KASPERSKY lab

# KASPERSKY FRAUD PREVENTION FOR ENDPOINTS

www.kaspersky.de

# KASPERSKY FRAUD PREVENTION

## 1. Methoden für den Angriff auf Onlinebanking-Systeme

Das Hauptmotiv hinter Angriffen auf Online-Banking ist finanzieller Natur. Cyberkriminelle von heute verfügen über eine breite Palette von Möglichkeiten, mit denen sie Online-Banking-Systeme und Online-Finanzdienstleister angreifen können. Egal, ob Malware eingesetzt wird, um legitime Transaktionen an eigene Konten umzuleiten, oder mit einer Kombination aus Social Engineering und Phishing versucht wird, Zugang zu Bankkonten zu erlangen – Online-Betrüger verwenden viele unterschiedliche Methoden, um an das Geld von Onlinebanking-Kunden zu kommen.

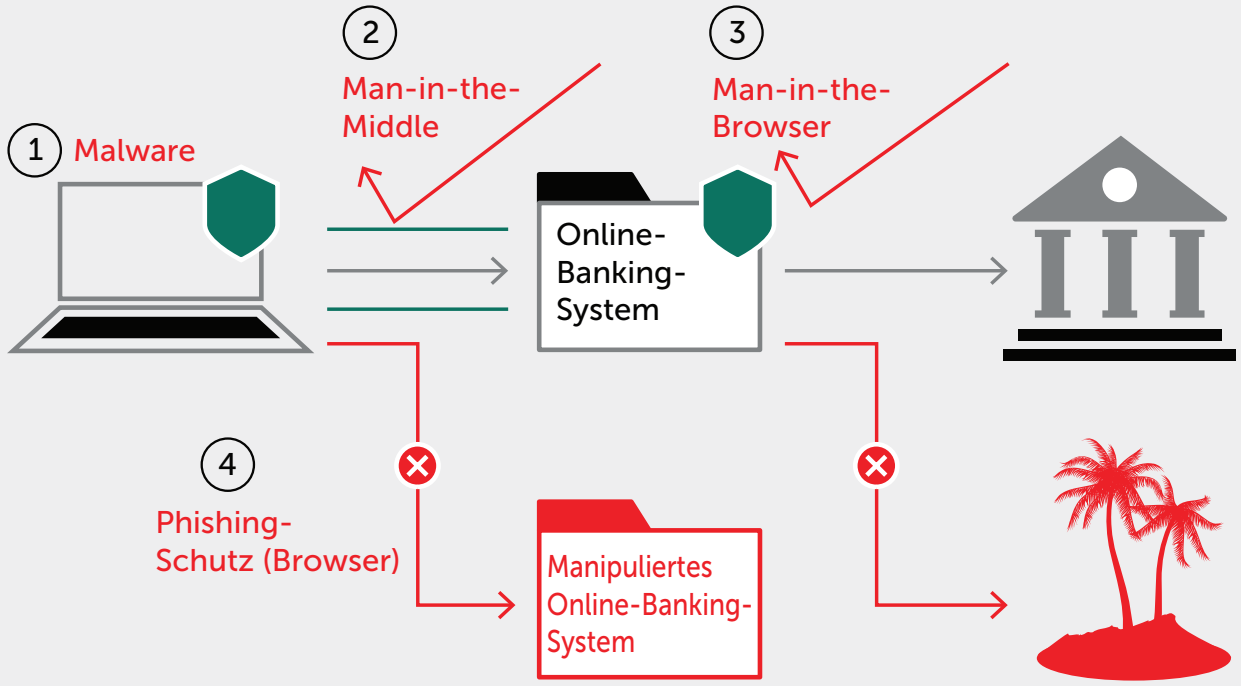
Zwei Hauptmethoden lassen sich unterscheiden:

- **Kontoübernahme:** Zugangsdaten zu Online-Konten werden abgefangen, die Konten anschließend geplündert.
- **Manipulation von Transaktionen:** Änderung der Transaktionsdetails bzw. Erstellen einer neuen Transaktion im Namen des Kunden

