frequently resulting in "one-click compromises" of entire organizational systems.

Sygnia observed 11 key escalation techniques in ADCS, facilitated by tools like Certify/Certipy. These include:

- **ESC1 to ESC8:** Various methods exploiting certificate template misconfigurations, enabling attackers to impersonate users, modify template configurations, and abuse enrollment rights.
- **ESC9 & ESC10:** Not directly related to Certipy features, yet exploitable through the tool.
- **ESC11:** Vulnerability in RPC service to NTLM relay attacks, targeting the certificate authority's configuration.

Each technique illustrates how attackers can exploit vulnerabilities to escalate privileges within a domain, often resulting in complete control over the infrastructure. To combat this, organizations must prioritize ADCS security by adhering to best practices for monitoring and securing their infrastructure. Essential measures include regular audits, applying security patches, and enforcing strict control over certificate issuance and template configurations.

CI/CD (Continuous Integration and Continuous Delivery/Deployment) Vulnerabilities: The application security domain has become a key area of focus for organizations, largely due to the wide array of technologies now available to development teams, courtesy of cloud providers and independent companies in the Infrastructure as a Code (IaC) sector. While the security risks within CI/CD processes are complex and multifaceted, key vulnerabilities include issues related to flow control mechanisms, identity and access management, and the secure management of dependencies and third-party services. Ensuring the integrity of the pipeline process itself is also a major challenge as it can often be compromised due to inadequate access controls or insufficient security configurations.

For organizations with CI/CD pipelines that integrate multiple stages and tools, the complexity lies in securing each component - from code repositories and "build" servers to deployment environments. Challenges such as managing access rights, protecting against code injections, and ensuring the integrity of external dependencies and services are common. For example, inadequate identity and access management or poor credential hygiene can lead to unauthorized access, while insufficient flow control mechanisms might allow unvetted code to progress through the pipeline, leading to potential vulnerabilities in the deployed software.

To protect themselves, organizations must proactively address these vulnerabilities by incorporating robust security practices at every stage of the CI/CD pipeline. This includes implementing comprehensive access controls, regularly updating and auditing dependencies, ensuring secure configurations, and maintaining thorough logging and monitoring systems. By integrating these security measures, organizations can strengthen their CI/CD pipelines against a wide array of threats, ensuring the safe and secure deployment of their applications.

2024 PREDICTIONS IN ADVERSARIAL TACTICS

Threatening the Threat Actors – Obstacles for Adversaries

In the ever-evolving cybersecurity landscape, the dynamics of threat and defense continually reshape the battleground. As we enter a new era of digital security, three main topics emerge as significant disruptors for cybercriminals: the advancement of endpoint security, the reinforcement of browser security, and the strategic implementation of Zero Trust Architecture. Each of these domains has undergone substantial evolution, not only in technology but also in strategy and execution. Endpoint security has become more intelligent and responsive, browser security has been fortified against sophisticated attacks, and Zero Trust Architecture has revolutionized the fundamental approach to network security. Together, they form a triad of formidable challenges for threat actors, shifting the balance in perpetual cyber warfare and setting new standards for what constitutes a secure digital environment in the contemporary world.

Endpoint Security: Comprehensive endeavors to enhance endpoint security primarily revolve around Microsoft operating systems, encompassing both on-premises and cloud-based machines. The adoption of Windows 11 significantly raises the bar for threat actors attempting to gain initial access within an organization. This is largely due to the default activation of advanced security features like HVCI (Hypervisor-protected Code Integrity) and Credential Guard in Windows 11. These features create formidable obstacles for malicious activities such as dumping LSASS memory and loading unauthorized drivers, effectively countering BYOVD (Bring Your Own Vulnerable Driver) tactics. As a result, it becomes increasingly challenging for attackers to compromise additional machines, especially those of critical stakeholders and peers.

Browser Security: Browser security is a concern that spans multiple technological domains, encompassing endpoint, network, and identity security. This concern is particularly pronounced given the widespread adoption of SaaS solutions and the predominant use of browsers for work tasks. While a robust technological stack can somewhat mitigate these risks—leveraging AV, EDR, and ERP for endpoint security; IDS, IPS, and FW for network security; and MFA, SSO, and email relay for identity security—browsers remain prime targets for threat actors. They exploit vulnerabilities in browsers to lure victims to compromised sites, facilitate the download of malicious content, and harvest credentials and session tokens for unauthorized access to other consoles.

The emerging trend of adopting “Secure Browsers” holds promise in enhancing browser security through stricter control, regular maintenance, and enhanced isolation mechanisms.
This advancement will make it more difficult for adversaries to distribute malicious content, extract data, and perpetrate identity theft.

Zero Trust Architecture: While Zero Trust Architecture isn’t a new concept in cybersecurity, its widespread adoption and integration into organizational systems has taken time. This gradual implementation can be attributed to the complexities associated with transitioning from traditional network security models to a Zero Trust framework. Nonetheless, when properly configured within organizations, Zero Trust poses a significant challenge for threat actors.

Zero Trust not only diminishes the attack surface for common vulnerabilities like misconfigurations and exploitation of weak points but also, through its granular access controls, ensures that the impact of any breach is limited. This is because lateral movement within the network is significantly restricted. By strategically implementing Zero Trust Architecture, organizations not only erect formidable barriers to unauthorized access but also substantially reduce the likelihood of extensive damage resulting from successful penetrations.

