STAMUS NETWORKS

Financial Services Customer's EDR Misses Clever Spyware Attempt

Situation:

A customer manages a vast datacenter and remote workforce with a mix of physical and virtual network sensors for their large financial institution. Due to the nature of their industry, their devices change IP addresses an average of every 30 minutes, making it nearly impossible to rely on IP addresses for threat detection.

Discovery:

While testing a new feature in their NDR — "Sightings" which identifies never-seen-before network communications — the customer discovered that a laptop belonging to a trusted member of the infrastructure team had unintentionally installed an adware program. The agent appeared to change its objectives, and was now attempting spyware-like exfiltration.

Outcome:

This spyware had managed to evade the endpoint defenses (EDR) and the company-wide browser restrictions and posed a growing risk to the organization. Detecting this from the network allowed the customer to open an incident and engage their EDR/SoC teams to evaluate further impact and other potential points of quarantine that may be needed.

Read the complete story »

Network Detection and Response

Network detection and response (NDR) is a critical component of a comprehensive cyber defense strategy, monitoring and analyzing network traffic to identify and thwart malicious activities that traditional security measures may miss.

Using a combination of automated detection algorithms, incident investigation, and threat hunting tools, NDR enables organizations to proactively detect, investigate, and respond to threats that pose a risk to network infrastructure.

At Stamus Networks, we have enjoyed the privilege of working closely with a diverse range of organizations around the world.

During our deployments, we have witnessed remarkable success stories. In each example, NDR has played a pivotal role in safeguarding networks, mitigating attacks, and minimizing the impact of security incidents.

Each story provides a quick example of how NDR achieves one or more of the following three use-cases:

Threat Detection and Response [TD]

NDR empowers users to automatically detect threats and respond quickly, filling gaps left by traditional security measures and ultimately strengthening organizations overall security posture.

Network Visibility and Incident Response [NV]

NDR enhances network visibility by capturing and analyzing network traffic, enabling organizations to gain comprehensive insights into their network activities and identify potential threats in a timely manner.

Threat Hunting [TH]

NDR enables security teams to proactively explore network data, detect potential threats that may have evaded traditional security measures, and investigate suspicious activities, shadow IT, and policy violations.

The Stamus Security Platform

The Stamus Security Platform is an open network-based threat detection and response (NDR) solution built on a Suricata foundation that delivers actionable network visibilityand powerful threat detection with:

- **Greater visibility into threats & activity**
- **Optional air-gapped deployment**
- **Our advanced probes or your Suricata sensors**
- **Transparent detections with detailed evidence**
- **Open and extensible for your environment**
- **Built for enterprise-scale operations**

Stamus Security Platform is trusted by some of the world's most targeted organizations, including government CERTs, central banks, insurance providers, managed security service providers, multinational government institutions, broadcasters, travel and hospitality companies, and even a market-leading cybersecurity SaaS vendor.

Like these organizations, your organization could likely benefit from including Stamus Security Platform in your cybersecurity strategy.

To learn more about SSP, visit us at www.stamus-networks.com