BlueVoyant

CASE STUDY:
SAFEGUARDING THE DIGITAL ECONOMY

An online travel agency eradicates a malware outbreak and prevents financial and reputational damage with BlueVoyant services.

Online travel agencies (OTAs) have taken over the traditional hospitality industry and this has created substantial cyber risks. Cybercriminals have found a gold mine in the digital economy.

In early 2018, a West Coast-based OTA contacted BlueVoyant regarding a chargeback fraud incident with losses approaching $1 million dollars. The unknown actor accessed a cloud-based payment card processing application using stolen credentials. BlueVoyant began a forensic investigation focusing on the custodian whose account had been used for the fraud and discovered a TrickBot malware infection. The presence of the malware, which has the ability to move laterally, prompted BlueVoyant to deploy sensors and initiate a hunt operation which ultimately identified an additional banking trojan on the OTA network.

Identifiying the source of the fraud and returning to operational status with the confidence that all threats were contained was of the utmost importance for the OTA.

Key Benefits

- Reduced the impact of attacks.
- Uncovered a dormant banking trojan that could harvest sensitive company data.
- Prevented regulatory risks by collecting all the information required to comply with the Payment Card Industry Data Security.
- Prevented significant business disruption by eliminating both trojans at once.
- Reduced the risk of reputational damage and platform leakage.

Trickbot is polymorphic malware that exploits vulnerabilities in Microsoft Windows.
It has been linked to disastrous campaigns such as WannaCry in 2017.

BlueVoyant

Stop chargebacks immediately.

The forensic analysis of the victim's device revealed an active TrickBot infection. TrickBot is a financial trojan most commonly used to harvest credentials via phishing campaigns. While the client's anti-virus detected and quarantined the executable, it was ineffective against the malware's persistent mechanism which allowed it to restore itself. TrickBot scraped saved credentials, giving access to the OTA's payment card system.

Concurrently, BlueVoyant identified an ongoing, global campaign which utilizes a new module allowing the malware to spread laterally.

Uncover unforeseen risks.

During the course of the 30-day hunt operation, a Gozi banking trojan was identified. The analysis revealed that Gozi, a known malicious application, had been introduced to the system six months prior. The BlueVoyant team found that the infected device contained nearly 18,000 recoverable "briefcase" files with potential PCI data labeled as "Credit Cards".

Eliminate regulatory and reputational damage.

The sensitive, PCI nature of the contents required that the card vendors be notified within 24 hours. The BlueVoyant team was able to provide the necessary data to the meet the legal notification requirement for the client and counsel.

After the investigation, BlueVoyant was able to contain previously unidentified threats, remediate all compromised credentials, and lead the OTA back into full operational status and with an exponentially increased cyber hygiene of their network.

"The Gozi virus [is] one of the most financially destructive viruses in history. It infected over one million computers globally and caused tens of millions of dollars in losses."

Federal Bureau of Investigation Archives.
https://archives.fbi.gov/archives/newyork/press-releases/2013/three-alleged-international-cyber-criminals-responsible-for-creating-and-distributing-virus-that-infected-over-one-million-computers-and-caused-tens-of-millions-of-dollars-in-losses-charged-in-manhattan-federal-court

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 Incident Response through offices in the United States, the United Kingdom, Israel, and Spain.

Secure your business now:
sales@bluevoyant.com