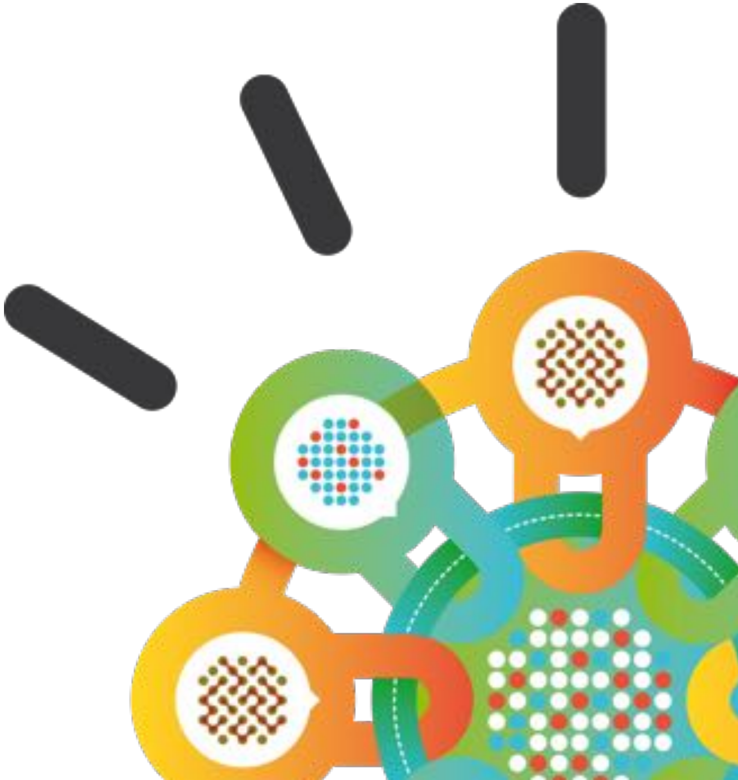
Security Intelligence.
Think Integrated.

IBM Security Trusteer Overview

George Tubin

October 2014



About IBM Trusteer?

- 450+ leading global organizations put their TRUST in us
- Intelligence gathered from more than 270 million endpoints

Prevent "Root Cause" of Fraud

Improve Your Customer Experience

Reduce Operational Impact

Utilize Real-time Intelligence Service

7/10 Top U.S. Banks

9/10 Top U.K. Banks

4/5 Top Canadian Banks

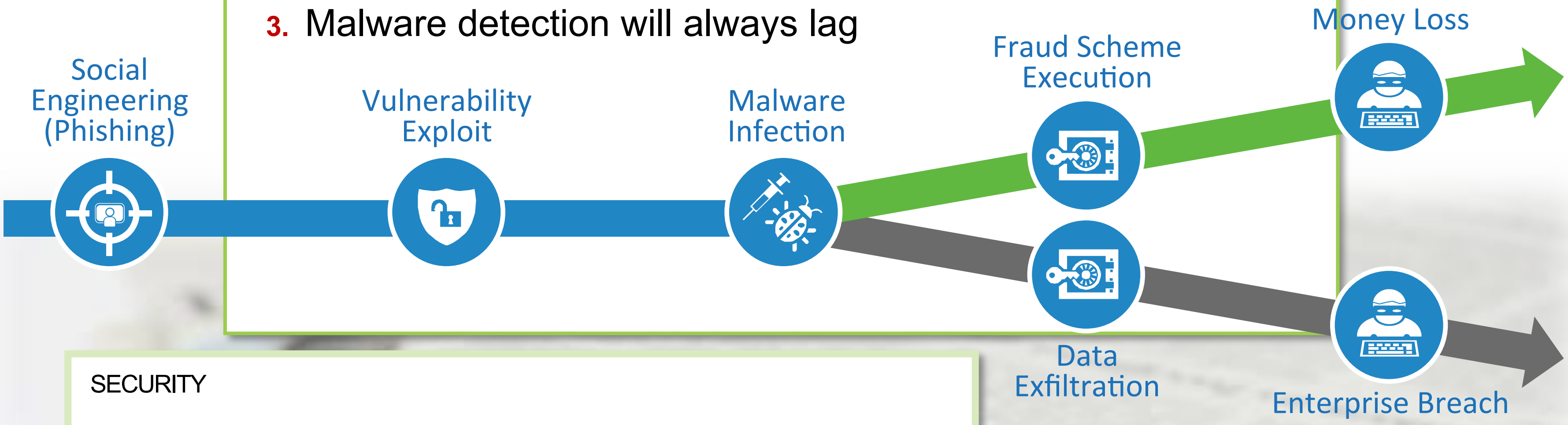
2/4 Top Japanese Banks

Major European Banks

Drivers for fraud prevention

Three Never-ending Battles

1. Humans will always make mistakes
2. System and application vulnerabilities continue to emerge
3. Malware detection will always lag



