CSIS Incident Response Kit (CIRK)

CASE STUDY

HIGHLIGHTS

CIRK is a powerful remote forensics tool that enables accurate and efficient threat detection and remediation.

Our customers place significant value on our forensics procedures, especially because they know we don't just rely on automated technology. Our security analysts are an essential part of the process.

CSIS's remote forensics tool helps a leading UK bank prevent fraud.

A LEADING UK BANK IS TARGETED BY MULTIPLE THREATS

A leading UK-headquartered bank with international operations, was suffering persistent attacks, directed at its business customers, including banking trojans and phishing. These attacks invariably led to stolen credentials, compromised accounts and stolen funds or fraudulent transactions. Such crimes lead to poor customer experience, while the bank suffered financially, as well as reputationally.

THE STATUS QUO APPROACH WAS FAILING TO SOLVE THE PROBLEM

At the time, the bank responded by instructing its customers to wipe clean their computers and re-install all software from scratch. However, no forensic investigation was conducted prior to doing so.

Among the various downsides to its customer of taking this approach were the time and effort involved, as well as the loss of valuable data.

However, another downside, which was at least as significant, was the fact that formatting computers without first conducting a forensic investigation, would lead to the loss of any possible insight into the nature of the threat, including its origin, general functionality and purpose.

The bank's approach at the time translated into a continuously reactive defense mode, without any systematic learning or defense strategy being possible.

ANALYSIS LEADS TO INSIGHT AND INSIGHT LEADS TO RESILIENCE

The ability to analyze specific threats enables an increasingly robust understanding of the overall threat landscape and how it is evolving. This understanding is crucial for companies that want to be resilient and that want to have a proactive security posture, where the capability to anticipate is at least as strong as the ability to react.

Companies cannot afford to be reactive in their fight against cybercrime and financial fraud.

One of the reasons that CIRK is unique is because it leverages the full extent of our Cyber Intelligence capabilities.

The challenge is that forensic investigations normally take a significant amount of time and neither the customer nor the bank wanted any delays in clearing the threat.

THE CSIS APPROACH: ADDING VALUE THROUGH PEOPLE AND TECHNOLOGY

In response to an unrelenting and growing number of threats affecting its business customers, the bank engaged CSIS's Cyber Threat Intelligence capability, which includes a crucial forensics tool called "CSIS Incident Response Kit", or CIRK. CIRK has a data collector, an automated forensics backend server and a reporting module.

The tool, which can be deployed easily and remotely, allows for rapid forensics inspections of computers and powerful analysis of any malicious indicators. CIRK is also powered by CSIS's world-class intelligence, which ensures that threats can detected and anticipated accurately and efficiently.

CIRK's automated analysis outputs are reviewed by CSIS's security analysts to ensure correctness and relevance of findings reported back to the bank and its customers. Additionally, CIRK has a 'Law Enforcement' notification feature, which the Bank can leverage where it is deemed appropriate.

WORKING WITH CSIS AND LEVERAGING CIRK DELIVERS RESULTS

By running fast and efficient investigation campaigns with CIRK, the bank was able to quickly identify infected customers, matching stolen credentials to its credit card register, and take the relevant internal and customer-facing actions to avoid financial losses. By providing this additional security added value, the bank not only stopped the negative experiences stemming from banking cybercrime and fraud, it strengthened its reputation as a trusted partner to its business customers.

Yet another benefit from working with CSIS has been the bank's ability to understand and stay on top of the threat landscape and to be able to spar with best-in-class security professionals to obtain fast and actionable support with respect to cybersecurity and fraud.