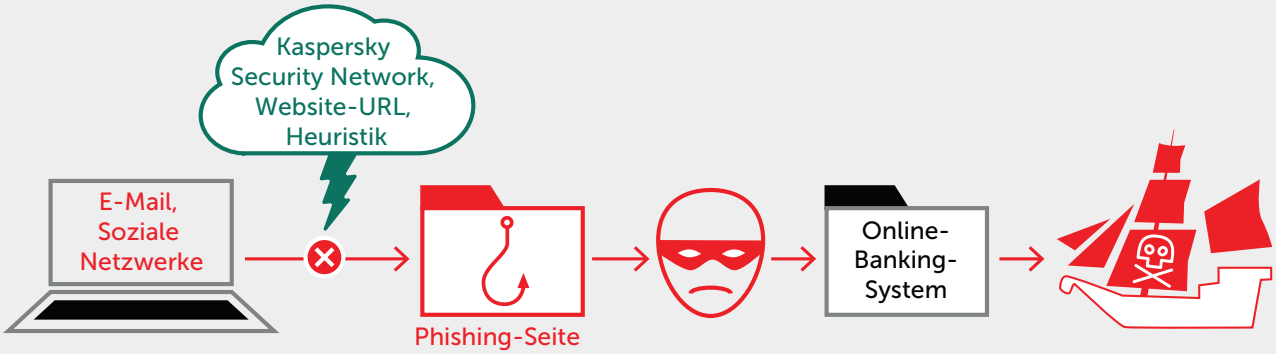
Beides wird in der Regel durch eine Kombination unterschiedlicher Verfahren erreicht, u. a. durch:

- Diebstahl von Zugangsdaten
- Phishing
- Webseitenmanipulation (Web-Injects)
- Formgrabbing
- Keylogging
- Screenshotting
- Spoofing-Angriffe
- Manipulation von Transaktionen
- Man-in-the-Middle-Attacken (MITM)
- Fernzugriff
- Man-in-the-Browser-Attacken (MITB)

# 2. Betrugsschutz in Aktion




## 2.1 Scannen und Entfernen von Malware



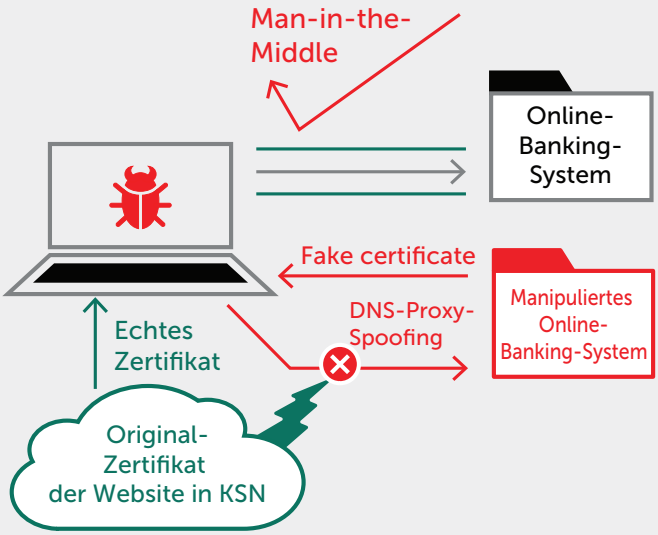

Selbst wenn sich auf dem Computer des Benutzers bereits Malware befindet, kann Kaspersky Fraud Prevention Online-Transaktionen immer noch schützen. Unmittelbar nach der Installation führt Kaspersky Fraud Prevention einen Systemscan aus, um nach Banking-Malware zu suchen. Wird die Software fündig, wird der Benutzer gefragt, ob die Datei(en) gelöscht werden soll(en) und ob das System bereinigt werden soll. Zusätzlich wird jedes Mal ein Scan ausgeführt, wenn der sichere Browser für Online-Transaktionen gestartet wird.

FALLSTUDIE

Eine große russische Bank wurde zum Opfer einer Malware, die die Bankkunden automatisch an eine Phishing-Seite umleitete. Hierdurch wurden die Benutzer nicht nur dazu verleitet, ihre Kontozugangsdaten preiszugeben, es war danach für sie auch nicht mehr möglich, auf die echte Webseite der Bank zuzugreifen. Kaspersky Fraud Prevention konnte die Malware von den Computern der Kunden entfernen und den Online-Zahlungsverkehr der Kunden wieder sicher machen.