SECURITY

Gameover ZeuS adds nasty trick

Crypto t

By Richard Chi

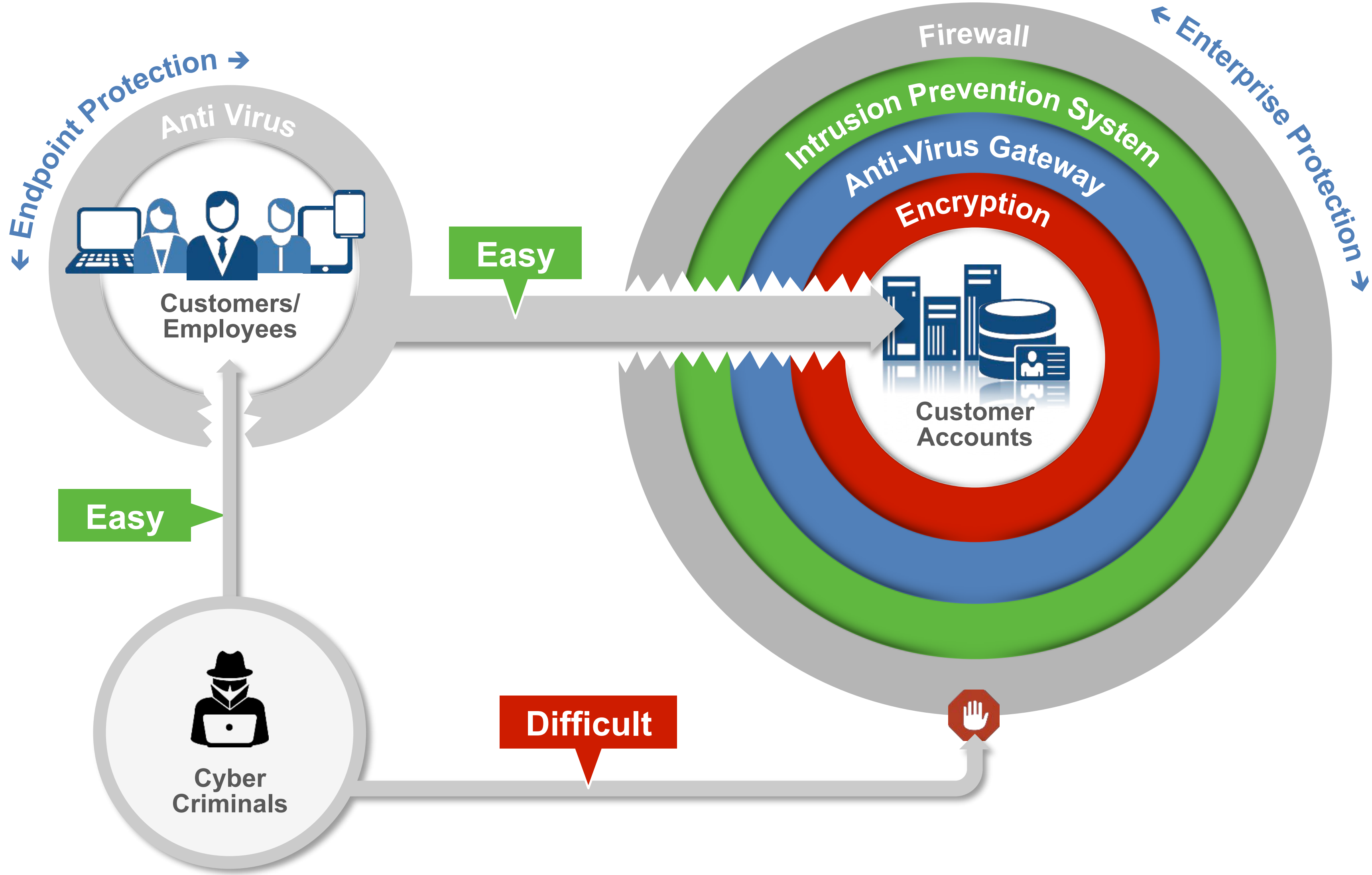
Cybercrime Losses Top $400 Billion Worldwide, Study Claims

