BlueVoyant

CASE STUDY:

BUILDING A MORE SECURE COMMUNITY

A municipality thwarts malware outbreak and prevents future attacks with BlueVoyant Incident Response and Managed Security Services.

Municipalities are constantly under attack by nation-states looking for access to critical infrastructure, such as power grids, as well as criminals looking for financial gain.

Late in 2017, a municipality contacted BlueVoyant with an immediate need for incident response. The organization was suffering an expansive outbreak of advanced malware (emotet) which had been injected into the organization via a phishing campaign. According to US-CERT, this particular malware is being used aggressively to target governments with emotet infections, costing them up to USD $1 million per incident to remediate.[1]

Reducing the impact of an attack and keeping services running and available were critical to this thriving municipality: they needed to contain their malware quickly and decisively.

Key Benefits

- Prevented business disruption.
- Delivered same day response to malware outbreak.
- Provided immediate visibility across the network.
- Devised and implemented strategy that allowed for rapid remediation while allowing the network to operate, uninterrupted.
- Eliminated thousands of man hours in incident response and network operations.
- Reduced the impact of subsequent attacks by decreasing the detection & response time from months to one hour.

"Emotet is one of the top five most-seen malware families of 2017."

Carbon Black Threat 2017 Report

1 https://www.carbonblack.com/resource/carbon-black-2017-threat-report/

BlueVoyant

Keeping critical services running.

With critical items such as water supplies and emergency response services at risk due to this attack, response and containment were critical. BlueVoyant responded on the same day and deployed its advanced endpoint protection platform. Within hours of the first contact with the municipality, BlueVoyant had begun the incident response and root cause analysis, quickly determined the type of malware, and tracked its movement around the network. Within a few days, BlueVoyant had full network visibility of every machine that was exhibiting malicious behavior. The incident response team developed a strategy to stop the malware from executing. In addition, BlueVoyant developed and deployed a custom software to remove emotet from the network.

An uncommon approach can yield the best and most cost-effective outcome.

Over the course of the incident response engagement, BlueVoyant utilized its endpoint protection platform and developed custom software to delete the remnants of the malware from the network. Other providers would have instructed the client to re-image all affected computers on the network, a process that would take significant time and resources, plus cause major network outages without solving the problem.

A sustainable and trusted approach to stay ahead of emerging threats.

Following the successful response and remediation of the initial outbreak, the municipality chose BlueVoyant as their managed security services provider. Within a month of the completion of the cleanup of the initial outbreak, the municipality was targeted again by a mutated form of emotet. This time, BlueVoyant detected the threat in near real-time. Within an hour, the attack was completely shut down and contained. The rapid detection and response significantly reduced the impact of the attack by limiting the malware's ability to infiltrate and replicate itself.

Staying ahead of evolving threats.

Emotet is a polymorphic, advanced malware, meaning that it is constantly mutating to avoid detection by common tools utilized by cybersecurity professionals. It is a fileless malware, which uses trusted programs to gain control of computers. Because this type of malware does not typically require downloading additional malicious files, they are particularly difficult to detect. According to 93% of security researchers, fileless attacks pose more of a business risk than commodity malware attacks.

For more information please visit:
www.bluevoyant.com

About BlueVoyant

BlueVoyant is an analytics-driven cybersecurity company whose mission is to protect businesses of all sizes against agile and well-financed cyber attackers by providing unparalleled visibility, insight, and responsiveness. BlueVoyant provides Advanced Threat Intelligence, Managed Security Services and Professional Services through offices in the United States, the United Kingdom, Israel, and Spain.

Secure your business now:
sales@bluevoyant.com