BlueVoyant

CASE STUDY:

MUNICIPALITY CASE STUDY

Large Municipality Recovers from Emotet Malware and Prevents Repeat Data Breach with BlueVoyant

In 2017, a mid-sized municipality came under attack by a sophisticated threat actor. An email-based phishing campaign gave the cyber attacker access to over 1,400 end points. A group of end users simply clicked a "legitimate looking link" which deposited a trojan within the system that was able to mutate, or morph, inside the system, transmitting from endpoint to endpoint undetected by existing security controls.

Fast identification, remediation, and expert handling were delivered by the BlueVoyant team who was able to keep the organization running while preventing future attacks with Managed Security Services and the experts in the BlueVoyant SOC.

Municipalities responsible for both large and small communities are often a target of cyber attackers because they are networked to key infrastructure and transmit sensitive financial data. Through keystroke recording malware, threat actors can gain unauthorized access to community infrastructure and steal sensitive information.

In this incident, the municipality was affected by an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojan called "Emotet". This malware changed its identity once it gained access to the network. It replicated like a virus and mutated to avoid detection as it spread. This type of attack tool behaves unusually and is virtually undetectable using standard anti-malware solutions.

RAPID RESPONSE URGENTLY NEEDED

The municipality called in BlueVoyant's forensic investigators requesting immediate assistance. BlueVoyant incident response experts were able to identify the banking trojan malware, emotet, which had infected much of the network.

Investigators determined that the malware was able to gain access, despite the organization's firewalls and virus protections, because a legitimate looking phishing email enticed several recipients to click on a link and unknowingly unleash the malware across the network.

KNOWN THREAT ATTACKS NEW TARGET

Immediate response and containment was crucial because the attack put several dependent organizations at risk. The municipality's critical infrastructure, including the power grid, water supply, fire and police departments, along with personal financial information of the citizens was compromised.

According to the United States Computer Emergency Readiness Team (US CERT) under the Department of Homeland Security, this malware was being used in numerous attacks and was exceeding $1M to remediate each incident. (www.us-cert.gov/ncas/alerts/TA18-201A)

FIRST REVIEW THEN RESPONSE & REMEDIATION

Within hours of BlueVoyant's engagement with the municipality, a proprietary endpoint protection platform, combined with custom software, was successfully deployed to eradicate all traces of the malware.

The disruption caused by this attack was expensive, not only from a technology perspective, but also from the rippling requirements for crisis response, legal, compliance and reporting standpoints. This prompted the municipality to engage BlueVoyant to manage their cybersecurity needs and safeguard them from future attacks, which turned out to be a great investment.

Less than a month later, a mutated form of the emotet targeted the same municipality. In real time, BlueVoyant's SOC experts detected and immediately contained the threat.

The analysts, responding to anomalous activity, were able to pinpoint the breach, isolate and quarantine the affected machines and prevent the virus from spreading across the network within hours.

BlueVoyant

Rapid Response

Immediate response and containment was vital. The attack put critical government services, such as the power grid, water supply, and emergency responder networks at risk.

Within hours of contact with the municipality, BlueVoyant devised and implemented a strategy that allowed for rapid remediation while allowing the network to operate uninterrupted.

Tailored Solutions

Using a best-in-class endpoint protection platform, BlueVoyant was able to detect, investigate, and remediate malicious activity on all networked devices, preventing critical infrastructure disruption.

Beyond just deploying our partners solutions, BlueVoyant tailored the software to seek out and eradicate all traces of the malware, eliminating the need to re-image affected network decides, saving the municipality both time and money.

Advanced Protection

Following the successful response and remediation of the initial outbreak, the municipality chose BlueVoyant as their Managed Security Services provider for Managed Detection and Response (MDR).

The comprehensive endpoint detection, real-time monitoring, and 24x7 security operations centers that go well beyond the capabilities of the municipality's IT staff.

"We were surprised and relieved that BlueVoyant could keep our critical networks online while they worked to fix the problem. We were already stressed about what to do next so minimizing user disruption was a welcome surprise. Their experts in the SOC kept us apprised of what was happening at key points of the discovery and that's what gave us confidence in relying on them for more - they guided my team as we worked together to educate our users."

- IT Manager

For more information please visit:
www.bluevoyant.com

Secure your business now:
sales@bluevoyant.com

BlueVoyant is an analytic-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 Incident Response through offices in the United States, the United Kingdom, Israel, and Spain.