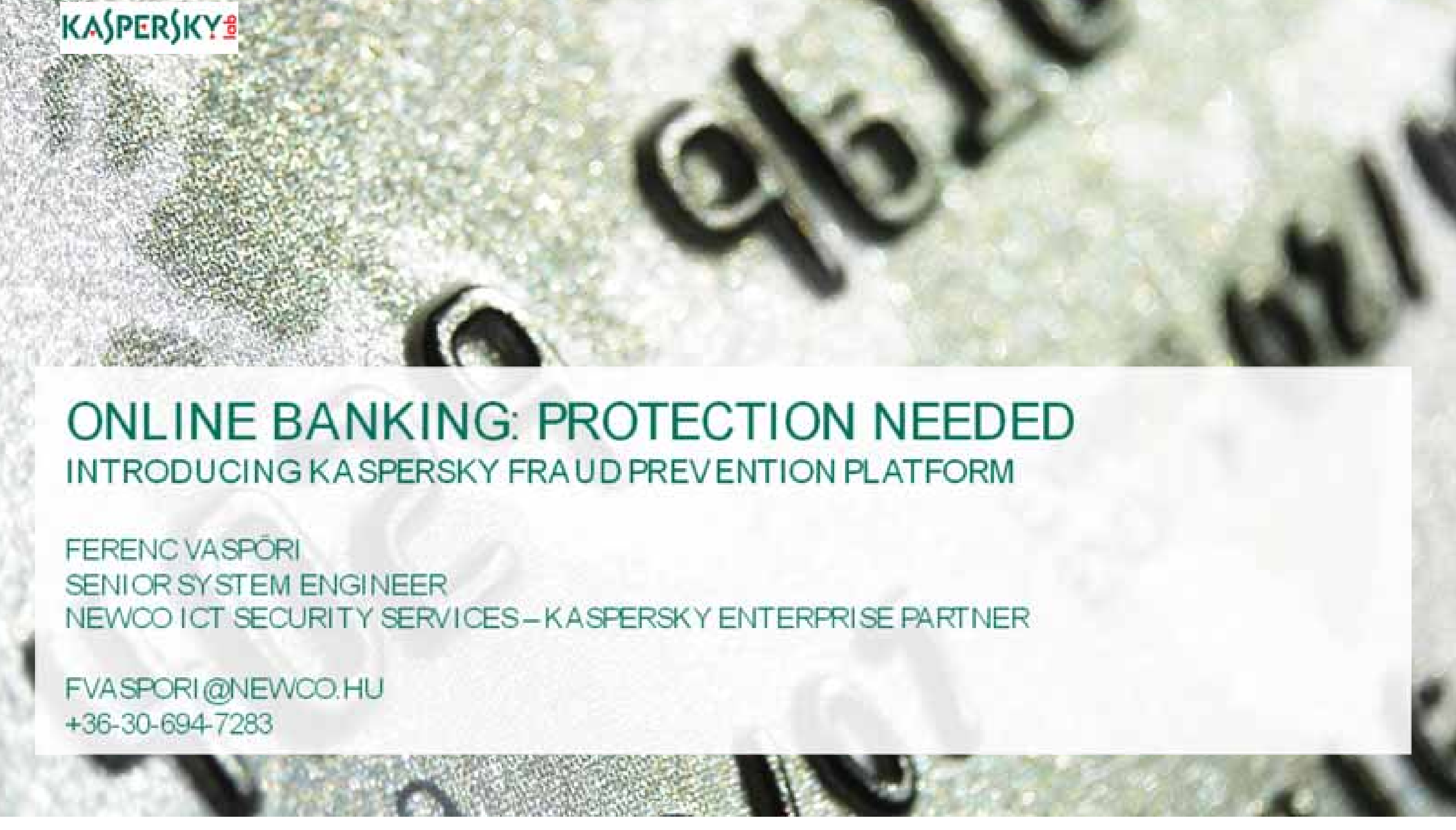


ONLINE BANKING: PROTECTION NEEDED

INTRODUCING KASPERSKY FRAUD PREVENTION PLATFORM

FERENC VASPÖRI
SENIOR SYSTEM ENGINEER
NEWCO ICT SECURITY SERVICES – KASPERSKY ENTERPRISE PARTNER

FVASPORI@NEWCO.HU
+36-30-694-7283

NEWCO ICT SECURITY SERVICES SNAPSHOT

IT security focus only

20 years of technical experience

Enterprise sized customers

Strategic partnership with Kaspersky

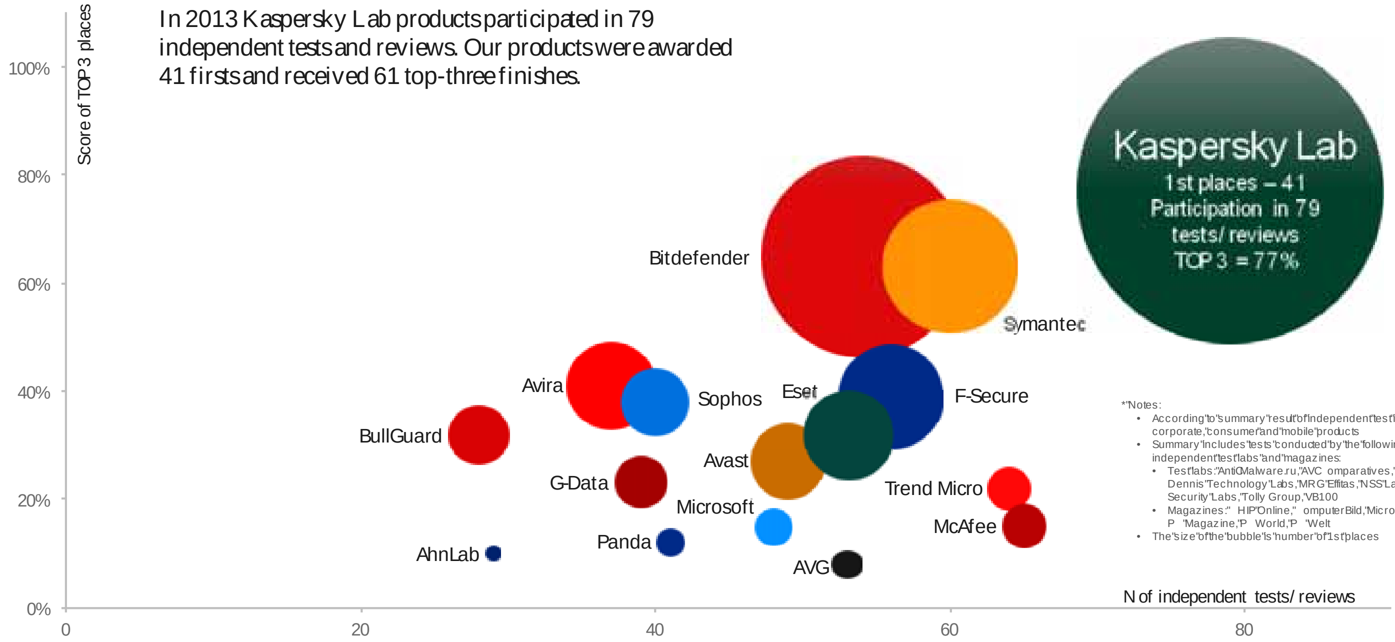
newco ICT SECURITY SERVICES

SOME VENDORS JUST PLAY IN THE SECURITY SPACE — WE DEFINE IT

- Kaspersky is a robust security leader with almost 20 years of experience in the security space
- We have a global threat intelligence made up of 300 mln protected users worldwide
- Kaspersky's main asset is security intelligence and a unique set of protection technologies
- We're not just technology focused — we're security focused too

KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION*

In 2013 Kaspersky Lab products participated in 79 independent tests and reviews. Our products were awarded 41 firsts and received 61 top-three finishes.