By Jeremy Kirk
Mon, June 09, 2014

Cybercrime worries and costs
on the rise

June 10, 2014, 3:00 pm MDT

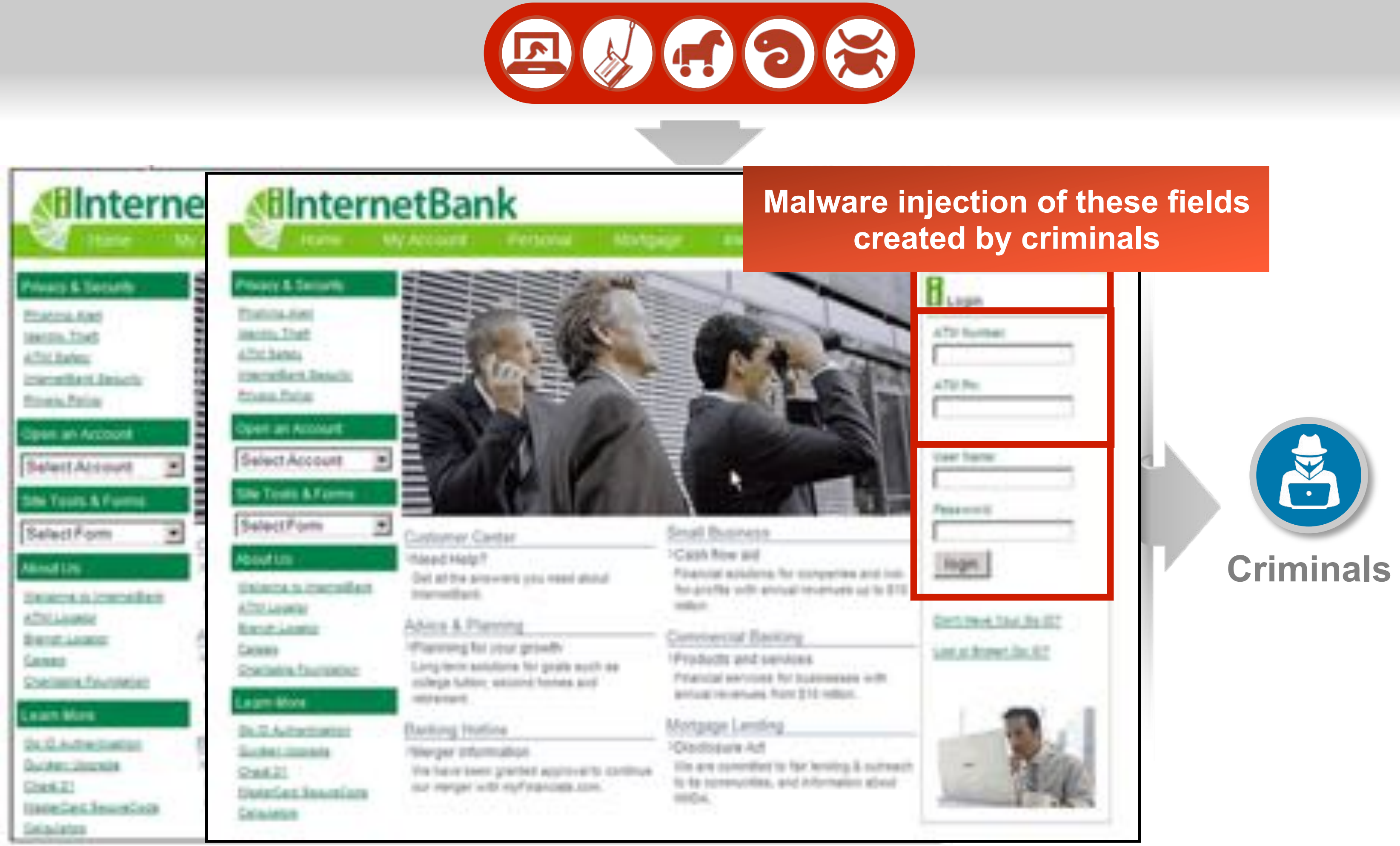
Criminals attack the weak link



Financial Fraud

Fraud attack methods evolve quickly

Man-in-the Browser Malware

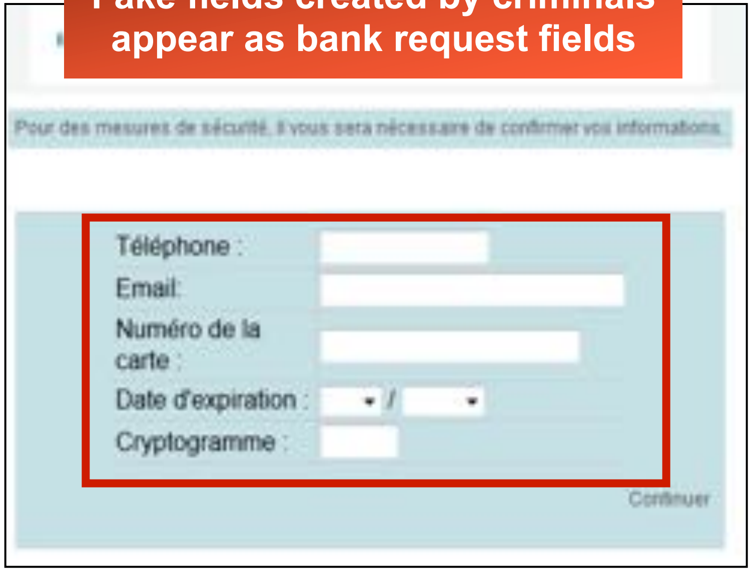


Malware injection of these fields created by criminals

Criminals

Fraud attack methods evolve quickly

Man-in-the Browser Malware

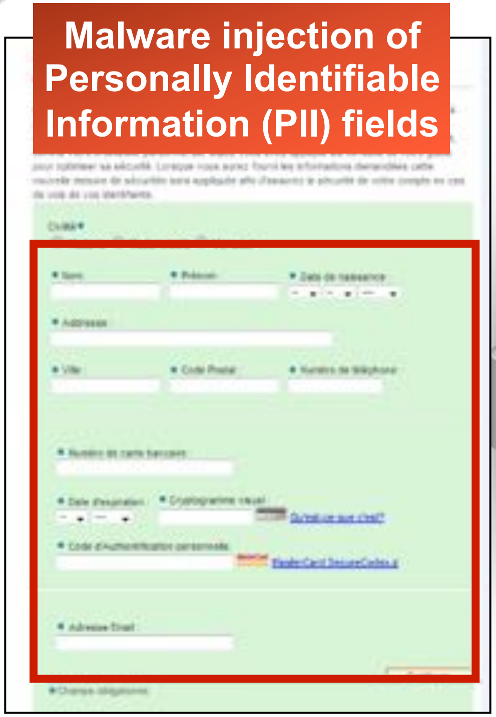


Fake fields created by criminals appear as bank request fields

Pour des mesures de sécurité, il vous sera nécessaire de confirmer vos informations.

Téléphone :	
Email:	
Numéro de la carte :	
Date d'expiration :	▾ / ▾
Cryptogramme :	

Zeus BabyBerta



Malware injection of Personally Identifiable Information (PII) fields

Civilité *

* Nom
* Prénom
* Date de naissance
* Addresse
* Ville
* Code Postal
* Numéro de téléphone
* Numéro de carte bancaire
* Date d'expiration
* Cryptogramme visuel

