

Proactive Threat Hunting Detects MoDI Rat Malware Before Damage Can Be Done



Situation:

A financial services organization had the NDR configured to automatically classify certain types of events as “relevant” to the security posture of the organization. During a regular check-in with the NDR vendor’s support team, the organization reviewed a set of these relevant events — just 20 of the 500 million total events gathered in the previous 24 hours.

Discovery:

One particular event — triggered by an ETPro malware IDS rule — stood out. Upon further investigation, the team discovered that a user had visited a Wordpress blog that was infected with MoDi RAT malware.

Outcome:

The customer was able to escalate the event, quarantine the device, and even notify the owner of the blog, catching the malware on the network before it caused any impact to the organization.

[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 visibility and 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.

