KASPERSKY lab

Kaspersky Fraud Prevention: a Comprehensive Protection Solution for Online and Mobile Banking

Today's bank customers can perform most of their financial activities online. According to a global survey conducted by B2B International and Kaspersky Lab, 60% of Internet users regularly use online banking services. At the same time, three quarters of respondents would like banks to provide special solutions to protect their financial transactions.

Most banks fight cyber-fraud with multifactor authentication and transaction approval services. They also make use of encryption technologies when transmitting data between an online service and a user's device. But there are some disadvantages to these approaches. Firstly, the use of additional authentication methods can negatively influence the user experience. Secondly, these measures are not always enough to prevent fraud: cybercriminals have an array of tools that help them to bypass the standard protective barriers used by banks. Fraudsters see a client as a weak link, so they write sophisticated malware, create fake bank web pages and use social engineering tricks in an attempt to reach a customer's bank account.

According to Kaspersky Lab, individual customers fall victim to malicious activity more often than banks do. In 2014, Kaspersky Lab products detected 22.9 million financial malware attacks, targeting 2.7 million users worldwide. Moreover, financial phishing attacks, including those against banks, payment systems and e-shops, accounted for 28.73% of all phishing attacks. This means that traditional protection methods used by banks could be in vain if users' devices are not secured. Of course, it is not possible to install a special security application on every user device. That is why there are clientless solutions that reside inside the bank's infrastructure and ensure an additional layer of protection by analyzing banking operations on clients' devices.

Banks can take several steps to deal with online financial fraud: prevention, detection, investigation and legal action. The earlier a bank begins protective action, the less expensive and the more effective it will be. That is why Kaspersky Lab suggests introducing countermeasures as early as possible — before the fraud happens.

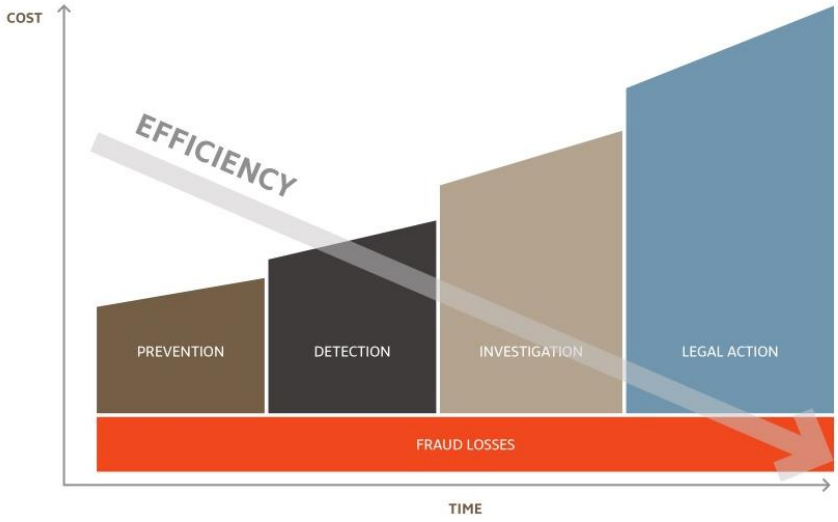

Figure 1. The process costs and efficiency of fighting fraud over time

For many years, Kaspersky Lab has been developing technologies for protection against all types of cyberthreats, including those targeting the financial sector. Using this experience, Kaspersky Lab has developed Kaspersky Fraud Prevention – a comprehensive security solution to counter online banking fraud. The platform provides multi-layered protection for online and mobile banking.