* Code d'Authentification personnelle

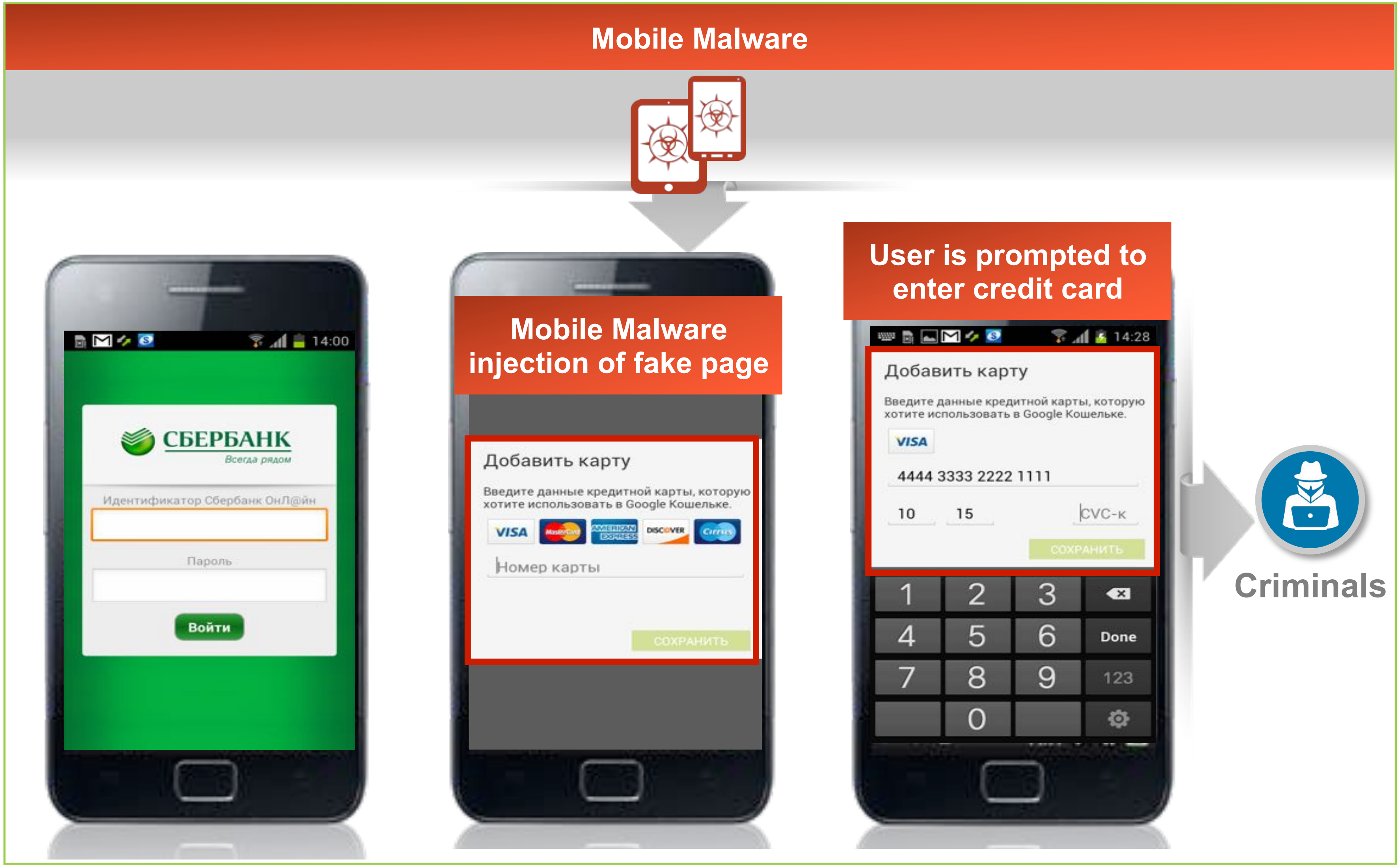
* Adresse Email

*Champs obligatoires

Citadel

Criminals

Fraud attack methods evolve quickly



Mobile Malware

Mobile Malware injection of fake page

User is prompted to enter credit card

Criminals

14:00

СБЕРБАНК

Всегда рядом

Идентификатор Сбербанк ОнЛ@йн

Пароль

Войти

Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

Номер карты

СОХРАНИТЬ

14:28

Добавить карту

Введите данные кредитной карты, которую хотите использовать в Google Кошельке.