Kaspersky Fraud Prevention for Endpoints ist mit allen führenden Anti-Malware-Produkten kompatibel und einzig und allein darauf ausgelegt, Banking-Malware aufzuspüren. Es sollte als Ergänzung zu herkömmlichen Anti-Malware-Lösungen, nicht als Ersatz eingesetzt werden.

## 2.2 Schutz von Internetverbindungen




Kaspersky Fraud Prevention stellt nicht nur sicher, dass der Computer zu einer sicheren Umgebung für das Online-Banking wird und eine echte Banking-Webseite aufgerufen wird. Unsere Lösung garantiert außerdem, dass keine Manipulation der Internetverbindung zwischen Bank und Kunde stattfinden kann.

Jedes Mal, wenn ein Benutzer sich für eine Online-Banking-Sitzung anmeldet, überprüft Kaspersky Fraud Prevention das Sicherheitszertifikat der Webseite. Hierzu wird dieses mit dem Referenzzertifikat verglichen, das im Kaspersky Security Network hinterlegt ist. Dieser Abgleich verhindert Man-in-the-Middle-Angriffe sowie DNS- und Proxy-Spoofing.

Wird ein verdächtiges Zertifikat gefunden, alarmiert das System den Benutzer.

## 2.3 Schutz vor Browser-Bedrohungen

### 2.3.1 EXTERNE BROWSER-KONTROLLE

Kaspersky Fraud Prevention for Endpoints bietet durch Meldungen an die Browser-Fenster Schutz vor externer Browser-Kontrolle. Cyberkriminelle können also keinen Remote-Zugriff auf den Browser erhalten.

### 2.3.2 CODE-INJEKTIONEN

Schützt vor dem Hochladen nicht vertrauenswürdiger Module während der Browserausführung. Hierzu wird die DLL-Signatur anhand der lokalen Datenbank und in der Cloud (KSN) verglichen.

### 2.3.3 SCHUTZ VOR SNAPSHOTS

Der Schutz vor Snapshots beinhaltet:

- Schutz vor Screenshotting-Techniken
- Schützt das aktuell im abgesicherten Browser geöffnete Fenster

### 2.3.4 BS-SCHWACHSTELLENPRÜFUNG

Eigene, aktualisierbare Schwachstellendatenbank:

- Nur Betriebssystem
- Nur Eskalation der Kernel-Modus-Berechtigungen

### 2.3.5 SICHERE TASTATUR

Im abgesicherten Browser-Modus schützt Kaspersky Fraud Prevention for Endpoints alle Eingabefelder. Kaspersky Fraud Prevention fängt sämtliche Tastaturanschläge ab und verarbeitet diese über den KFP-Tastaturtreiber. Hierdurch wird verhindert, dass die eingegebenen Daten von Malware abgefangen werden. Die Sichere Tastatur kann im Sicheren Browser und in normalen Browserfenstern eingesetzt werden.

### 2.3.6 SCHUTZ DER ZWISCHENABLAGE

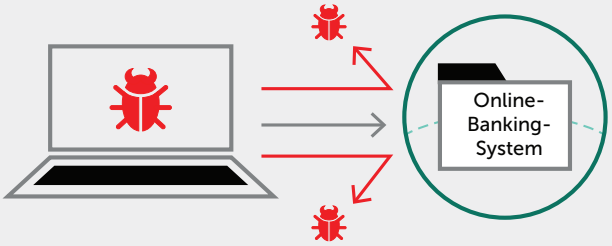
Verhindert, dass nicht vertrauenswürdige Programme auf die Zwischenablage zugreifen.

### 2.3.7 SELBSTSCHUTZ

Schützt Kaspersky Fraud Prevention for Endpoints vor Manipulationen an der Software selbst.

- Windows-Registrierungsschlüssel
- Dateien
- Prozesse
- Threads

## 2.4 Phishing-Schutz für den Browser




Für den Phishing-Schutz von Kaspersky Lab werden heuristische und Cloud-basierte Technologien mit herkömmlichen Offline-Datenbanken kombiniert. So wird sichergestellt, dass sogar neu entstehende, noch nicht registrierte Bedrohungen, abgewehrt werden können.

