CASE STUDY

HOW A MAJOR LATIN AMERICAN TELECOM COMPANY STOPPED THE FLOW OF STOLEN DATA

THE CHALLENGE

A major player in the Latin American telecom sector knew its network was regularly breached. Its extensive connectivity to distributors increased its vulnerability, giving cybercriminals multiple points of entry into their networks. It was also aware that proprietary and customer information was for sale on the dark web.

Internal processes to investigate breaches were inefficient. No SOC was in place, the volume of alerts was high, they lacked visibility, and the time from detection to response was slow.

THE SOLUTION

The company began an aggressive search to find an integrated solution that would address both the technical and manpower problems while delivering clear forensic evidence to guide prioritization of prevention activities. They needed a technology that would be able to automatically investigate and prioritize attacks across the networks from internal and external actors.

Ultimately, after a thorough PoC process, they chose to deploy Verint Threat Protection System to strengthen security and accelerate time from detection to response.

Complete network visibility and insight

Verint Threat Protection System monitors payloads, networks and endpoints, providing a complete picture of attacks against the network.

Insight into breaches

The solution detects and analyzes complex breaches across the entire attack chain, including command and control channels and lateral movement, across the network and endpoints. The solution also provides evidence of all findings.

Extends the capabilities of the threat intelligence team

Threat Protection System mimics the activities of human analysts to automate the investigation process, turning thousands of data points into actionable intelligence – rapidly accelerating the path from detection to response.

Reduces false positives

All leads are automatically investigated and validated with forensic evidence to triage, prioritize and minimize false positives.

THE RESULTS

The Threat Protection System deployment itself proved to be highly revealing – the company had no idea of the extent of the breaches. It not only discovered malware, but it also discovered the company was financially affected. Cybercriminals were facile at stealing customers' personally identifiable information, selling customers' locations, and accessing data to commit fraud.

Beyond the generic malware, Threat Protection System found custom-made malware designed just for this telecom company to exfiltrate specific customer information. Investigators suspected that some of the data piracy was perpetrated by insiders, but they couldn't prove it. Information from the Threat Protection Systems helped identify three staff members, who were immediately dismissed.

Threat Protection System in Action

Network wide installation was straightforward and took several days. Verint also helped them establish and train a five-person SOC.

Investigations are now completed rapidly, with two distinct response modes - contingent upon whether the notification of a breach come from Threat Protection System or another tool.

Upon notification from the Threat Protection System, the team immediately goes into triage mode and reviews involved endpoint-actors and network forensics within the system.

If the notification comes from another tool, Threat Protection System remains an integral part of the investigation. Its network forensics are the source by which the team reviews actor activity and tracks the investigation and reviews data

No matter the location, they also review proxy, firewall and endpoint logs (if available). If it's an email, domain or IP attack, they prepare and apply new rules to the firewall.

"With Verint Threat Protection System, our staff can more easily manage the volume of alerts and prioritize how they handle threats, more quickly addressing breaches."

Accelerated ROI

The telecom company has seen a significant drop in incidents and a sharp decrease in customer complaints on their website. Investigation efficiency has improved by 30-40%.

Overall, the deployment of Threat Protection System has secured the telecom's customers' personal data, ended the bot-attack problem, enhanced and sped investigations, and protected the company's bottom line and reputation.

"For every breach we had previously, the ripple effect was considerable. With Verint Threat Protection System, we're able to catch breaches before they become major attacks."