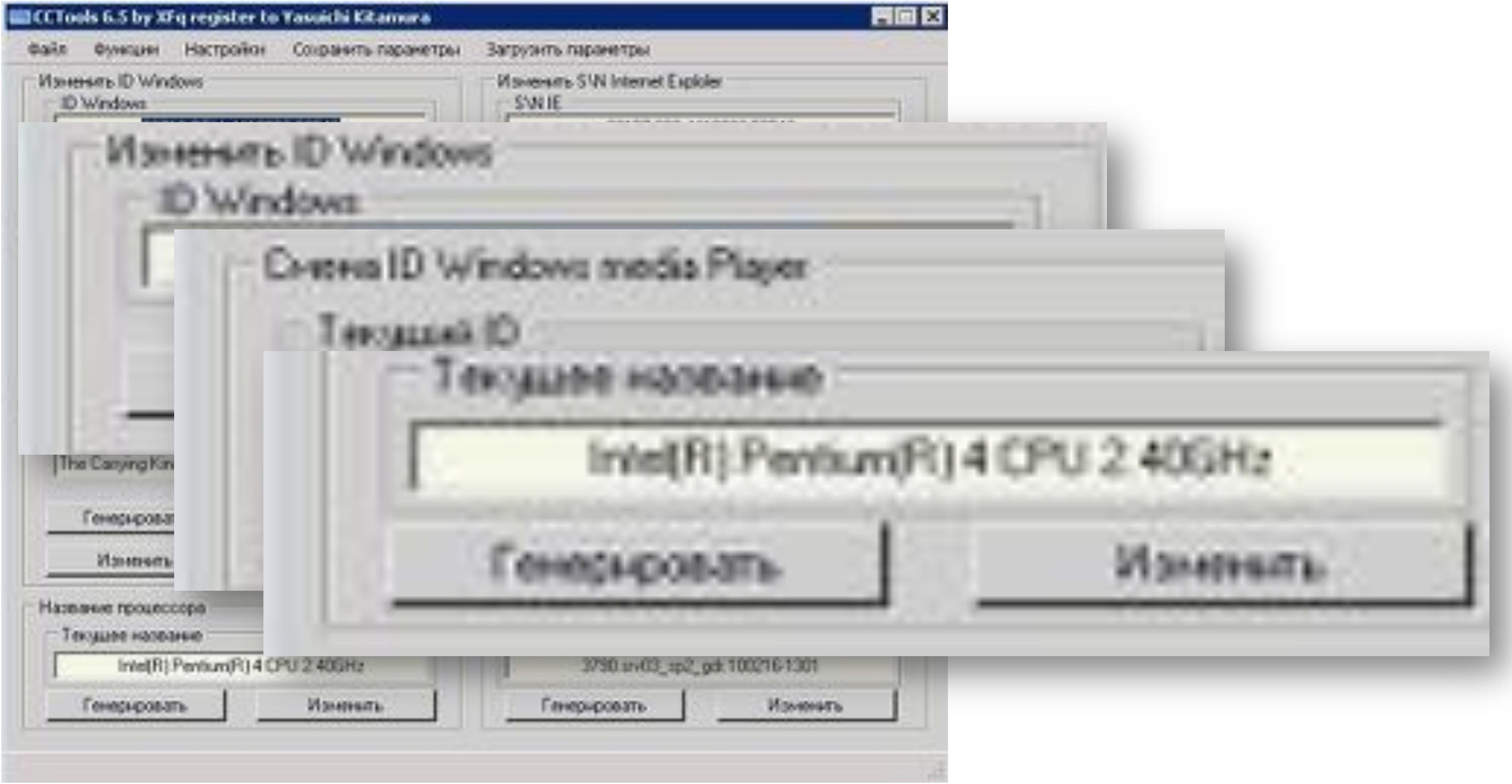
VISA

4444 3333 2222 1111

10 15 CVC-к

СОХРАНИТЬ

Bypassing fraud defenses – Device ID



CCTools 6.5 by XFq register to Yasuichi Kitamura

Изменить ID Windows

ID Windows

Изменить S\N Internet Explorer

S\N IE

Смена ID Windows media Player

Текущий ID

The Carrying Kin

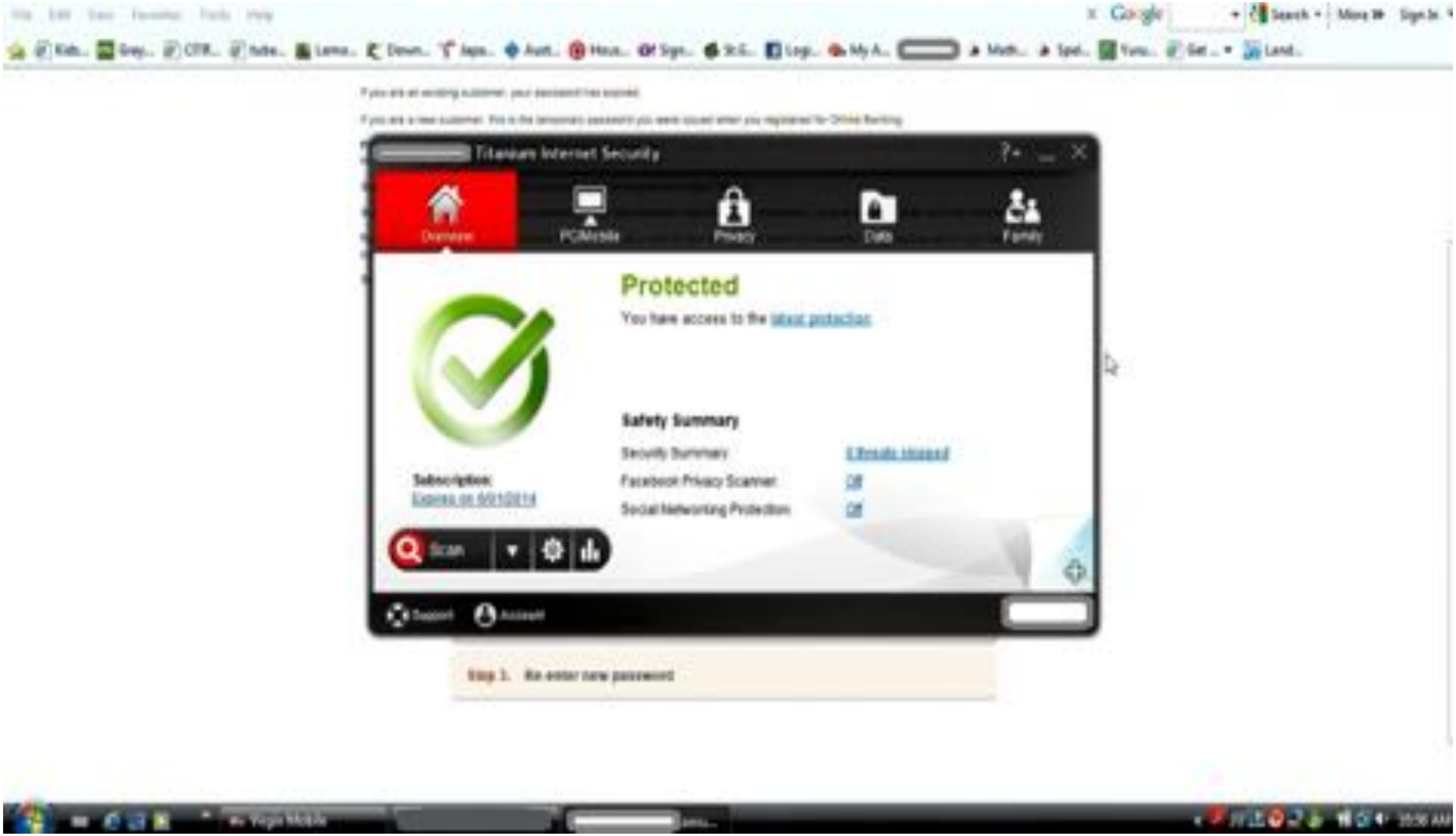
Название процессора

Текущее название

Intel(R) Pentium(R) 4 CPU 2.40GHz

3790.srv03_sp2_gdr.100216-1301

Bypassing bank defenses - Behavior Analytics



If you are an existing customer, your password has expired.

If you are a new customer, this is the temporary password you were issued when you registered for Online Banking.