*"Notes:

- According'to'summary'result'of'independent'test'in'2013'for' corporate,'consumer'and'mobile'products
- Summary'includes'tests'conducted'by'the'following' independent'test'labs'and'magazines:
  - Test'labs:'AntiCMalware.ru,'AVC omparatives,'AVCTest,' Dennis'Technology'Labs,'MRG'Effitas,'NSS'Labs,'P " Security'Labs,'Tolly Group,'VB100
  - Magazines:" HIP'Online," omputerBild,'Micro'Hebdo," P 'Magazine,'P World,'P 'Welt
- The'size'of'the'bubble'is'number'of'1st'places

© 2014 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their

MATURE TECHNOLOGY WITH MILLIONS OF THANKFUL USERS WORLDWIDE

- Fraud Prevention technology was introduced by Kaspersky Lab in 2011 under the name of Safe Money
- Safe Money used by 30+ mln endpoint users of Kaspersky Lab products

BARCLAYS

AL-ARAFAH ISLAMI BANK LIMITED

NORTHSTAR BANK
OF TEXAS
www.nstarbank.com

Eastern Bank Ltd.
Simple. Math.

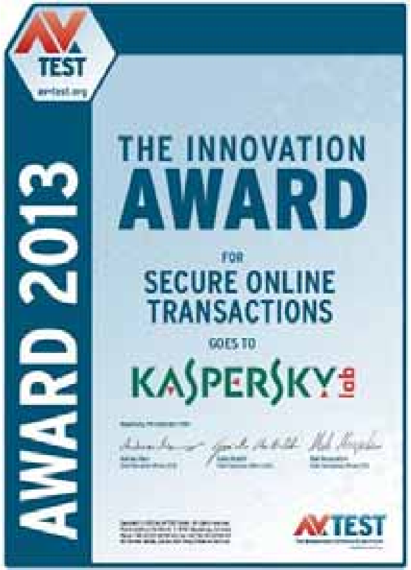
BASIC

Southeast Bank Limited
a bank with vision

Shahjalal Islami Bank
Limited
Committed to Cordial Service

Leading bank in Ecuador, 750,000 online users covered

BEST ONLINE BANKING PROTECTION. NOW.
AV-TEST INNOVATION AWARD 2013



AWARD 2013

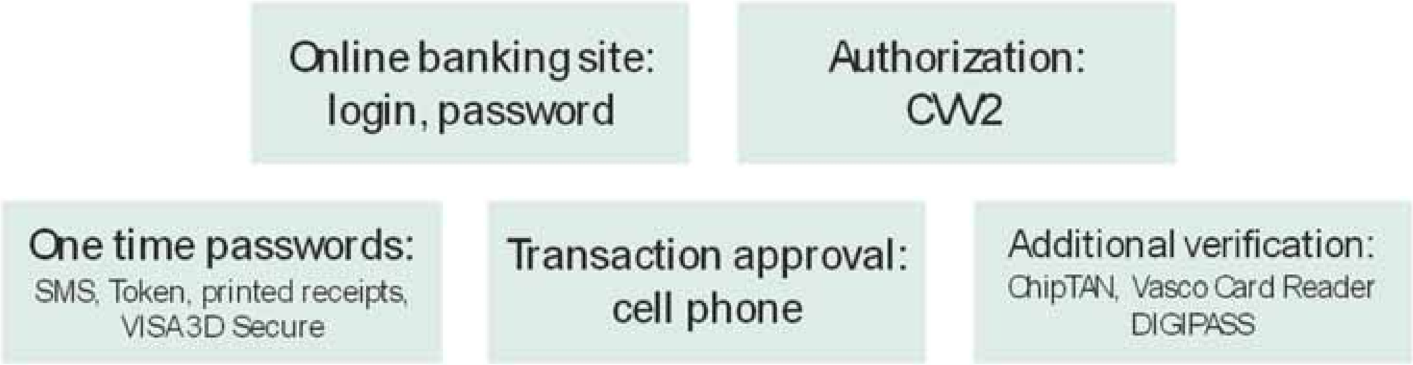
THE INNOVATION AWARD FOR SECURE ONLINE TRANSACTIONS GOES TO KASPERSKY lab

AV TEST
av-test.org
AV TEST

> “The security products produced by the company Kaspersky Lab have been standing out due to rapid and continuous improvements in their level of protection for many years.
> Kaspersky Lab was therefore recently presented with the AV-TEST INNOVATION AWARD 2013 in the category of Secure Online Transactions in recognition of its pioneering role in the pursuit of and battle against online criminals.”

ATTACKING THE BANK VS. ATTACKING THE USER

MODERN PROTECTION MECHANISMS USED BY BANKS



Online banking site:
login, password

Authorization:
CVV2

One time passwords:
SMS, Token, printed receipts,
VISA 3D Secure

Transaction approval:
cell phone

Additional verification:
ChipTAN, Vasco Card Reader
DIGIPASS

SECURITY TIPS ON HUNGARIAN NETBANK SITES

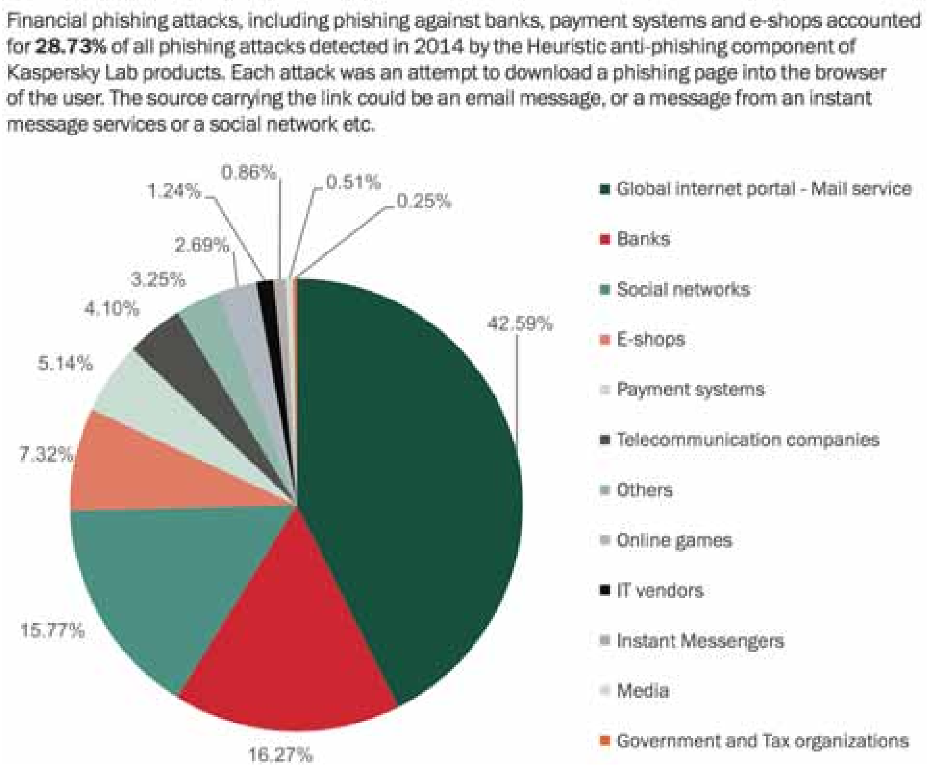
TOP-ADVICES-(it"can be"read on 7"Hungarian banks'"site)

- Be"aware of"phishing campaigns
- Use strong password
- Upda
- Secu

- Log"
- Do not use netbank"from a"public place
- Update"your OS"and"browser
- Remove the temporary internet"files of"your browser

- Check your balance continuously"(!!)
- Check the certificate of"the site.
- Install firewall for home use.

DO YOU THINK THIS IS ENOUGH?



Financial phishing attacks, including phishing against banks, payment systems and e-shops accounted for **28.73%** of all phishing attacks detected in 2014 by the Heuristic anti-phishing component of Kaspersky Lab products. Each attack was an attempt to download a phishing page into the browser of the user. The source carrying the link could be an email message, or a message from an instant message services or a social network etc.

DO YOU THINK THIS IS ENOUGH?

