A study conducted by Google found that over 75% of leisure travelers reported using Online Travel Agencies (OTA) because they offer the best pricing.

While OTAs 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. The data that they collect including credit card credentials - is very attractive to threat actors

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 everyone uses email. To be successful, the outreach to an employee has to look legitimate - people are savvy enough to not click on links from addresses that 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. 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 was able to exploit a vulnerability in Microsoft Word in order to infect the Windows environment.

HUNT OPERATION IDENTIFIES LURKING GOZI

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". BlueVoyant was able to eradicate Gozi and fully restore business operations.

FORENSICS, A HUNT AND COMPLIANCE SUPPORT

FORENSIC ANALYSIS

Forensic analysis revealed an active TrickBot infection. While the OTA's anti-virus detected and quarantined the executable, it was ineffective against the persistence mechanism. 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.

The threat actor was able to request and generate fraudulent refunds with the access and stolen credentials.

HUNT OPERATIONS

Over the course of the 30-day hunt operation, investigators actively searched for behavioral characteristics indicative of advanced malware. Analysis revealed the presence of the Gozi banking trojan, a malicious application that had been introduced to the system six months prior.

Additionally, 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 meet mandatory PCI DSS requirements.

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.