



Ongoing Risk Analysis and Investigation of Malware-Related Fraud Incidents

Financial institutions are especially sensitive targets when it comes to malware related fraud. Strong authentication and fraud detection are a good start but, to keep fraudsters out of customer bank accounts, it's important to identify the specific malware variants attacking you, analyze them and incorporate these findings to prevent their infiltration in the future. Drilling down to acquire this data requires extensive investigation of customer computers, a process that's complex, labor intensive and hard to scale to the entire customer base. With sophisticated malware being unleashed everyday, how can financial institutions identify and track specific malware variants and criminal groups causing losses to stay one step ahead of the game?

Trusteer Flashlight

Trusteer Flashlight is an end to end service enabling financial institutions to perform ongoing risk analysis and investigate malware related fraud incidents easily and quickly. Here's how it works:

When an incident of fraud is reported by a customer, a financial organization can instantly initiate a remote investigation process by asking their customer to install Trusteer's desktop forensic and protection software. Following a brief installation and detection process, a report identifying the malware variant on the customer's computer is quickly received. In the case of unidentified malware, Trusteer's software immediately identifies suspicious malware behavior and allows the lifting of malware samples from the computer. These samples are then examined and reverse engineered by Trusteer's fraud and malware experts, to demonstrate how the malware variant works to commit fraud. Once completed, the organization receives a full report on the malware, detailed recommendations on how to detect and block it as well as the complete source code for future reference. Trusteer goes on to report the malware to major desktop security vendors for better coverage

and protection, performs ongoing analysis of malware command and control centers, and even submits them to takedown services. The Flashlight service includes ongoing consulting by Trusteer's security experts to help mitigate future threats.

Flashlight is available as part of the Rapport offering, as an add-on module or as a stand alone solution.

Features

- Instantly and remotely analyze the relevant computer and identify the cause of fraud
- Reverse engineering of new malware samples to understand how they commit fraud
- Perform ongoing analysis of relevant malware command and control centers
- Submit malware samples to Anti-Virus vendors to ensure removal from desktops
- Submit command and control servers to takedown services
- As needed consulting in mitigating malware attacks

Benefits

- Definitively and quickly determine whether fraud events are malware related.
- Acquire metrics and categorization on fraud events
- Ensures simple, automated risk analysis and reporting for investigations
- Full life cycle management - from analysis right up to submission to takedown services
- Feedback from malware analysis tells you what fraudsters are trying to achieve
- Backed by Trusteer's extensive malware and security expertise