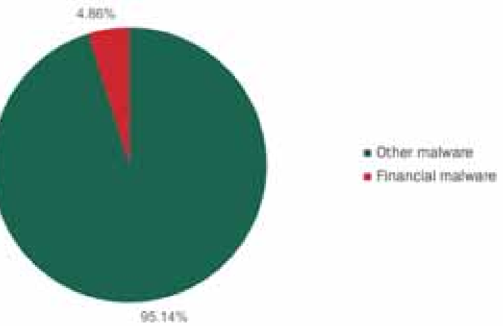
steal+any+bank+information+from+computers

cannot+be+visually+traced+and+is+thus+hard+to+detect

rootkit+technologies+as+selfH+defense

penetrate+computers+by+visiting+infected+Internet+pages

8m+attacked+were+detected+globally



Banking malware

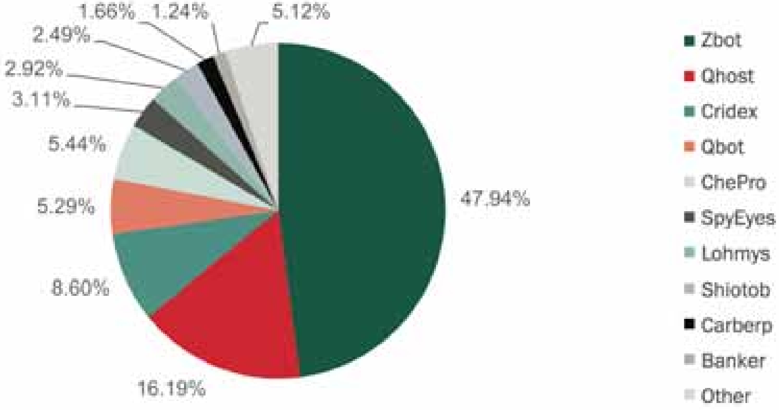
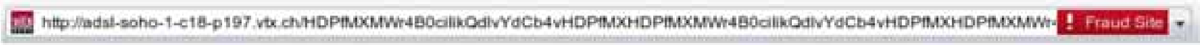


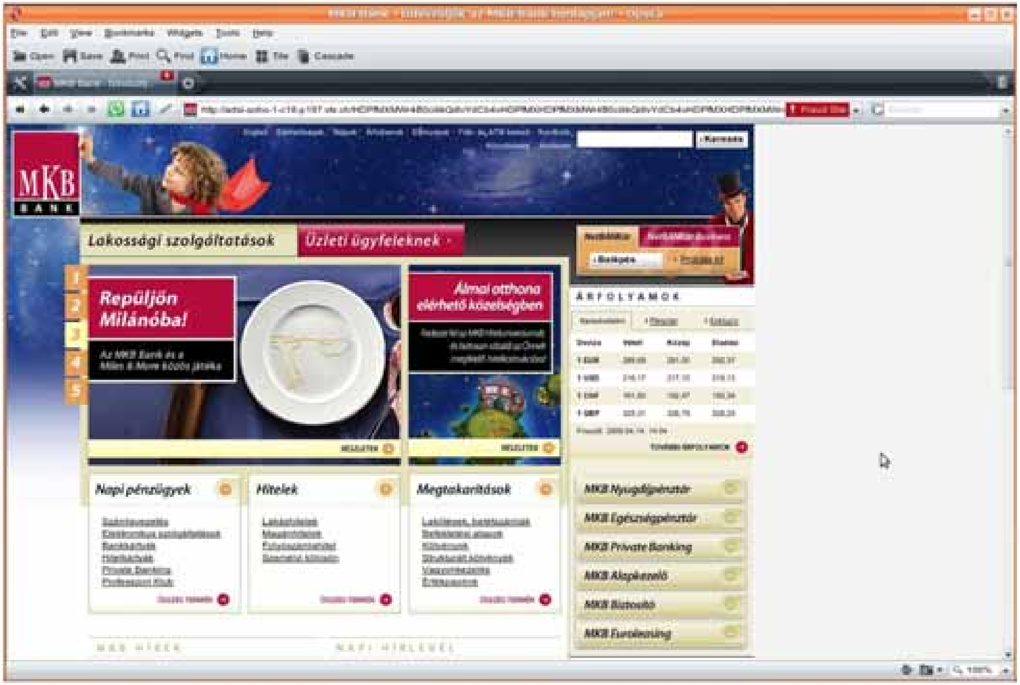
Fig 11. Top 10 of the most often used banking malware families

As can be seen on the pie chart above, only 10 families of malware are responsible for more than 94% of all banking malware attacks. It comes as no surprise that the top position again goes to the infamous Zbot – the most widespread and one of the most dangerous banking malware families.

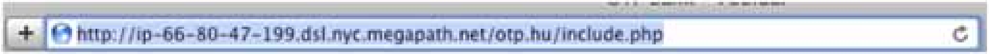
PHISHING EXAMPLES



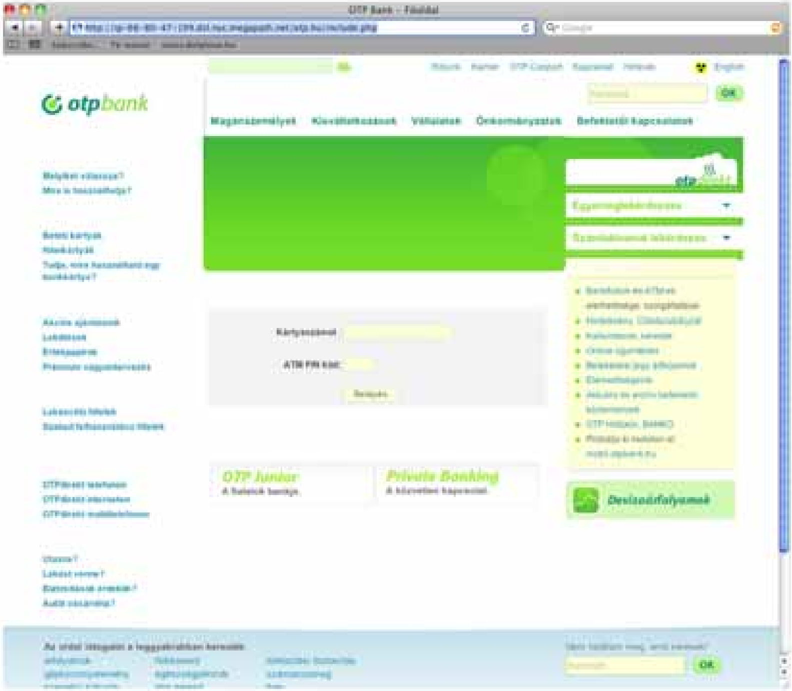
http://adsl-soho-1-c18-p197.vtx.ch/HDPfMXMWr4B0cilikQdlvYdCb4vHDPfMXHDPfMXMWr4B0cilikQdlvYdCb4vHDPfMXHDPfMXMWr