Protected

You have access to the latest protection

Safety Summary

Security Summary: 0 threats stopped

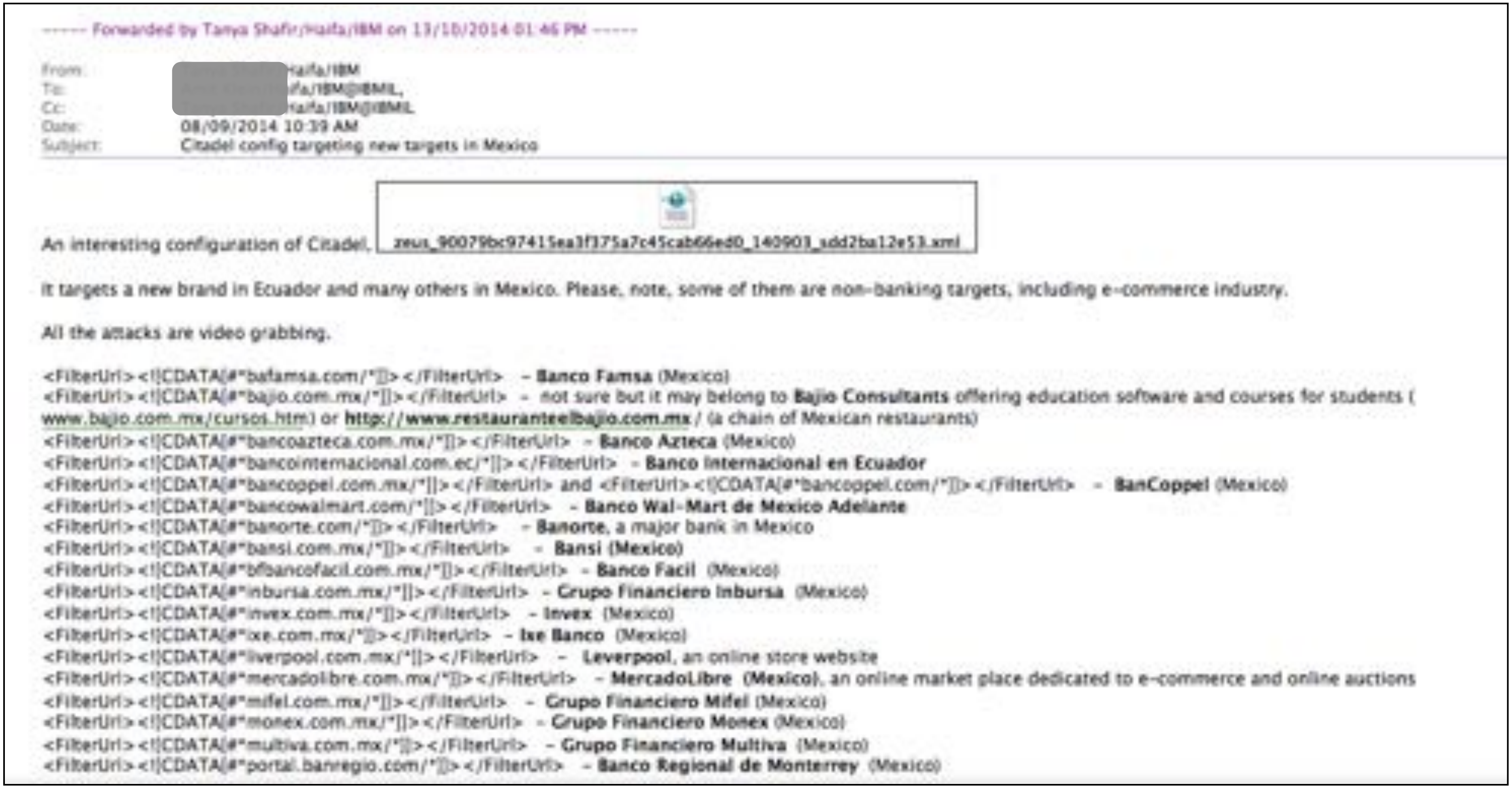
Facebook Privacy Scanner: Off

Social Networking Protection: Off

Subscription:
Expires on 6/01/2014

Step 1. Re-enter new password

Be aware of latest malware configurations



------ Forwarded by Tanya Shafir/Haifa/IBM on 13/10/2014 01:46 PM ------

From: [redacted]Haifa/IBM
To: fa/IBM@IBMIL,
Cc: Haifa/IBM@IBMIL
Date: 08/09/2014 10:39 AM
Subject: Citadel config targeting new targets in Mexico

An interesting configuration of Citadel. zeus_90079bc97415ea3f375a7c45cab66ed0_140903_sdd2ba12e53.xml

It targets a new brand in Ecuador and many others in Mexico. Please, note, some of them are non-banking targets, including e-commerce industry.

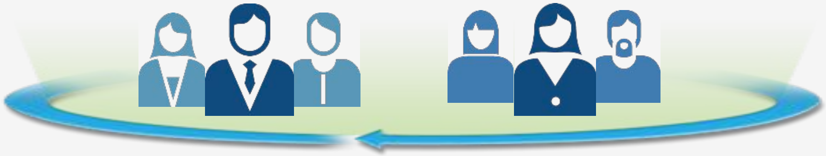
All the attacks are video grabbing.