Das Cloud-basierte Anti-Phishing-Modul wird beständig aktualisiert und enthält Masken mit Phining-URLs. Neue Bedrohungen werden bereits Sekunden nach ihrer Entdeckung hinzugefügt, wodurch eine Erkennung von Phishing-Websites möglich wird, die in lokalen Datenbanken noch nicht erfasst sind. Immer wenn ein Benutzer auf eine URL trifft, die noch nicht in der lokalen Datenbank vorhanden ist, wird diese automatisch mit der Cloud-Datenbank abgeglichen.

Die heuristische Webkomponente des Anti-Phishing-Systems wird aktiviert, sobald der Benutzer auf den Link zu einer Phishing-Webseite klickt, die noch nicht in den Datenbanken von Kaspersky Lab gespeichert ist.

Zusätzlich enthält eine lokal auf dem Benutzergerät abgelegte Anti-Phishing Offline-Datenbank die gängigsten Masken mit Phishing-URLs.

# 3. Kaspersky Fraud Prevention Console

Zur Vereinfachung der Verwaltung besitzt Kaspersky Fraud Prevention for Endpoints nur eine Verwaltungskonsole, die umfassende Informationen über den Benutzer, das verwendete Gerät und die Sitzung bietet.

## 3.1 Reporting-Dashboard

Die Konsole erfasst Informationen aus Kaspersky Fraud Prevention for Endpoints über das Gerät, die Sitzungen und die Umgebung des Benutzers sowie über etwaige Attacken, die auf dem Computer des Benutzers gestartet wurden (Phishing, MAN-IN-THE-BROWSER, MAN-IN-THE-MIDDLE, Malware).

## 3.2 Remote-Konfiguration

Die Konsole verfügt über Management-Funktionen, mit denen sich Kaspersky Fraud Prevention for Endpoints per Fernzugriff konfigurieren lässt.

## 3.3 Statistik-Feed

Die Konsole besitzt eine Integrationsschnittstelle, über die Statistiken an interne Systeme, die die Transaktionen überwachen, gesendet werden können. Hierdurch wird die Erkennungsrate verbessert und die Anzahl der Fehlalarme (False-Positives) verringert.

## 4. Details zur Implementierung

Die Integration läuft normalerweise in drei Schritten ab:

**1.** Anpassen der Lösung an die Anforderungen der Bank, um einen benutzerdefinierten Onlinebanking-Dienst zu erstellen: Mit unserem White-Labeling-Modell können Banken ihre eigene, maßgeschneiderte Benutzeroberfläche mit eigenen Logos, Farbschemata, Schriftarten und Layouts erstellen. Auch die Desktop- und Systempaletten-Symbole lassen sich nach Bedarf anpassen.

**2.** Integration mit den bankeigenen Systemen: Kaspersky Fraud Prevention for Endpoints ermöglicht es, beim Herstellen der Verbindung zu einer Online-Bank Details zu Produktversion und -status abzurufen. Diese Informationen werden, wie in der Dokumentation beschrieben, über ein spezielles Skript abgerufen. Wir empfehlen im Wesentlichen drei unterschiedliche Arbeitsszenarios, aber jede Bank kann mit den abgerufenen Daten nach eigenem Ermessen verfahren.

**3.** Die Bank hat nun die Wahl, wie sie ihren Kunden das Programm zur Verfügung stellen möchte. Es empfiehlt sich zu überprüfen, ob Kaspersky Fraud Prevention bereits auf dem Computer des Benutzers ausgeführt wird, und Kaspersky Fraud Prevention dann bei Bedarf zum Download anzubieten. Die Bank kann aber auch eine andere Bereitstellungsmethode wählen. Um die Rechenressourcen der Bank zu schonen, liegt ein Großteil des Programms auf den Kaspersky-Servern. Der eigentliche Zugriff erfolgt dann über eine 2 MB große Download-Datei, die der Bank während der Implementierungsphase zur Verfügung gestellt wird.

Der vollständige Installationsprozess dauert in der Regel zwei Wochen. Kaspersky Lab stellt während der Installationsphase ein spezielles Implementierungsteam ab, das bei der Integration der Lösung in das Bankennetzwerk behilflich ist und sich etwaiger Probleme annimmt.

Kontaktieren Sie uns, um mehr zu erfahren: KFP@kaspersky.com
http://www.kaspersky.com/de/business-security/fraud-prevention



Whitepaper zu Kaspersky Fraud Prevention for Endpoints, August 2015 GL