PHISHING EXAMPLES



http://ip-66-80-47-199.dsl.nyc.megapath.net/otp.hu/include.php

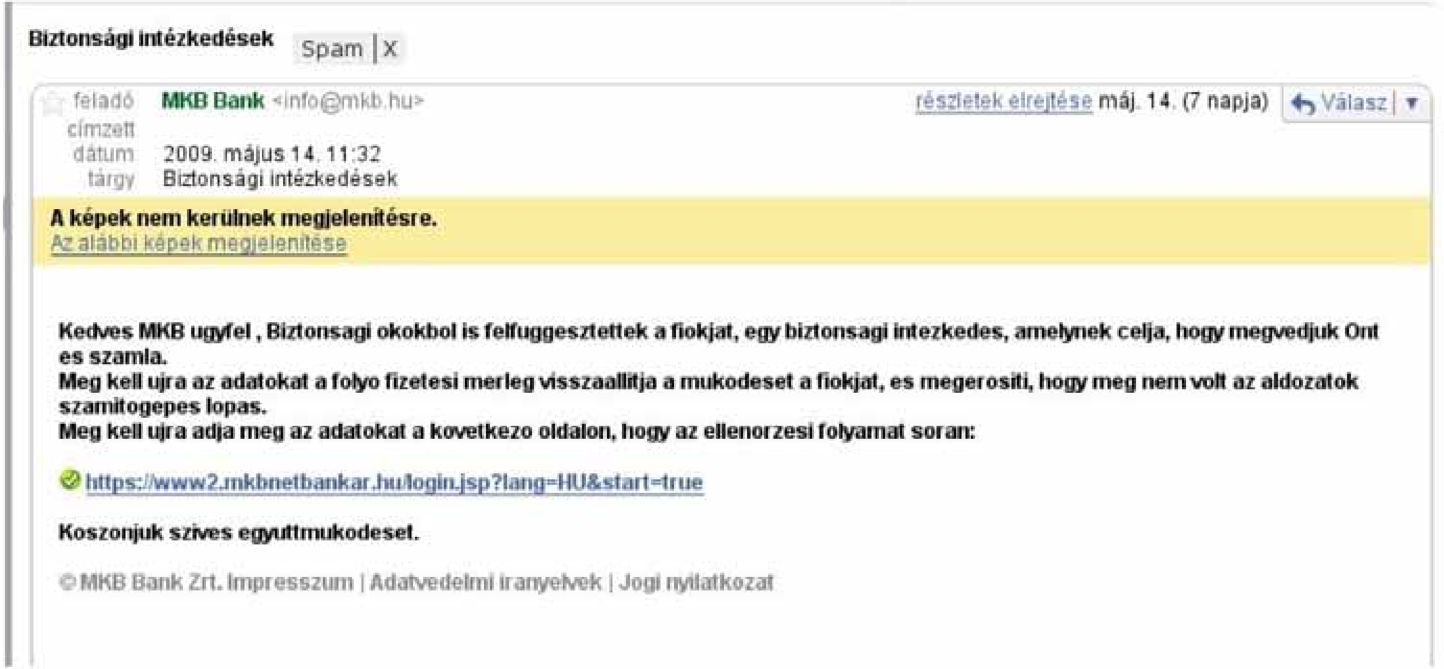


OTP Bank - Főoldal

Kártyaszám:

ATM PIN kód:

PHISHING EXAMPLES



Biztonsági intézkedések Spam | X

feladó **MKB Bank** <info@mkb.hu> részletek elrejtése máj. 14. (7 napja) Válasz

címzett

dátum 2009. május 14. 11:32

tárgy Biztonsági intézkedések

A képek nem kerülnek megjelenítésre.
Az alábbi képek megjelenítése

Kedves MKB ugyfel , Biztonsagi okokbol is felfuggesztettek a fiokjat, egy biztonsagi intezkedes, amelynek celja, hogy megvedjuk Ont es szamla.
Meg kell ujra az adatokat a folyo fizetesi merleg visszaallitja a mukodeset a fiokjat, es megerositi, hogy meg nem volt az aldozatok szamitogepes lopas.
Meg kell ujra adja meg az adatokat a kovetkezo oldalon, hogy az ellenorzesi folyamat soran:

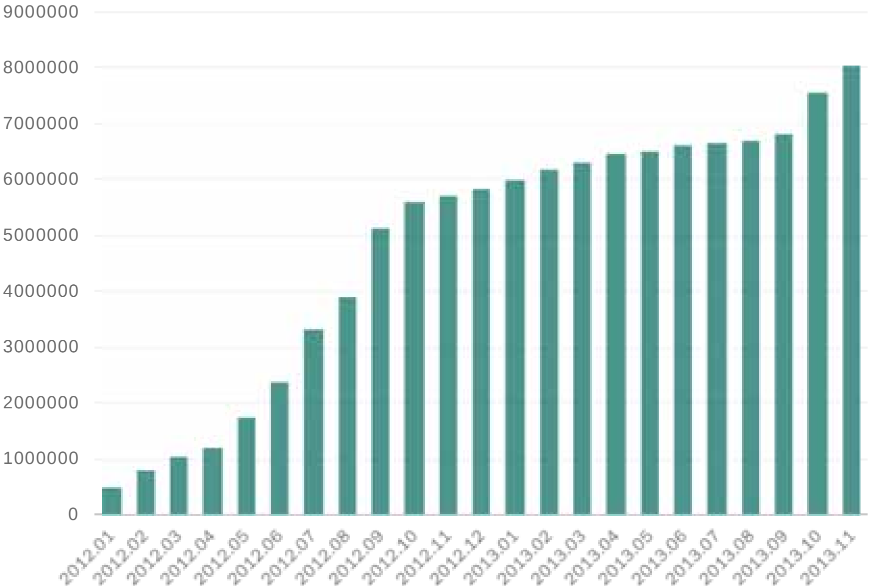
✓ **https://www2.mkbnetbankar.hu/login.jsp?lang=HU&start=true**

Koszonjuk szives egyuttmukodeset.

© MKB Bank Zrt. Impresszum | Adatvedelmi iranyelvek | Jogi nyilatkozat

ANDROID MALWARES

Malicious APK



First malware in'2004

10,000,000+

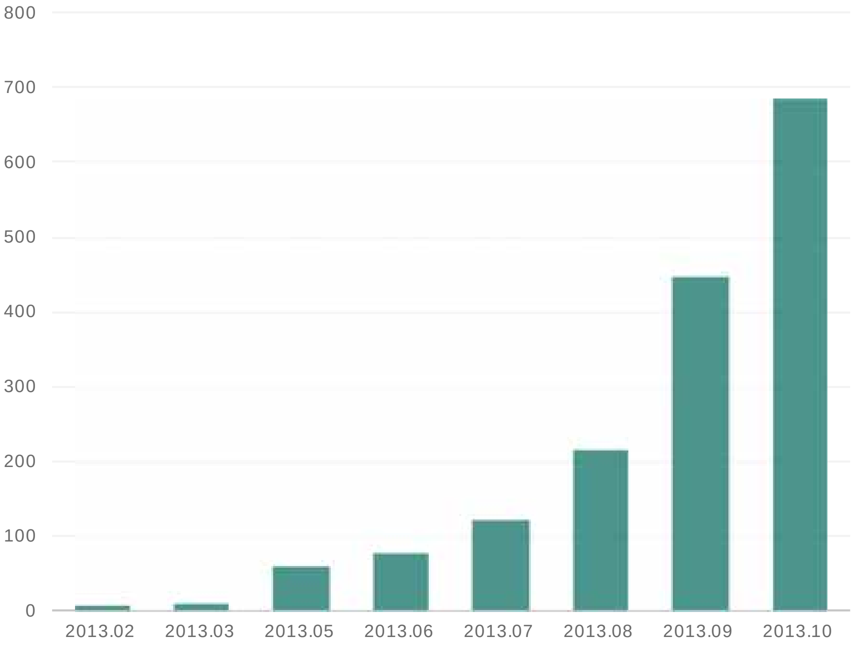
Total numbers of'Android malwares (Kaspersky'Lab)

