EXTRAHOP®

2024 CrowdStrike Threat Report

Highlights Need for Packet-Level Network Visibility

by Marianne Ousen

Cybersecurity companies have observed a steady shift in attacker TTPs over the past five years. Due to advances in endpoint security and other factors, threat actors have gradually switched from malware-based attacks to “malware-free” attacks, where they exploit compromised credentials, software vulnerabilities, trusted relationships, or weaknesses in cloud security to gain initial access.

The CrowdStrike 2024 Global Threat Report shows this transformation from malware-based attacks in full effect, with 75% of attacks observed by CrowdStrike in 2023 being “malware-free” compared with 40% in 2019.

The report also shows threat actors increasingly gravitating toward hands-on-keyboard “interactive intrusion” techniques, where they “actively execute actions on a host to accomplish their objectives” and “mimic expected user and administrative behavior, making it difficult for defenders to differentiate between legitimate user activity and a cyberattack.”

Notably, the 2024 Global Threat Report suggests that traditional cybersecurity defenses–VPNs, firewalls, IDS/IPS, secure email gateways, antivirus software, SIEMs, and even some legacy endpoint detection and response tools–are not designed to prevent or detect these increasingly sophisticated attacks techniques. Even more noteworthy, several findings from the report speak to the need for network visibility and behavioral-based network detection and response (NDR) capabilities to complement EDR tools.

Attackers Increasingly Target the "Network Periphery"

> "Threat actors have adapted to the enhanced visibility of traditional endpoint detection and response (EDR) sensors by altering their exploitation tactics for initial access and lateral movement. They are now targeting the network periphery, where defender visibility is reduced by the possibility that endpoints may lack EDR sensors or cannot support sensor deployment."
>
> —CrowdStrike 2024 Global Threat Report

In these growing cases where threat actors circumvent traditional EDR tool controls by "targeting the network periphery" (seen, for example, in the CVE-2017-9805 Apache Struts 2 Exploit attempt), network visibility becomes essential to early threat detection.

But not just any network visibility will do. Organizations need packet-level visibility across the data link, transport, session, presentation, and application layers of a network (OSI layers 2-7) to get the rich context and metadata required to fuel behavior-based machine learning algorithms and accurately distinguish malicious activity from benign. Relying on NetFlow data alone or only capturing packets from the network and transport layers are likely to yield more false positives, and threat actors can circumvent techniques like deep packet inspection.

Use of Legitimate Tools for Illegitimate Activities

Threat actors are increasingly using legitimate IT tools, such as PowerShell, to blend in with normal network activity and evade detection. Malicious use of PowerShell to facilitate lateral movement lends itself to network-based detection because PowerShell lateral movement tends to happen over the MSRPC protocol. However, if the MSRPC protocol is encrypted, which is often the case, the ability to decrypt MSRPC is essential: It allows security teams to see the details of the lateral movement (e.g., the details of the code being executed and whether the code loads in memory or onto a disk). If the code loads into memory, traditional endpoint security tools are unlikely to see it.

Lateral Movement from Cloud to On Premises

Another trend that lends itself to network-based detection is the rise in lateral movement between on-premises and cloud environments. The CrowdStrike report cites the SCATTERED SPIDER group as an example of this kind of behavior:

> "SCATTERED SPIDER often used access to victims' Microsoft 365 environments to search SharePoint online for virtual private network (VPN) setup instructions and then logged on to the VPN and moved laterally to on-premises servers. SCATTERED SPIDER was also observed using Azure run commands and similar capabilities to move laterally from the cloud control plane to compute instances."
>
> —CrowdStrike 2024 Global Threat Report

An NDR platform like RevealX™ uses packet mirroring and cloud taps to allow organizations to automatically discover cloud assets connecting to the network and to see which cloud services are sending and receiving data to and from on-premises systems. RevealX also detects lateral movement between cloud workloads to uncover malicious behavior such as SSRF and CSRF payload attacks, credential enumeration, data staging, and data exfiltration.

Identity-Based Attacks Skyrocket

Identity-based attacks have taken center stage, with adversaries leveraging social engineering tactics to circumvent multifactor authentication measures.

According to the CrowdStrike 2024 Global Threat Report, identity-based and social engineering attacks surged in 2023. To counter these threats, implement technology that can detect and correlate threats across identity, endpoint, and cloud environments. Cross-domain visibility and enforcement enables security teams to detect lateral movement, get full attack path visibility, and hunt for malicious use of legitimate tools.

Kerberos attacks highlight the massive escalation in identity-based intrusions. The CrowdStrike report indicates that 62% of hands-on intrusions in 2023 involved the abuse of valid accounts. CrowdStrike also observed a “staggering” 583% increase in attacks using stolen or forged Windows Kerberos tickets, a technique known as “Kerberoasting.” By stealing or forging Kerberos tickets, bad actors can gain access to encrypted credentials, which can then be cracked offline. Adversaries go to great lengths to get user credentials via techniques like Kerberoasting because this enables them to pose as a legitimate user and avoid detection while advancing the attack path.

Kerberoasting is well-suited for network detection because requests for Kerberos tickets are sent over the network. To that end, RevealX helps to support a holistic identity protection strategy by closing security gaps with network visibility into malicious behaviors, including the theft of Kerberos tickets. Additionally, RevealX has integrations with Identity Service Engine and network access control (NAC) systems, which can quarantine a wireless or wired session of a compromised endpoint.

Read the full report from our technology partner CrowdStrike and discover how RevealX can defend against these and other threats with a personalized demo.