Malware and Phishing Fraud

Detecting and preventing malware and phishing attacks on customers' endpoints

Highlights

- Use intelligence-based endpoint and browser protection to help prevent malware infection and secure the browser against current and emerging threats
- Remediate infected endpoints by accurately detecting and removing Man-in-the-Browser malware
- Detect mobile malware and mobile fraud risk
- Provide accurate and immediate malware detection

Organizations are challenged with protecting their customers against cybercrime as they use personal endpoints that are outside the organization's control. Criminals target this weak link with Man-in-the-Browser (MitB) malware and phishing attacks that enable personal information and credentials theft. This data is later used for account takeover and new account fraud. Furthermore, financial institutions experience automated, malware-driven transaction fraud perpetrated from the victim's computer – rendering many fraud prevention technologies useless. It is no surprise that the regulators have issued guidance requiring financial institutions to take measures to detect and prevent these attacks.

The IBM® Security Trusteer suite of products effectively protects tens of millions of endpoints all over the world against malware and phishing threats. Unlike other solutions that don't have a global footprint, IBM's distinctive and proprietary intelligence enables our solutions to rapidly adapt to emerging threats, shutting down the criminals' window of opportunity.

IBM Security Trusteer endpoint protection solutions eliminate malware from the endpoint and alert users before they submit their credentials to phishing sites. IBM also offers a clientless solution to accurately detect malware infections and phishing incidents in real-time. This detection capability enables customers to take automated fraud mitigation actions and streamline their fraud prevention processes by focusing on truly high risk transactions and account access.

IBM's holistic fraud prevention incorporates account compromise history based on malware and phishing attack data with device reputation and risk factors to accurately detect complex, multi-vector attacks. IBM's unique visibility to the entire fraud life cycle enables organizations to mitigate fraud risk from the online and mobile channels and eliminate the overhead of forensic investigations and recovery of funds. By eliminating fraud risk, organizations protect their customers' assets, maximize adoption of online channels, and protect their brand and the overall customer experience.

For more information

To learn more about the IBM Security Trusteer portfolio of fraud prevention solutions, contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

IBM Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

October 2014