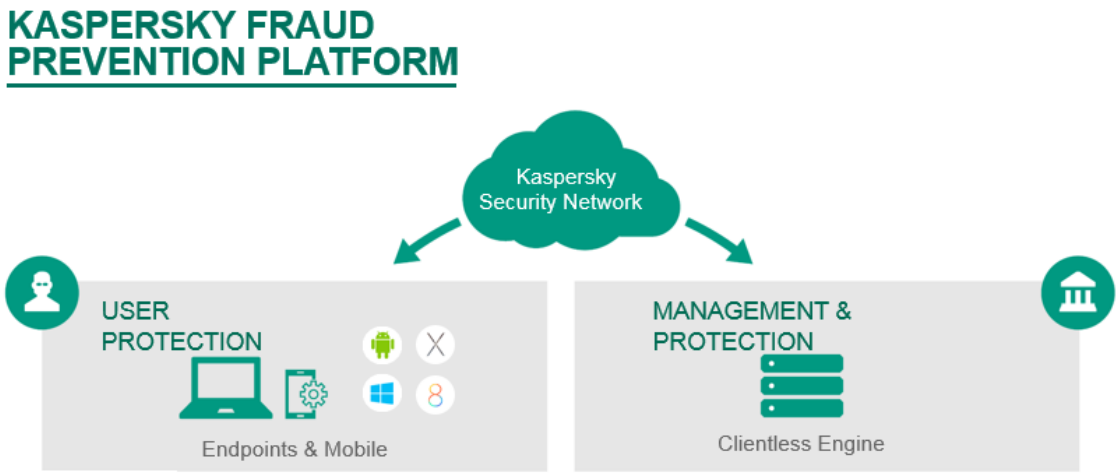

Figure 2. Kaspersky Fraud Prevention subsystems can work separately or in conjunction with each other, providing efficient multi-layered protection

Detecting fraudulent activity from within the bank

The main component of the Kaspersky Fraud Prevention platform is a Clientless Engine that enables banks to internally detect a fraudulent activity. The service detects infected user devices and notifies the bank's fraud prevention team. It employs two different approaches: passive and active.

Passive detection is a fast, signature-based method. It uses a JavaScript code integrated into the bank's web page. When a client addresses the bank's page, the code runs in their browser and searches for the signatures of web injections that are known to be dangerous to this exact URL.

The active method involves a "honeypot". This emulates popular online banking scenarios to provoke financial malware that can be hiding on a user device to reveal itself.

Another feature of the Clientless Engine is the live monitoring of user devices. This involves looking through data about a client's payment activity, the operating systems and browser they use and, most importantly, any security incidents they have faced, such as malware, vulnerabilities and phishing attempts. It gives banks management capabilities that allow them to remotely change settings, if needed.

The Clientless Engine can send statistics to internal transaction monitoring systems, increasing the detection rate and decreasing the number of false positives. Information transmitted to a bank from endpoints is exclusively for internal use and storage.