<FilterUrl><![CDATA[#*bafamsa.com/*]]></FilterUrl> - **Banco Famsa** (Mexico)
<FilterUrl><![CDATA[#*bajio.com.mx/*]]></FilterUrl> - not sure but it may belong to **Bajio Consultants** offering education software and courses for students (www.bajio.com.mx/cursos.htm) or **http://www.restauranteelbajio.com.mx**/ (a chain of Mexican restaurants)
<FilterUrl><![CDATA[#*bancoazteca.com.mx/*]]></FilterUrl> - **Banco Azteca** (Mexico)
<FilterUrl><![CDATA[#*bancointernacional.com.ec/*]]></FilterUrl> - **Banco Internacional en Ecuador**
<FilterUrl><![CDATA[#*bancoppel.com.mx/*]]></FilterUrl> and <FilterUrl><![CDATA[#*bancoppel.com/*]]></FilterUrl> - **BanCoppel** (Mexico)
<FilterUrl><![CDATA[#*bancowalmart.com/*]]></FilterUrl> - **Banco Wal-Mart de Mexico Adelante**
<FilterUrl><![CDATA[#*banorte.com/*]]></FilterUrl> - **Banorte**, a major bank in Mexico
<FilterUrl><![CDATA[#*bansi.com.mx/*]]></FilterUrl> - **Bansi (Mexico)**
<FilterUrl><![CDATA[#*bfbancofacil.com.mx/*]]></FilterUrl> - **Banco Facil** (Mexico)
<FilterUrl><![CDATA[#*inbursa.com.mx/*]]></FilterUrl> - **Grupo Financiero Inbursa** (Mexico)
<FilterUrl><![CDATA[#*invex.com.mx/*]]></FilterUrl> - **Invex** (Mexico)
<FilterUrl><![CDATA[#*ixe.com.mx/*]]></FilterUrl> - **Ixe Banco** (Mexico)
<FilterUrl><![CDATA[#*liverpool.com.mx/*]]></FilterUrl> - **Leverpool**, an online store website
<FilterUrl><![CDATA[#*mercadolibre.com.mx/*]]></FilterUrl> - **MercadoLibre (Mexico)**, an online market place dedicated to e-commerce and online auctions
<FilterUrl><![CDATA[#*mifel.com.mx/*]]></FilterUrl> - **Grupo Financiero Mifel** (Mexico)
<FilterUrl><![CDATA[#*monex.com.mx/*]]></FilterUrl> - **Grupo Financiero Monex** (Mexico)
<FilterUrl><![CDATA[#*multiva.com.mx/*]]></FilterUrl> - **Grupo Financiero Multiva** (Mexico)
<FilterUrl><![CDATA[#*portal.banregio.com/*]]></FilterUrl> - **Banco Regional de Monterrey** (Mexico)

Users demand convenience AND security

Address root cause of fraud without impacting customer experience

Focus on Preventing the Root Cause of Fraud

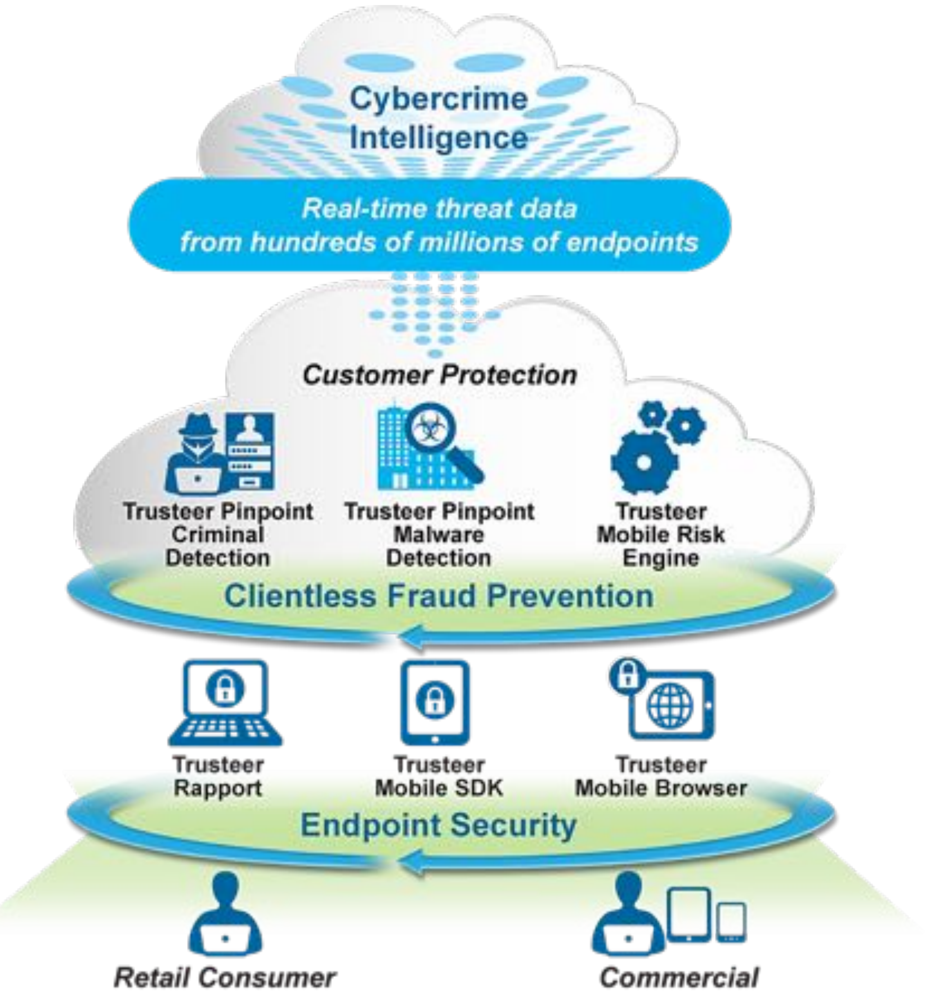


Convenience + Security

- ▪Prevent malware from taking hold
- ▪Stop fraudulent transactions **BEFORE** they are created
- ▪Reduce authentication challenges
- ▪Eliminate false positives that create unnecessary customer actions

