MINERVA

BlueVoyant

Case Study

Cybersecurity Services firm BlueVoyant partners with Minerva Labs to contain sophisticated malware attacks.

Facing a persistent malware infection—one that had proven stubbornly resistant to repeated antivirus applications—an educational institution reached out to BlueVoyant's Cyber Forensics and Incident Response team for help in conducting a forensic examination.

When the BlueVoyant team collected, analyzed, and reverse-engineered samples from several of the infected machines, the results revealed that the organization was dealing with something far more severe than a minor malware outbreak. Instead, it was a victim of a highly persistent banking trojan called Emotet that had wormed its way onto 1,400 endpoints. Notoriously difficult to neutralize, this pernicious strain of malware continuously modifies its techniques, updating daily and spreading laterally to evade antivirus, endpoint detection, and other cyber security measures. Once inside an organization, the malware can infiltrate systems, steal passwords, capture keystrokes, and transmit stolen data. Many organizations with this level of infestation are forced to consider a total network rebuild.

BlueVoyant's partnership model allows it to provide clients with best-of-breed solutions that can address complex needs such as this. Through its partnership with Minerva Labs, BlueVoyant was able to immediately deploy Minerva's Anti-Evasion Platform. The sophisticated solution deceives the malware and causes it to disarm itself, providing the containment necessary to remove highly-active malware like Emotet. Once the malware was contained, BlueVoyant developed a customized tool that removed all persistence, then applied a vaccine that eradicated Emotet from the infected network.

The BlueVoyant and Minerva partnership neutralized the epidemic within a mere 12 weeks and saved a grateful client from what would otherwise have been a months-long overhaul costing several hundred thousand dollars. "When our clients' environments are breached," said Austin Berglas, global head of BlueVoyant's Cyber Forensics and Incident Response business, "we need specific tools with critical strengths that we can count on 100 percent of the time. Minerva is that tool when it comes to containing sophisticated and evasive endpoint attacks."

"With the help of Minerva Labs, we were able to contain and clean up the Emotet infection 60-70 percent faster than if we had used our previous manual method," said Vincent D'Agostino, deputy head of Cyber Forensics and Incident Response at BlueVoyant. "This resulted in drastically lower remediation costs, almost zero network downtime, and fewer losses for the client."

> *With the help of Minerva Labs, we were able to contain and clean up the Emotet infection 60-70 percent faster than if we had used our previous manual method*
>
> *Vincent D'Agostino, deputy head of Cyber Forensics and Incident Response at BlueVoyant.*

About BlueVoyant

BlueVoyant is a Threat Intelligence, Managed Security Service, and Cyber Forensics and Incident Response business with offices in New York, the Washington D.C. area, London and Tel Aviv. More information on BlueVoyant can be found online at www.bluevoyant.com

About Minerva Labs

Minerva Labs is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva Labs' Anti-Evasion Platform blocks threats that bypass antivirus and other baseline protection solutions by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, the Minerva Labs solution deceives the malware and causes it to disarm itself, thwarting it before the need to engage costly security resources.

Headquartered in Petach Tikva, Israel, and with offices in New York and Atlanta, Minerva Labs boosts customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture. To learn more about Minerva, visit www.minerva-labs.com

www.minerva-labs.com | contact@minerva-labs.com | +1-404-805-1510