



Cernious CamoView™ Use Case

Real-Time Protection Against In-Use Data Theft

Business Problem

Consumers are increasingly targeted by cyber criminals for their login credentials (e.g. usernames and passwords) required by businesses for online transactions. But criminals don't stop there. According to RSA, there is an alarming growth in tools enabling cyber criminals to scale their operations to automatically harvest data "in use."

One such tool, dubbed the "balance grabber," mechanically grabs the balance of an online bank account (along with the end user's login credentials) for delivery to a cyber criminal:

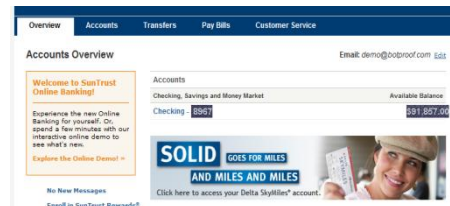
- First the criminals penetrate unprotected PCs with key loggers – programs that record every keystroke on a keyboard.
- Once the end user has logged into the site, the "balance grabber" scrapes the unsuspecting user's screen for account information and balances.
- The malware then quietly send the logs to remote sites to parse for usernames, passwords, PINs, account balances, and more.
- With this information, criminals immediately log into the user's bank account, transfer money out of the account (at amounts low enough to avoid bank fraud detection software), and "re-paint" the balance amount with what the user expects.

As recently as the fall of 2009, Ukrainian-based cyber criminals deployed just such an attack to drain German bank accounts of EUR300k in just three weeks (*source: Finjan, 2009*).

Cernious Solution

Cernious' CamoView™ protects sensitive data from being harvested by automated screen scrapers as well as those employing more advanced Optical Character Recognition (OCR).

Once logged in, sensitive information such as balances and account numbers can be presented in Cernious' proprietary format, safe from malicious programs.



Illustrative mock-up

Animated images of text and numbers are readable by the end user, but not by automated "balance grabbers" and OCR programs – meaning the end user's sensitive information is safe beyond the encrypted SSL tunnel.

Key Advantages

- **Certainty** that sensitive information "in use" cannot be harvested by automated screen scrapers and OCR programs
- **Extends reach of enterprise data protection measures** to circumvent threats residing on PCs operating outside managed security environments– with no client hardware or software required!
- **Additional layers of security** beyond the point where encryption ends for on-line transactions
- **Dynamic security delivery model** enabling real-time adjustments to stay ahead of evolving security threats

Contact Cernious for additional information or to schedule a demo

Tim Brown
Tim@Cernious.com
(801) 673 – 3322
www.Cernious.com