CASE STUDY

Containing Trickbot and Emotet

Bytes Computer & Network Solutions

Background

In 2017, Clint Bergman joined as Chief Technology Officer at Bytes Computer & Network Solutions. Inheriting an endpoint security stack comprised of Windows Defender and Malwarebytes, he describes the decision to add Huntress:

"Our peer groups recommended it, and the concept of a lightweight endpoint detection service with people behind it for remediation support was intriguing."

A Pivotal Moment

Bytes' incident response program was put to the test in late 2018 when one of their newer clients clicked a malicious email attachment. Shortly afterwards, Clint's office received a call asking about a Windows Defender alert for two self-propagating banking trojans: Emotet and Trickbot. These trojans are also known to act as droppers for additional malware, such as ransomware, so it was important to act quickly.

The calls and alerts piled up, making it clear the network worm was spreading fast. They needed a solution that would help identify the exact actions to address the infection. Within minutes, they made the decision to deploy Huntress and Trend Micro to all the client's hosts for threat hunting and additional endpoint protection.

Fast Response

Once deployed, Huntress identified malicious footholds on more than 200 endpoints and provided easy to follow remediation instructions for each host. Clint worked with John Ferrell, VP of ThreatOps at Huntress, to develop a PowerShell script that aggregated details from the remediation instructions to kill processes and delete services, files, registry entries, and scheduled tasks. Once complete, Clint's team executed the script through their RMM on all workstations and servers. The script was re-run every 15 minutes to clean all of their affected endpoints as they came online. The support from the Huntress ThreatOps team—with their background in security and incident response—complemented the Bytes' team throughout the entire incident. The joint effort was crucial in thoroughly removing the footholds to quickly remediate within 72 hours.

HUNTRESS

Bytes Computer & Network Solutions

Location
Scottsville, Nebraska

3000+ managed endpoints across all industries

Security stack
Huntress, Windows Defender, Malwarebytes, Trend Micro

Threats encountered
Trickbot, Emotet

"I have never received anything but absolute excellence from anyone I've worked with at Huntress."

Clint Bergman, CTO
Bytes Computer & Network Solutions

CASE STUDY

Bytes Computer & Network Solutions

Proactive Threat Hunting

After experiencing the speed at which threat actors attempted to cripple their client's business, Clint committed to proactively hunting for threats going forward. He notes:

"It may sound cliché, but the value Huntress brings at its cost is a no-brainer, and the support during our incident—even working directly with the John Ferrell, the VP of ThreatOps at Huntress, until 2 AM some nights—was priceless."

Realizing the benefits that Huntress delivers to protect their customers, Bytes Computer & Network Solutions plans to expand Huntress to the rest of their 3,000 managed endpoints and include it as part of their core service package.

Read our Guide to Selling Cybersecurity to learn more about essential layers in a comprehensive security stack.

Moving the Needle

Continuously improving from lessons learned is a key tenet at Huntress. The **remediation script** created in collaboration with Bytes Computer was so effective that it was modified and shared to help others with **Emotet and Trickbot** infections.

Building upon this, Huntress created **Assisted Remediation**, a new capability that enables the Huntress agent to remove discovered footholds with the click of a button for an even faster response.

HUNTRESS

For more information and to sign up for a free trial, visit **huntress.com**