120,000

Nem Android malware per" months

Source: Kaspersky Lab Security Network

ANDROID BANKING MALWARES



684

Android malwares affected banks

2,500

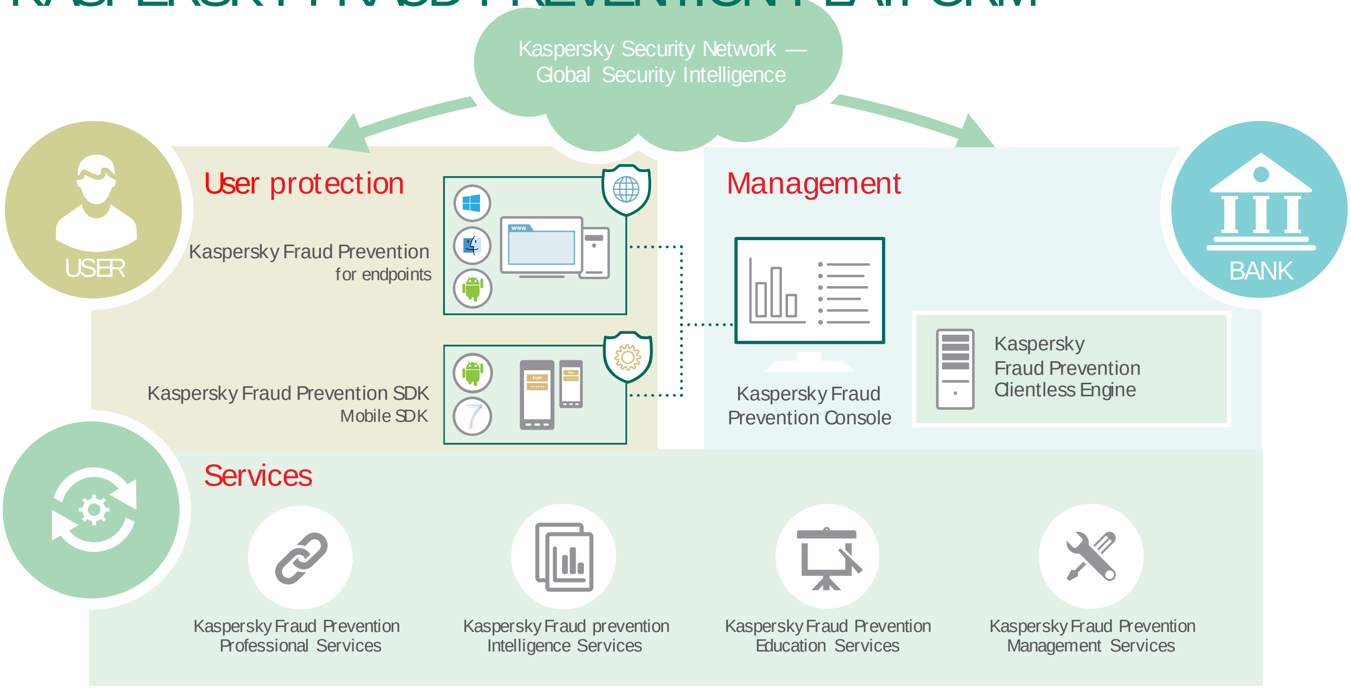
New"alerts per"month

x100

Increasing numbers per"year

Source: Kaspersky Lab Security Network

KASPERSKY FRAUD PREVENTION PLATFORM



Kaspersky Security Network — Global Security Intelligence

USER

BANK

User protection

Kaspersky Fraud Prevention for endpoints

Kaspersky Fraud Prevention SDK Mobile SDK

Management

Kaspersky Fraud Prevention Console

Kaspersky Fraud Prevention Clientless Engine

Services

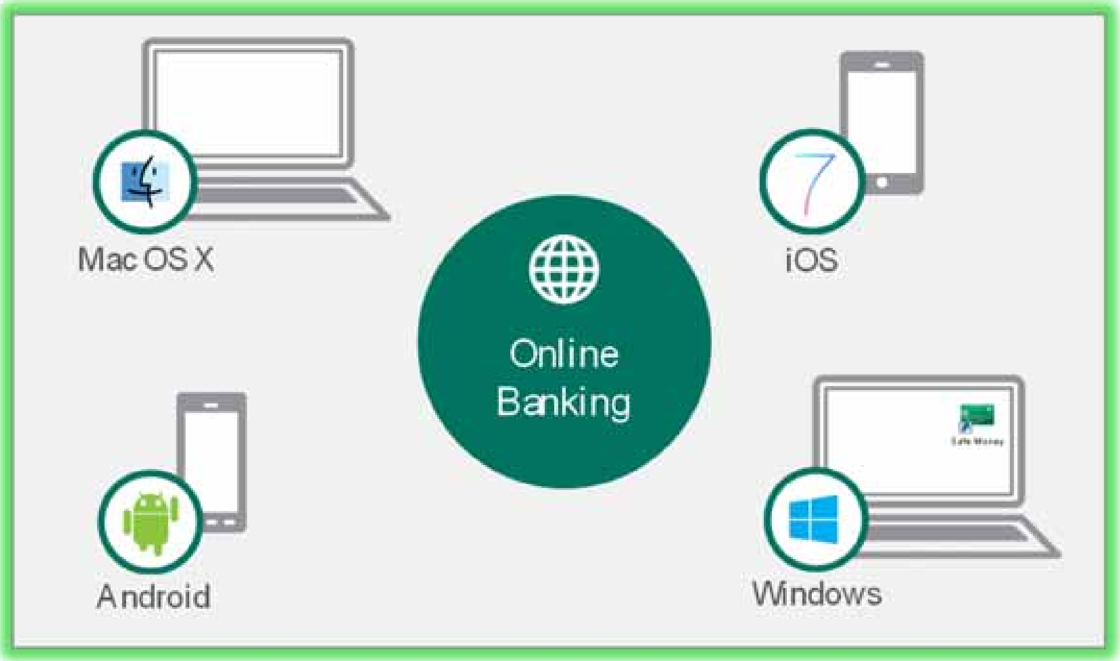
Kaspersky Fraud Prevention Professional Services

