BlueVoyant

CASE STUDY:

ONLINE TRAVEL AGENCY

Online Travel Agency Engages BlueVoyant to Remediate Severe Malware Attacks

A study conducted by Google found that over 75 percent of leisure travelers reported using Online Travel Agencies (OTA) because they offer the best pricing. While OTAs may have taken over the hospitality industry, in their rush to move online many neglected focusing attention on crucial security measures. Now they are a gold mine for cybercrime because the data that they collect is very attractive to threat actors including: contact information, birthdays, passport numbers, and credit card credentials.

In early 2018, a West Coast-based OTA, experiencing almost $1 million in losses, contacted BlueVoyant to assist with a chargeback fraud incident. An unknown threat actor was able to access the agency's cloud-based payment card processing application using stolen credentials, putting clients at risk for credit card fraud, damaging the reputation of the agency and risking their PCI compliance.

PHISHING, A COMMON CULPRIT

Phishing campaigns have become increasingly sophisticated because every modern business uses email. To be successful, the outreach to an employee has to look legitimate - people are savvy enough to not click on links from places they don't recognize, but with spoofing on the rise, more and more people are duped by "legitimate looking links" than ever before.

It can be very difficult to identify a phishing email and on average, one in five employees who have undergone training, will still click a link in a carefully crafted, seemingly urgent phishing email.

BlueVoyant's team of expert forensic investigators focused their attention on the account used to initiate the fraud. Forensic analysis of the victim's device revealed an active TrickBot infection.

The TrickBot malware, delivered via a phishing campaign, was able to exploit a vulnerability in Microsoft Word in order to infect the Windows environment.

TrickBot, a financial Trojan commonly used to harvest credentials, was able to scrape saved usernames and passwords on the device, giving the threat actor access to the OTA's payment card system.

Although the client's anti-virus detected and quarantined the executable, it was ineffective against the malware's ability to rapidly restore itself. The threat actor was able to request and generate fraudulent refunds with the access and stolen credentials.

HUNT OPERATION IDENTIFIES LURKING GOZI

The presence of the malware prompted BlueVoyant to deploy sensors and initiate a 30-day hunt operation to uncover all traces of the TrickBot. BlueVoyant's highly skilled security analysts scanned the network in search of any signs that threat actor might have left behind.

The hunt ultimately identified an additional banking trojan virus on the OTA network. Analysis revealed that banking trojan virus, 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 data labeled as "Credit Cards". The BlueVoyant experts, operating with a concern that Payment Card Information was compromised, provided the OTA with the necessary information necessary to meet mandatory PCI DSS reporting requirements.

BlueVoyant was able to eradicate Gozi and provide data for compliance reporting. As with most of our clients, identifying the source of the fraud, preventing further losses and returning to operational status with the confidence that all threats are contained was of the utmost importance for the OTA and for BlueVoyant.

BlueVoyant

Forensic Analysis

The victim's device revealed an active TrickBot infection upon forensic analysis.

While the OTA's anti-virus detected an quarantined the executable, it was ineffective against the malware's persistence mechanism, which allowed it to restore itself.

A hunt operation was recommended after the forensic analysis identified a recently updated variant of TrickBot containing a new module, which allowed for lateral movement.

Hunt Operations

Over the course of the 30-day hunt operation, BlueVoyant's hunt operators actively searched for behavioral characteristics indicative of advanced malware infections.

Analysis revealed the presence of the Gozi banking trojan, a malicious application which had been introduced to the system six months prior.

Additional forensic analysis revealed the Gozi application had been quietly gathering and storing sensitive payment card data for months.

Compliance Support

Payment Card Industry Data Security Standards require that card vendors be notified within 24 hours of incident discovery. The BlueVoyant team was able to provide all necessary data to the meet the legal notification requirements for the OTA and its counsel.

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

"We called BlueVoyant when fraudulent refunds, costing us close to a million dollars, indicated that we had severe problem. We were thrilled that BlueVoyant took our problem as seriously as we did. Their experts responded on the day we called them. They hunted across our network to eradicate all traces of malware and found another virus we might never have been aware of. The BlueVoyant experts vastly improved our network security and stood beside us until compliance reporting was complete."

- Chief Technology Officer

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.