BlueVoyant

Municipality Client 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 endpoints. 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.

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 particular incident, the municipality was affected by an advanced, modular banking Trojan that primarily functions as a downloader or dropper of another 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 REQUESTED

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.

FIRST REVIEW THEN RESPONSE & REMEDIATION

Within hours 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.

RESPONSE, REMEDIATION, AND PREVENTION

RAPID RESPONSE

Immediate response and containment was crucial. 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 for rapid remediation while allowing the network to operate uninterrupted.

TAILORED SOLUTIONS

BlueVoyant was able to detect, investigate, and remediate malicious activity on all networked devices, preventing critical infrastructure disruption. BlueVoyant tailored the software to seek out and eradicate all traces of the malware, eliminating the need to re-image affected network devices, 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 go well beyond the capabilities of the municipality's IT staff.

MDR+ PREVENTS RECURRENCE

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. 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.