Kaspersky Fraud prevention Intelligence Services

Kaspersky Fraud Prevention Education Services

Kaspersky Fraud Prevention Management Services

1. USER PROTECTION - ALL PLATFORMS COVERED



Mac OS X

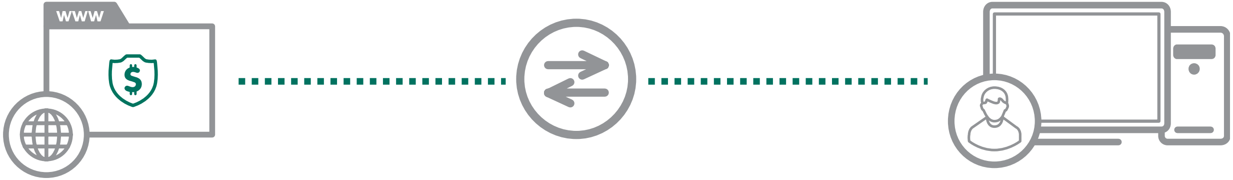
iOS

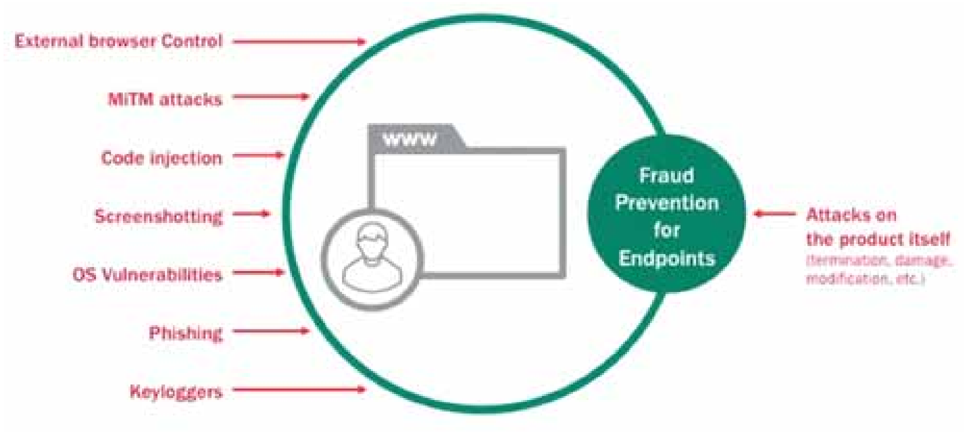
Online Banking

Android

Windows

KFP ON COMPUTERS





Secure connection

SSL"certificate"check

Phishing+detection

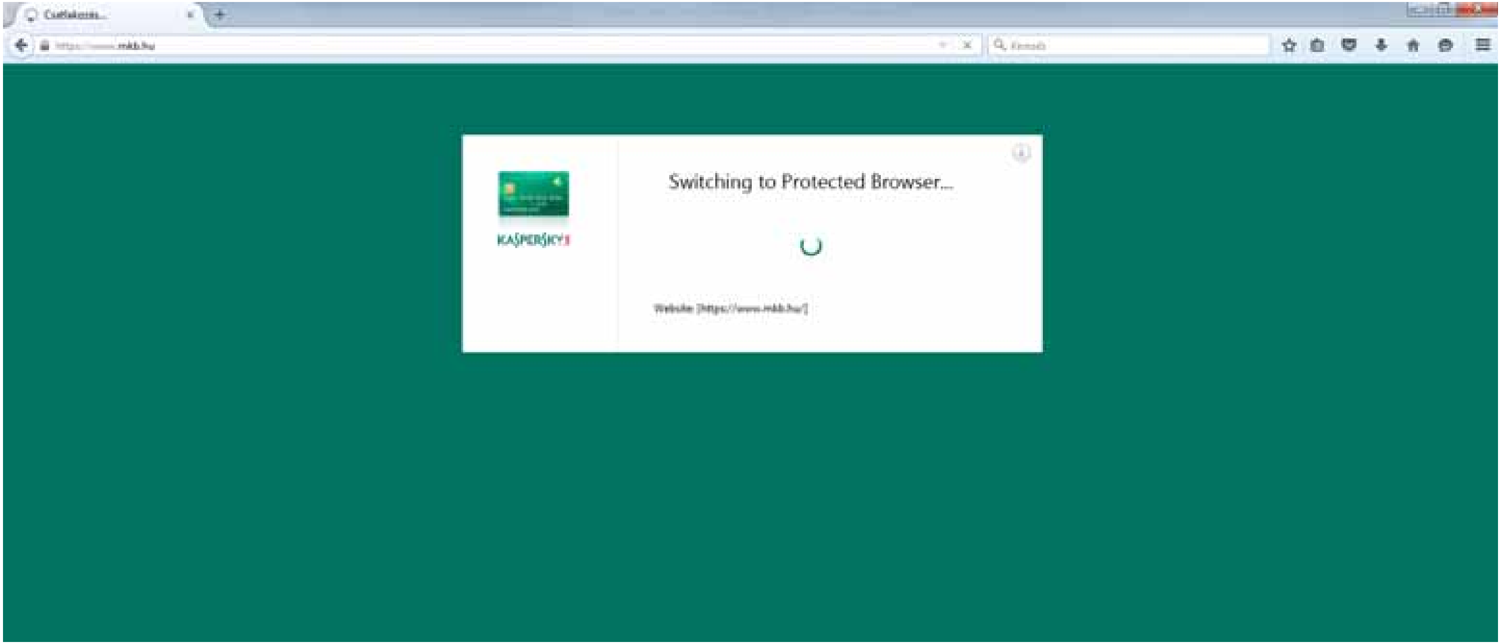
Secure browser+(antiH keylogging,+anti screenshot)

Vulnerability scan

USABILITY

- Installer of"the agent on netbank"sites
- Silent installer
- Browser"plugCin

- Automatic operation
  - Boot"of"the machine
  - Icon on desktop C>"NETBANK
  - Browser"plugin detects protected netbank"site
- ThirdCparty AVs"supported
- Rebranding,"custom language



Switching to Protected Browser...

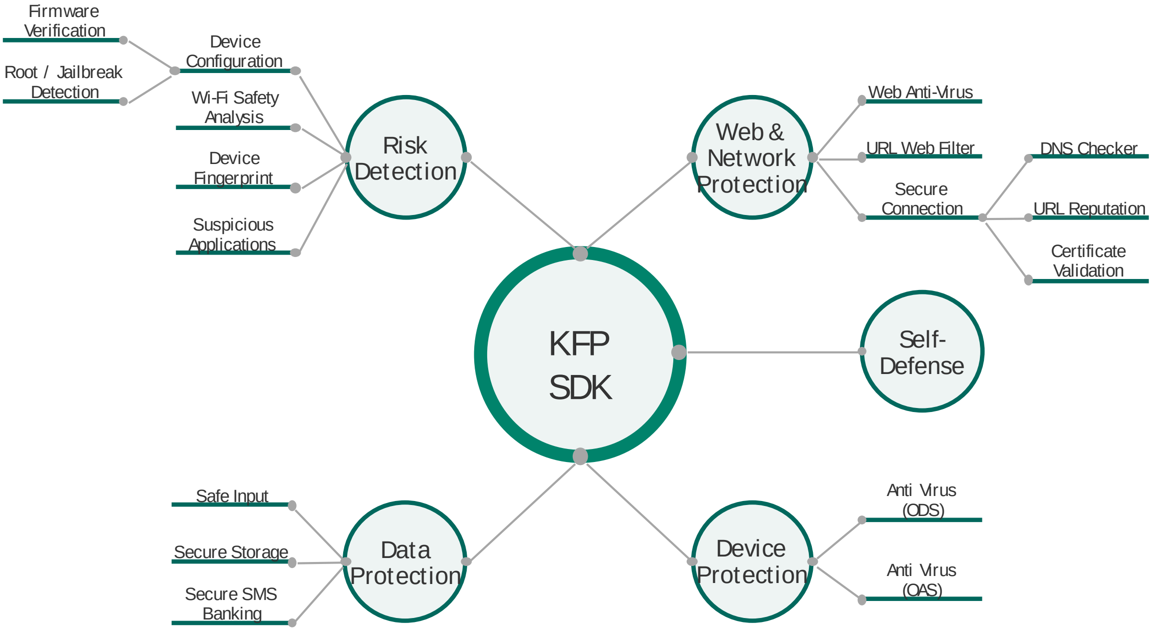
Website: [https://www.mkb.hu/]

WHY USE KFP FOR ENDPOINTS IF AN ANTIVIRUS SOLUTION IS ALREADY INSTALLED?

- Not all users install or update security software
- Traditional AV is vulnerable to zero-day and targeted attacks
- Kaspersky Fraud Prevention for Endpoints is compatible with most popular anti-malware solutions of other vendors