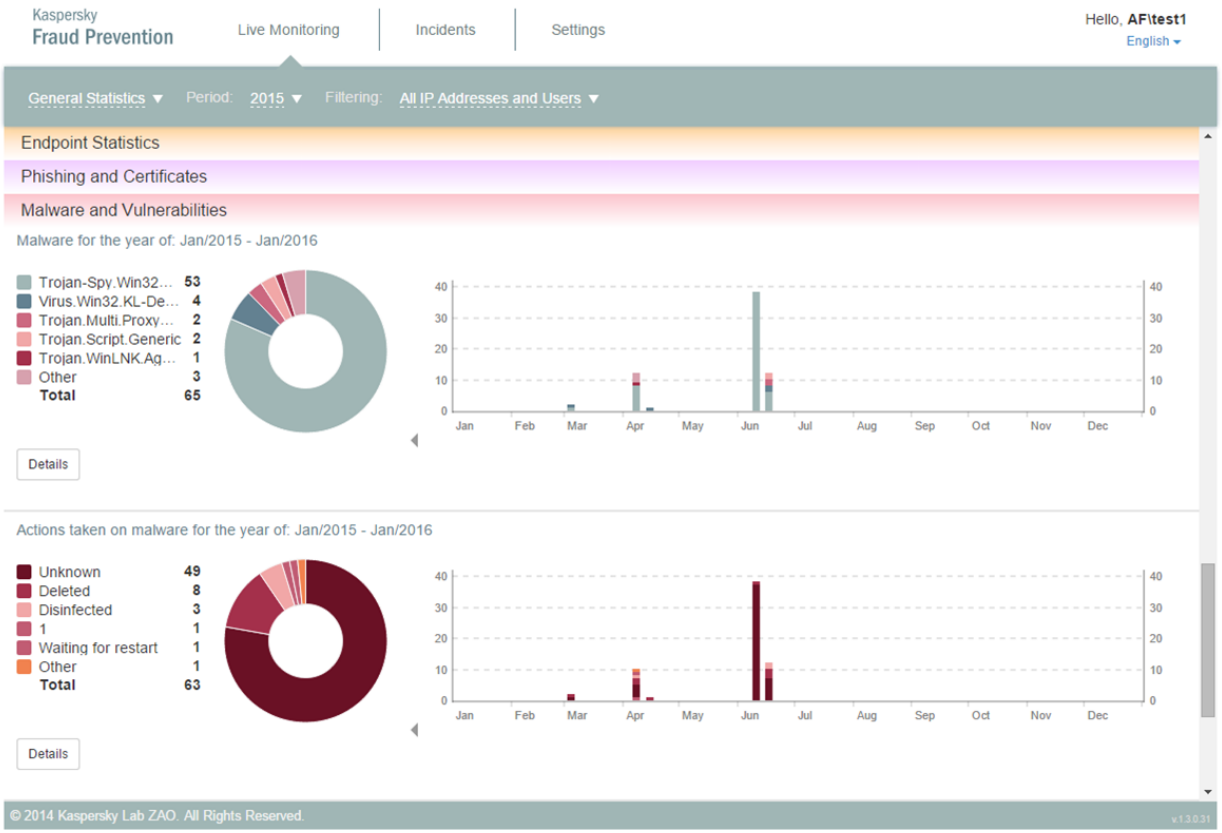

Figure 3. Kaspersky Fraud Prevention Management Console interface with malware statistics

Client-side protection

Users do not always install security solutions. Those that do can rely on generic antivirus products that don't have dedicated defenses against complex financial attacks. According to the survey, just about 60% of computers based on the OS X operating system and mobile devices on the Android platform are equipped with security solutions, while one in ten Windows devices also has no protection. This places banks' money and reputation at risk. That is why the Kaspersky Fraud Prevention platform contains specific protection technologies that ensures users of online banking are safe. It includes two main subsystems for the protection of customers' devices: a solution for Endpoints and a mobile SDK.

Kaspersky Fraud Prevention for Endpoints

Kaspersky Fraud Prevention for Endpoints works on the client's side for Windows and OS X operating systems. It ensures that the environment for financial transactions is safe and checks the authenticity of websites using the following methods:

- Performs a vulnerability check of the operating system and system applications
- Scans the computer for financial malware
- Analyses the bank's web page opened by the client to determine whether it is a phishing site
- Verifies the site's SSL certificate through the Kaspersky Security Network
- Opens the page in 'protected' mode to ensure that all personal data is protected against theft or modification
- Prevents keystroke interception by allowing the use of a Virtual Keyboard that is displayed on the screen and controlled with the mouse

In order to resist platform-specific threats, the version for Windows also employs the following methods:

- It verifies DLL signatures locally in order to block any attempts to introduce malicious code into the browser process (such as fake input fields)
- Blocks attempts to take screenshots
- Protects access to the clipboard, where passwords or login data could be stored for some time
- Activates the Secure Keyboard driver that protects data input from a hardware keyboard

Kaspersky Fraud Prevention SDK

The Kaspersky Fraud Prevention platform includes a Software Development Kit (SDK) that allows applications secured against online financial fraud to be created for Android, iOS or Windows Phone platforms. The bank's IT security specialists are free to equip these applications with various protection technologies intended to combat threats specific to each platform.