Adversarial Opportunities - Threats from The Future

Attack Surface Expansion: Amidst the evolving cybersecurity landscape, where advanced defensive measures present new hurdles for threat actors, the expanding and intricate digital environment continually offers fresh avenues for exploitation. This constant flux presents a dual challenge: while organizations fortify their defenses, the widening attack surface creates ample opportunities for cyber threats to proliferate. Three key areas have emerged as particularly fertile grounds for exploitation including, the intricate networks of supply chain attacks, the nuanced domain of DevSecOps, and the rapidly advancing field of Artificial Intelligence (AI).

Supply Chain Attacks: As security controls and products evolve, establishing more robust defense against traditional attack methods, ‘quick wins’—such as phishing campaigns and guessed passwords—are becoming increasingly elusive. With these once-easy exploits now posing greater challenges due to enhanced security measures, threat actors are shifting their focus towards more strategic and high-value targets.

Supply chain attacks are popular today and will only increase in popularity going forward since they provide an infiltration vector into multiple organizations simultaneously, and often from a position of greater access or trust.

Supply chain attacks can exploit vulnerabilities in less secure, third-party vendor systems or software dependencies, which can then be used as conduits to compromise the primary targets. Given the interconnected nature of supply chains, a single breach can have cascading effects, potentially impacting numerous organizations at once. This maximizes an attack's impact and allows threat actors to bypass the increasingly robust security defenses of individual organizations. As a result, supply chain security will soon become a critical focus in cybersecurity, with organizations needing to enhance their vigilance and security measures not only within their own systems but across their entire network of partners and suppliers.

DevSecOps: The integration of development, security, and operations signifies a paradigm shift in how organizations approach software development and security. The trend towards DevSecOps marks a departure from traditional models where security was often an afterthought, instead embedding security considerations deeply within the development process from the outset.

The forecast for DevSecOps includes an enhanced focus on automation in security testing. Tools and practices that enable automated scanning and testing for vulnerabilities will be integrated directly into CI/CD pipeline. This not only streamlines the development process but also guarantees that security remains a continuous and integral component throughout. Furthermore, as threats evolve, there is an anticipation for DevSecOps to adopt advanced threat modeling and risk assessment techniques, thereby proactively tackling potential security issues before they arise in production environments.

The rise of infrastructure as code (IaC) is also expected to play a significant role in DevSecOps. By treating infrastructure setup and configuration as code, organizations can apply the same security and compliance checks to their infrastructure as they do to their application code. This leads to more secure and consistent deployment environments.

Moreover, the growing importance of compliance and privacy concerns, driven by regulations like General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), means DevSecOps teams will increasingly need to incorporate compliance-as-code. This entails automating compliance monitoring and reporting, ensuring that software development aligns not only with security best practices but also with legal and regulatory requirements.

However, while the move towards DevSecOps promises a more secure software development lifecycle, it also presents an evolving attack surface for malicious actors. As organizations transition to DevSecOps practices, they undergo significant changes in their workflows, tools, and infrastructure. During this transition period, security gaps may emerge due to misconfigurations, inadequate security controls, or human error. Attackers often exploit such transitional phases, targeting vulnerabilities in newly integrated tools or misconfigured automation scripts. Thus, while DevSecOps aims to enhance security, the journey towards its full implementation presents opportunities for attackers to exploit nascent security weaknesses.

AI for Adversaries: A prominent and trending topic for years, AI has gained even more exposure in recent times thanks to breakthroughs like ChatGPT, GitHub Copilot, and similar tools. These innovations are poised to significantly enhance efficiency and proficiency across numerous technological domains, including cybersecurity. As we approach 2024, we can anticipate a marked increase in the use of AI by threat actors. This includes more sophisticated phishing campaigns, advanced malware development, and accelerated vulnerability research, all completed in relatively short timeframes. Such advancements enable threat actors to pivot and upgrade their toolsets more quickly than ever before, posing new challenges for cybersecurity professionals.

One of the key concerns revolves around the dual-use nature of AI. While it is beneficial in enhancing security measures, it also serves as a potential attack vector for threat actors. They can leverage AI to automate attacks, craft phishing emails with alarming precision, and exploit vulnerabilities at unprecedented speeds. AI's capability to analyze vast amounts of data can also be misused to identify new vulnerabilities and orchestrate large-scale, sophisticated attacks across various industries.

Crucially, AI systems themselves are vulnerable to targeted cyberattacks, such as input attacks or data poisoning, which can inflict significant damage on corporate and government infrastructures. For instance, manipulating the input data to AI systems can result in critical errors in decision-making processes. Furthermore, data poisoning, involving tampering with the AI's training data, leads to flawed learning and biased outcomes. As AI becomes increasingly integral to our digital infrastructure, the need for robust defenses against these AI-targeted threats becomes paramount. This includes stringent data validation, continuous monitoring of AI systems for anomalies, and the development of AI models resilient to adversarial manipulation. As we embrace the benefits of AI in cybersecurity, preparing for and mitigating these emerging threats is essential to ensure the security and reliability of AI systems across various sectors.

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.