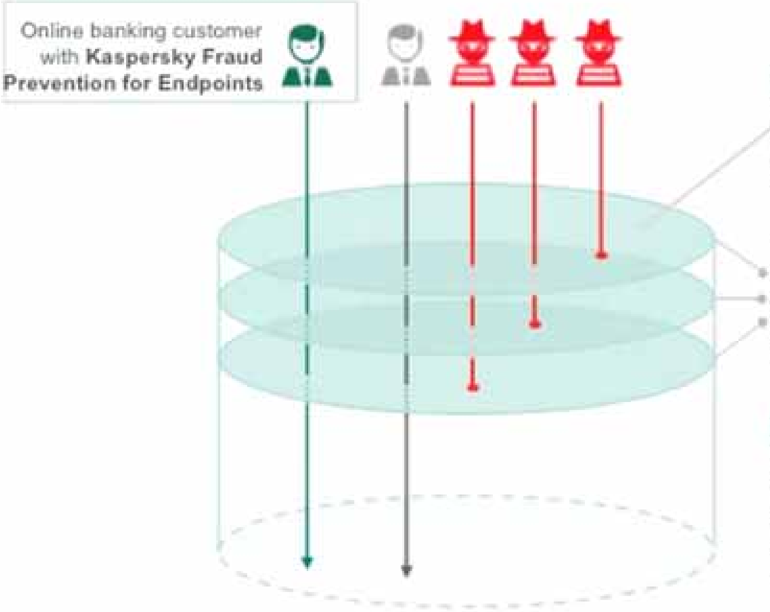
PROTECTION ON MOBILES– SOFTWARE DEVELOPMENT KIT

SDK$which can be$used in$developing own netbanking$app



KASPERSKY lab

2. SERVERSIDE – CLIENTLESS ENGINE


Online banking customer with **Kaspersky Fraud Prevention for Endpoints**

CLIENTLESS ENGINE

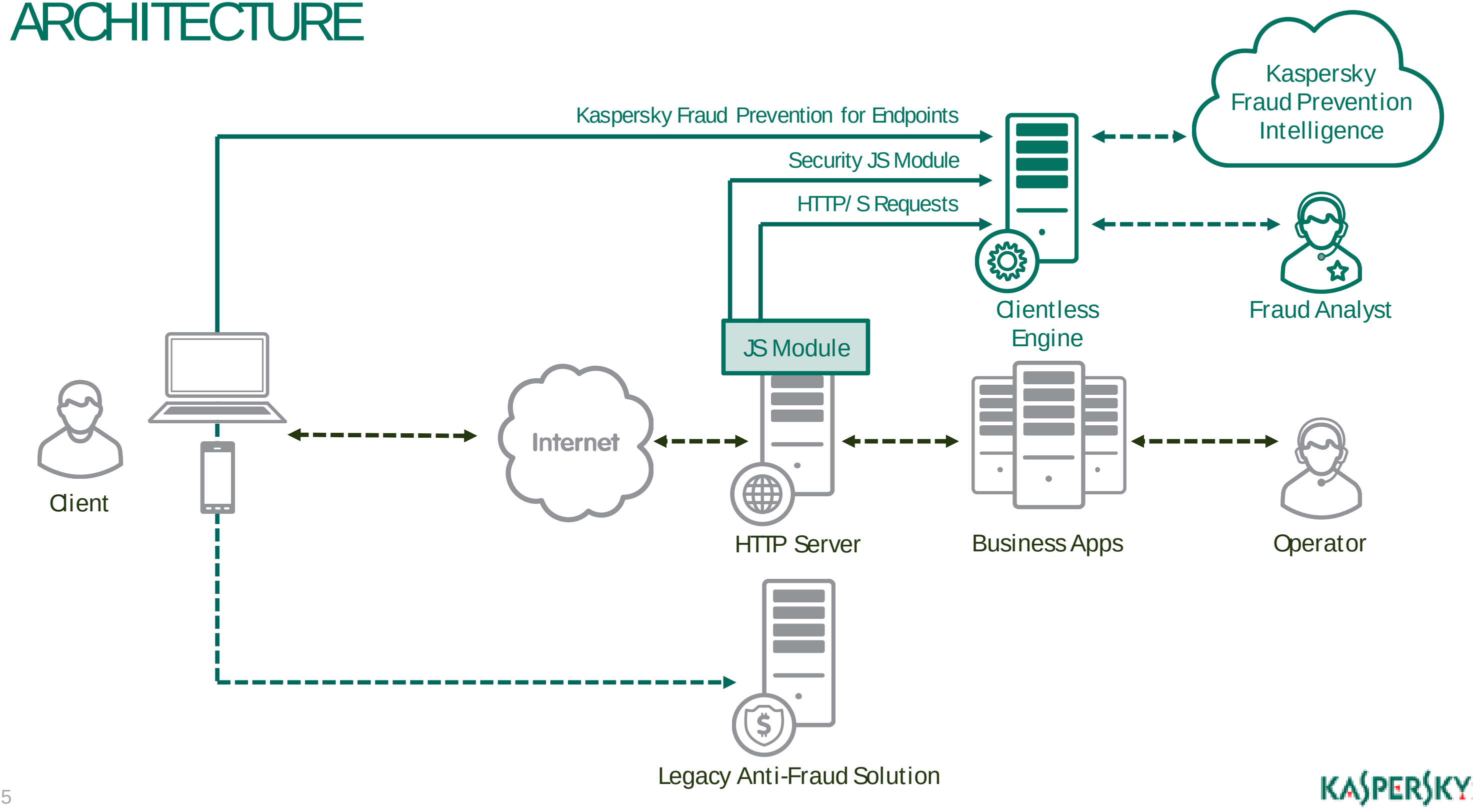
Multi-layered security approach with **Management Console.**

- Malware Detection Service
- Rule Engine
- Behavior Analysis

DATA SOURCES

- Kaspersky Fraud Prevention for Endpoints
- Kaspersky Security Network
- Online banking customers
- Fraud Analyst from Bank

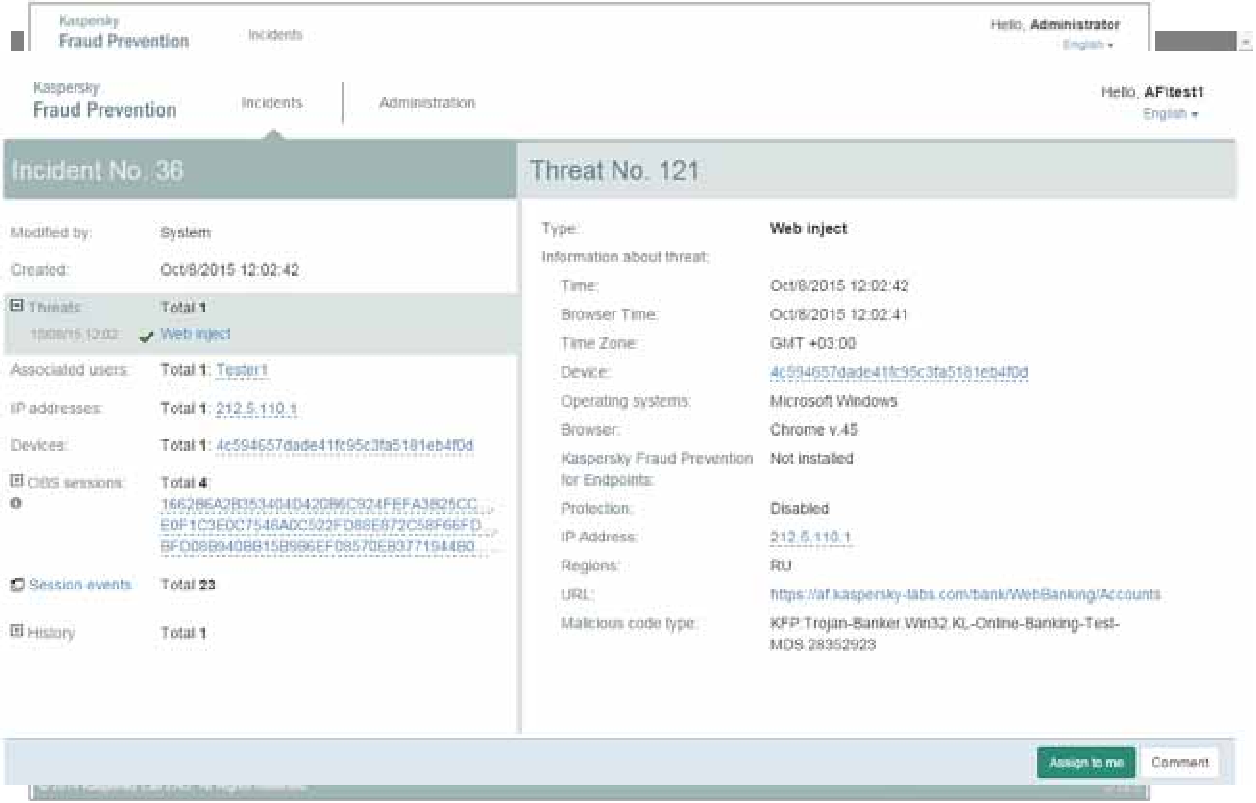
ARCHITECTURE



WHERE THE DATA COMES FROM

Collects data on three different levels:

- HTTP Server: http request and headers (for standard device fingerprinting)
- Kaspersky JS Module:
  - Transaction attributes (accounts, amount, date-time, comments/ reasons, …)
  - Browser info (plugins & versions) – advanced device fingerprinting
  - Structure of the user-facing Web page
  - User Behavior Pattern —link chain, mouse & keyboard events
- Kaspersky Fraud Prevention for Endpoints
  - Protection status
  - Presence of PUA apps (remote management software)
  - Usage of physical mouse & keyboard (advanced user-behavior pattern)