The protection technologies available include countermeasures against the most widespread threats – anti-malware and anti-phishing engines, DNS Checker, Web Antivirus and so on. The complete list of these technologies and information about their availability for each of the platforms can be found in Appendix.

Benefits of Kaspersky Fraud Prevention

- The solution has been created by world-renown cybersecurity experts with a deep understanding of modern financial threats and banks' needs
- It reduces the costs of investigating incidents by preventing them in the first place
- It can be operated alongside the bank's existing security solutions as an additional, proactive layer
- The methods employed in Kaspersky Fraud Prevention are developed with exceptional care for the user experience and exert minimum influence on user behavior
- Kaspersky Security Network delivers the most up-to-date information, enabling protection from the very latest financial threats, even if they were launched in the Internet just minutes before
- It covers most popular platforms and also offers clientless protection
- The endpoint protection solution is white-labeled and can be branded by a bank

The Kaspersky Fraud Prevention platform uses an advanced, multi-layered security system where the components enhance each other to deliver maximum protection. As a result, Kaspersky Lab's solution allows banks to reduce to a bare minimum the risk of cybercriminal incidents and subsequent financial and reputational costs.

Appendix: Kaspersky Fraud Prevention SDK

Feature	Description	iOS	Android	Windows Phone
Anti-Phishing and Fake Apps Protection				
Fake Apps Protection	Detects in real time whenever the banking application's window is concealed by another application, which may be malicious.		■	
Anti-phishing	Uses KSN to analyze every URL it encounters to identify whether it displays characteristics typical of a phishing website.	■	■	■
Financial Malware Protection				
Malware Scan and Removal	Runs in the background and actively scans the user's device for malicious files.		■	
Secure Connectivity				
Certificate Validation	Verifies the authenticity of a website using a database of trusted banking system addresses and the corresponding SSL certificates of individual banks stored in the Kaspersky Security Network (KSN).	■	■	
DNS Checker	Protects against DNS spoofing by using KSN data to verify that the financial organization's domain name corresponds to a trusted IP address.	■	■	■
Web Antivirus	Checks site content for malicious code in the body of the web page and scans incoming traffic.	■	■	■
URL Web Filter	Enables monitoring of web traffic on user devices and intercepts attempts to connect to insecure URLs.		■	■
Wi-Fi Safety Analysis	Checks the Wi-Fi connection used and verifies whether it's secure and trusted (e.g. secured with WPA, WPA2, WEP or not) using KSN to obtain Wi-Fi hotspot reputation.	■	■	
Device Protection				
Device Configuration	Checks if a user has the latest version of the OS and notifies about existing system vulnerabilities. It also includes firmware verification if all updates have been installed on the device.	■	■	■
Root / jailbreak detect	Detects if a device has been rooted or jailbroken, and sends an alert to both the user and the bank.	■	■	

Suspicious applications detection	Detects suspicious and potentially dangerous applications, including those which send / receive SMS, contain bank-specific data, take screenshots and request root permissions.		■	
Screenshots detection	Detects any attempt to take screenshots.	■		
Second Factor Protection				
Data input protection	Protects entered data (e.g. account credentials) from interception with secure data entry component (Secure Keyboard) and secure entry field (Secure Input).	■	■	
Secure SMS	An incoming SMS from the bank can be intercepted by malware. A mechanism in the KFP SDK intercepts incoming SMS messages sent by the bank, deletes them from the inbox and moves them to secure storage before any other process can get access to them.		■	
Secure data storage	Secure Storage is a protected folder where a user can store account information or other sensitive information. Verified SMS messages from banks are automatically routed to this secure location.	■	■	■
Self-defense				
Self-Defense	Ensures protection against injections and real-time modifications to the application code, runs application integrity checks in case intruders attempt to switch off the user's protection and disables debugging mode.	■	■	