STAMUS NETWORKS

Multiple Security Vendors Miss Suspicious HTTP User Agent Activity

Situation:

A subsidiary of a large European banking and insurance conglomerate has a mix of on-premise, branch office, public and private cloud assets. In addition to NDR, their substantial security infrastructure includes endpoint detection (EDR), VPN, firewall, and multi-factor authentication from many of the industry's top security vendors.

Discovery:

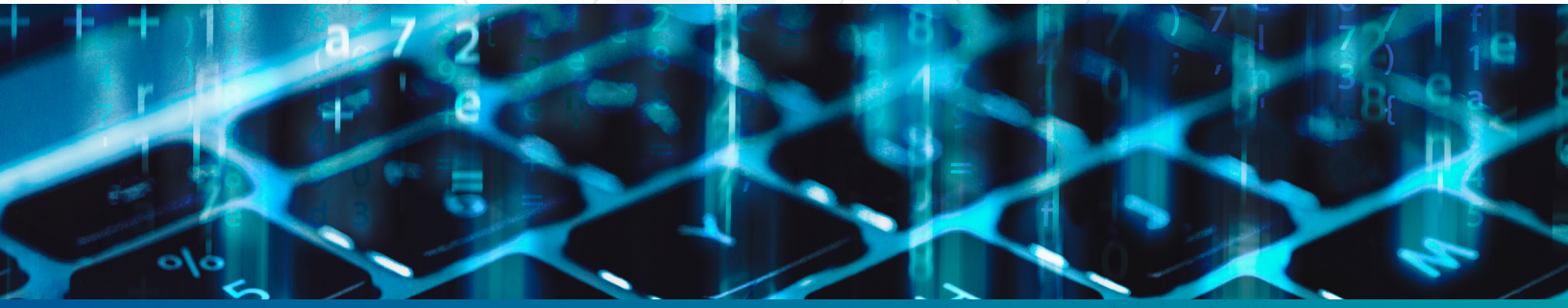
By reviewing the host insights data available in the NDR's integrated threat hunting interface, the customer discovered a series of transactions involving very unusual HTTP user agents. They identified what appeared to be Chinese and Korean alphabet characters in the HTTP user agent fields within protocol transactions on the accounting department's network. This was suspicious because the bank does not do business in China or Korea, and would not expect to see these characters from any of its systems.

Outcome:

The customer isolated the internal sources of this unusual communication to a specific department (accounting) and group of staffers from within that department. The security team determined that the staffers were accessing an unapproved legacy software system that was generating the communications, leading the customer to escalate the activity and launch a formal investigation.

Read the complete story »

> By reviewing the host insights data available in the NDR's integrated threat hunting interface, the customer discovered a series of transactions involving very unusual HTTP user agents.



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