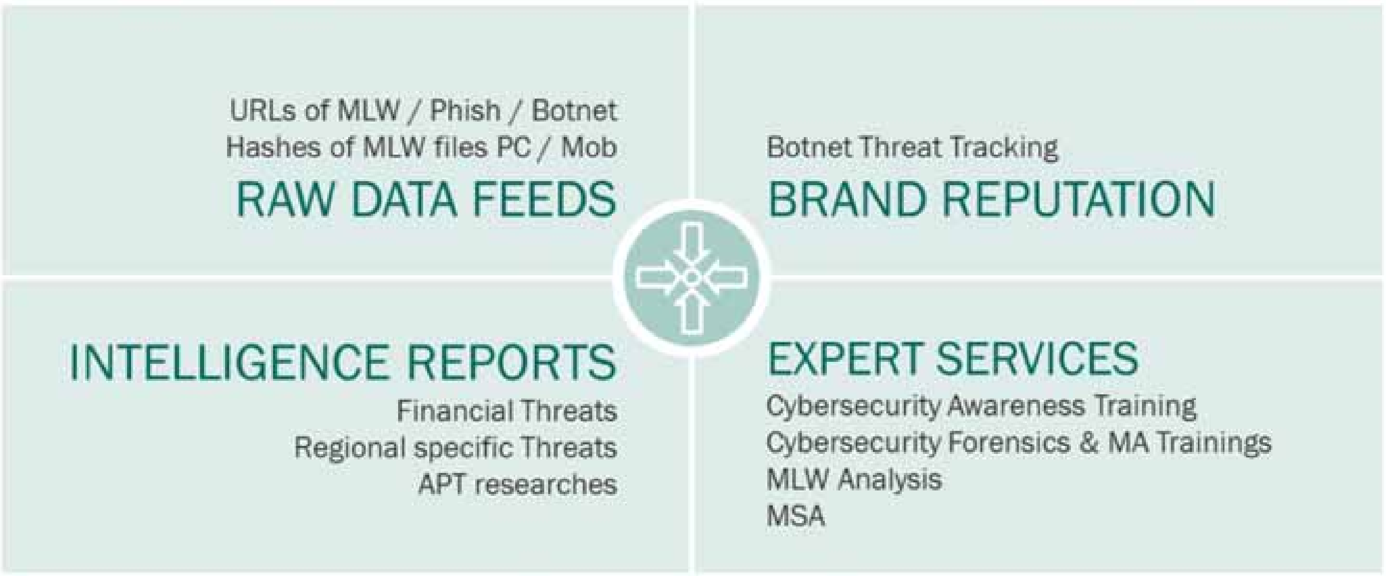
Incident No. 36

Modified by:	System
Created:	Oct/8/2015 12:02:42
⊟ Threats:	Total 1
10/08/15 12:02	✓ Web inject
Associated users:	Total 1: Tester1
IP addresses:	Total 1: 212.5.110.1
Devices:	Total 1: 4c594657dade41fc95c3fa5181eb4f0d
⊞ CBS sessions:	Total 4: 16628 6A2B35340D420B6C924FEFA3821CC... E0F1C3E0C7546A0C522FD88E872C58F66FD... BFD089940BB15B986EF08570EB37719448D...
Session events:	Total 23
⊞ History	Total 1

Threat No. 121

Type:	**Web inject**
Information about threat:	
Time:	Oct/8/2015 12:02:42
Browser Time:	Oct/8/2015 12:02:41
Time Zone:	GMT +03:00
Device:	4c594657dade41fc95c3fa5181eb4f0d
Operating systems:	Microsoft Windows
Browser:	Chrome v.45
Kaspersky Fraud Prevention for Endpoints:	Not installed
Protection:	Disabled
IP Address:	212.5.110.1
Regions:	RU
URL:	https://af.kaspersky-labs.com/bank/WebBanking/Accounts
Malicious code type:	KFP Trojan-Banker.Win32.KL-Online-Banking-Test-MDS.28352923

3. RELATED SERVICES



URLs of MLW / Phish / Botnet
Hashes of MLW files PC / Mob

RAW DATA FEEDS

Botnet Threat Tracking

BRAND REPUTATION

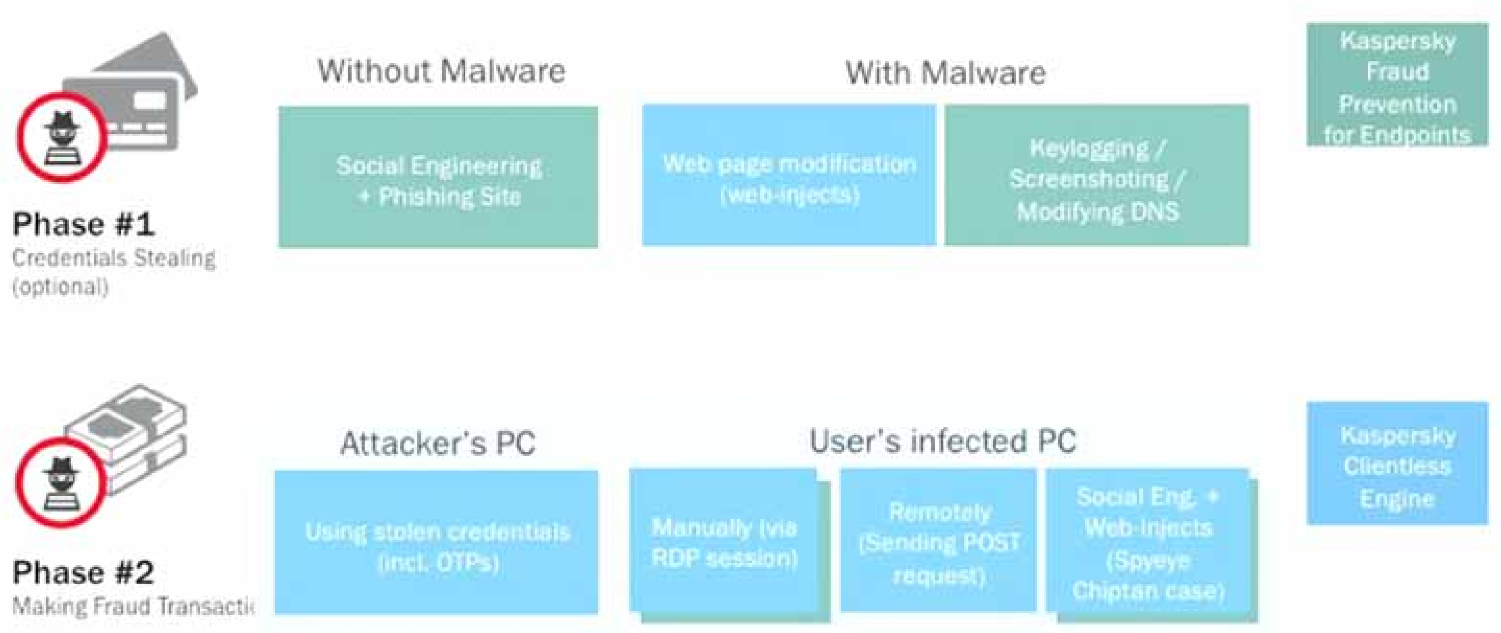
INTELLIGENCE REPORTS

Financial Threats
Regional specific Threats
APT researches

EXPERT SERVICES

Cybersecurity Awareness Training
Cybersecurity Forensics & MA Trainings
MLW Analysis
MSA

SEPARATE OR COMBINED COMPONENTS



Phase #1
Credentials Stealing (optional)

Without Malware

Social Engineering + Phishing Site

With Malware

Web page modification (web-injects)

Keylogging / Screenshoting / Modifying DNS

Kaspersky Fraud Prevention for Endpoints

Phase #2
Making Fraud Transacti

Attacker's PC

Using stolen credentials (incl. OTPs)

User's infected PC

Manually (via RDP session)

Remotely (Sending POST request)

Social Eng. + Web-Injects (Spyeye Chiptan case)

Kaspersky Clientless Engine

MAJOR BENEFITS FOR BANKS

- Minimizes the number of security incidents due to targeted attacks against online banking users
- Minimizes reputation risks

- Increases customer loyalty and awareness of threats
- Provides competitive advantage
- Motivates customers to use remote banking on different platforms: Windows, Mac OS X , Android, iOS

- Improves compliance with legal regulations
- Additional communication with clients

„Fraud+prevention+could+become+a+competitive+advantage+for+institutions+moving"forward,"as"Infosys”"survey"found"that"83%+of"the"respondents"said"they"would"switch"banks"if"they"were"offered"assurances"regarding"the"safety"of"their"money"and"data."Fighting"fraud"isn’t"enough anymore"for"banks "the"customer"needs"to"know"what"the"bank"is"doing"to"fight"fraud"and"be"involved"in"that"process.”

WHY KFP IS BETTER THAN COMPETITION

- IT security industry leadership – Eugene, CERTs, Interpol, GReAT
- Unparalleled insight into local and global threats
- Broad expertise in all types of IT security threats – not just threats to financial transactions
- Effective protection – across all types of users
- Protection that can be tailored to individual needs

LET'S TALK?

Ferenc Vaspöri
fvaspori@newco.hu

newco
ICT SECURITY SERVICES

KASPERSKY lab