Huntress Managed EDR alerts partners to attackers actively targeting VMware Horizon servers—enabling them to swiftly react and mitigate the threat within one day.

Huntress Empowers Blue Tree Technology and IntelliData Solutions to Fight Off an Active Exploit

While the Huntress 24/7 ThreatOps team was hard at work one Friday afternoon, we received a Windows Defender alert that warned our team of a Cobalt Strike implant on one of our partners' networks. Within minutes, another similar-looking Defender alert came in from a completely different organization. After digging into both alerts, we found a commonality: Hackers were targeting VMware Horizon servers using Log4Shell vulnerabilities.

After realizing that these were not isolated incidents, our ThreatOps team quickly jumped into action to protect any other potentially affected partners. One of the first actions was to roll out Huntress Managed EDR, which offers advanced endpoint detection and response (EDR) backed by ThreatOps, to all partner systems with VMware Horizon. By giving our team insight into detailed information about processes, Huntress Managed EDR enabled us to proactively detect and respond to non-persistent malicious behavior. Within minutes, Huntress Managed EDR surfaced which partners had certain malicious commands executed on their systems—all of whom immediately received an incident report with the most up-to-date information and mitigation techniques. Blue Tree Technology was one of those partners.

"Huntress notified us of the threat before we had any idea what was happening," said Tom Noon, VP of Operations at Missouri-based MSP, Blue Tree Technology. "Their team gave us all the information we needed to get up to speed, including the machine name that was infected, the steps to confirm the infection and how to remediate the threat." In this case, the infected machine was hosted by IntelliData Solutions, a hosting partner of Blue Tree Technology.

Blue Tree Technology

LOCATION

Riverside, Missouri

THREAT ENCOUNTERED

Log4Shell Vulnerabilities

IntelliData Solutions

LOCATION

Long Beach, New York

THREAT ENCOUNTERED

Log4Shell Vulnerabilities

We get so many alerts, noise and false positives from our other cybersecurity tools—it's hard for our technicians to know what to focus on. Huntress filters out all that noise. Their ThreatOps team does a remarkable job of verifying threats and only sending alerts when they need our attention or action.

"We had VMware servers that were patched, yet hackers were still able to sneak through," said Pavan Agrawal, CTO at IntelliData Solutions. "Huntress gave us a specific set of instructions that told us how to confirm that there was an infection and how to remediate the threat. We were able to easily follow the instructions to evict the malicious content and confirmed with Huntress once it was complete. We avoided a really messy situation—that's all thanks to Huntress."

After following Huntress' remediation steps, both IntelliData Solutions and Blue Tree Technology successfully restored their data to its pre-infected state by the end of the day. "Huntress helped us be more proactive, rather than reactive," said Alec Smith, President at IntelliData Solutions. "If we hadn't confirmed and remediated the threat, client information would have been compromised and we could have suffered severe damage to our reputation."

Huntress Managed EDR captures threat actor activity by actively monitoring processes in near-real-time. The forensics performed by Huntress Managed EDR identifies and alerts administrators to suspicious activity. However, unlike traditional cybersecurity technology which relies on administrators to comb through all the data and alerts, our Managed EDR is backed by Huntress' team of human threat hunters. The Huntress ThreatOps team filters through the alerts for partners to verify threats and send only incident reports that require attention paired with remediation instructions. This eliminates false positives and assures partners that alerts are timely and relevant.

"Artificial intelligence is good, but there is nothing better than the human intelligence of Huntress' threat hunters," explains Tom of Blue Tree Technology. "We get so many alerts, noise and false positives from our other cybersecurity tools—it's hard for our technicians to know what to focus on. Huntress filters out all that noise. Their ThreatOps team does a remarkable job of verifying threats and only sending alerts when they need our attention or action. Our techs know that when an alert from Huntress comes through, they better look at it. This incident was an example of that—and it gave us the validation we needed to roll out Huntress to all our clients."

Learn more at huntress.com

Follow us on social @HuntressLabs

About Blue Tree Technology

Blue Tree Technology is a vibrant, women-minority owned IT firm located in Riverside, Missouri. We love giving world-class friendly IT Support. Our IT support staff has over 100 years of combined experience in installing, configuring, and maintaining IT Infrastructure for Small and Medium Businesses. We are able, to understand our clients' needs and plan and implement solutions that work for your business, both in the short term and long term.

Learn more at www.bluetreetechnology.com and contact us at 816-256-2595.

About IntelligentData Solutions.

We are the only expansive hosting provider that substantially reduces infrastructure CapEx for complex environments such as engineering & architecture firms using the "Once & Done" rapid deployment of virtual desktop infrastructure (VDI) solutions without cost and time overruns... backed by our "Uptime Permanence Guarantee".

Learn more at www.intellidsi.com and contact us at info@intellidsi.com.

About Huntress

Hackers are constantly evolving, exploiting new vulnerabilities and dwelling in IT environments—until they meet Huntress.

Huntress protects small and mid-market businesses from modern cyberattackers. Founded by former NSA Cyber Operators—and backed by a team of 24/7 threat hunters—our managed security platform defends businesses from persistent footholds, ransomware and other attacks.

We're on a mission to secure the 99%. Learn more at www.huntress.com and follow us on social @HuntressLabs.