Cybercrime prevention architecture

Comprehensive platform for fraud detection and prevention


Cybercrime Intelligence
Real-time threat data from hundreds of millions of endpoints
Customer Protection
Trusteer Pinpoint Criminal Detection
Trusteer Pinpoint Malware Detection
Trusteer Mobile Risk Engine
Clientless Fraud Prevention
Trusteer Rapport
Trusteer Mobile SDK
Trusteer Mobile Browser
Endpoint Security
Retail Consumer
Commercial

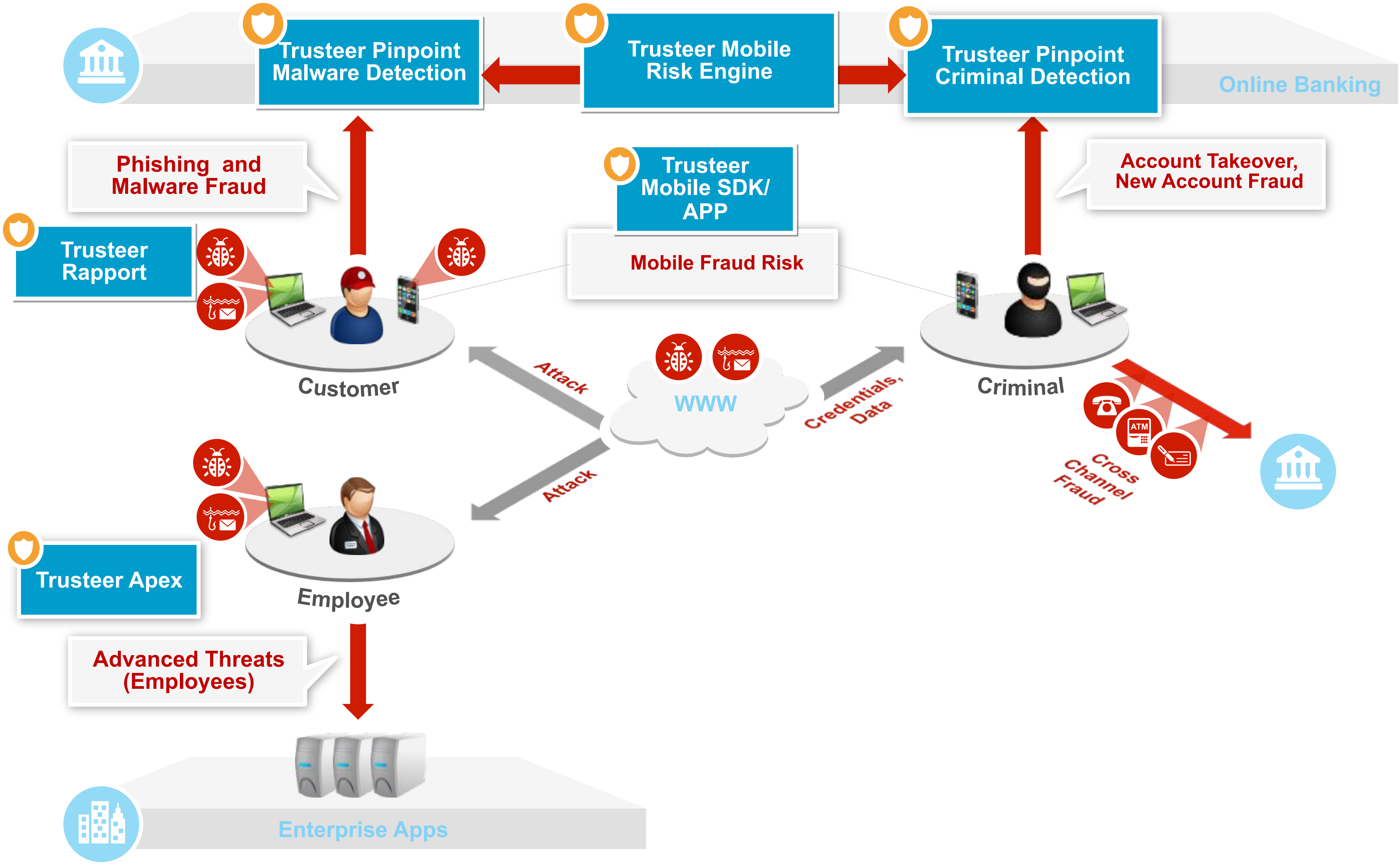
Clientless Fraud Prevention

- **Trusteer Pinpoint Criminal Detection**
  Evidence-based detection of account takeover attempts
- **Trusteer Pinpoint Malware Detection**
  Real-time malware detection
- **Trusteer Mobile Risk Engine**
  Detects mobile-fraud risks from compromised end user and criminal-owned devices

Endpoint Security

- **Trusteer Rapport**
  Prevents and removes financial malware and detects phishing attacks
- **Trusteer Mobile SDK**
  Embedded security library for native apps that detects compromised / vulnerable devices
- **Trusteer Mobile Browser**
  Risk-based analysis of mobile web access

Trusteer Cyber Fraud Prevention


Trusteer Pinpoint Malware Detection
Trusteer Mobile Risk Engine
Trusteer Pinpoint Criminal Detection
Online Banking
Phishing and Malware Fraud
Trusteer Mobile SDK/ APP
Mobile Fraud Risk
Account Takeover, New Account Fraud
Trusteer Rapport
Customer
Attack
WWW
Credentials, Data
Criminal
ATM
Cross Channel Fraud
Attack
Employee
Trusteer Apex
Advanced Threats (Employees)
Enterprise Apps

Trusteer’ s unique value

Comprehensive solution built upon real-time intelligence and adaptable protection

Prevent “Root Cause” of Fraud

- Remove infections and block attacks
- Detect active threats in real-time
- Identify account takeovers and fraudster log-ins

Reduce Operational Impact

- Reduce false positives typical of other fraud analytical solutions
- Integrate real-time data into existing systems and workflows
- Leverage Trusteer's 24x7 turnkey SaaS service

Advanced
Web Fraud
Prevention

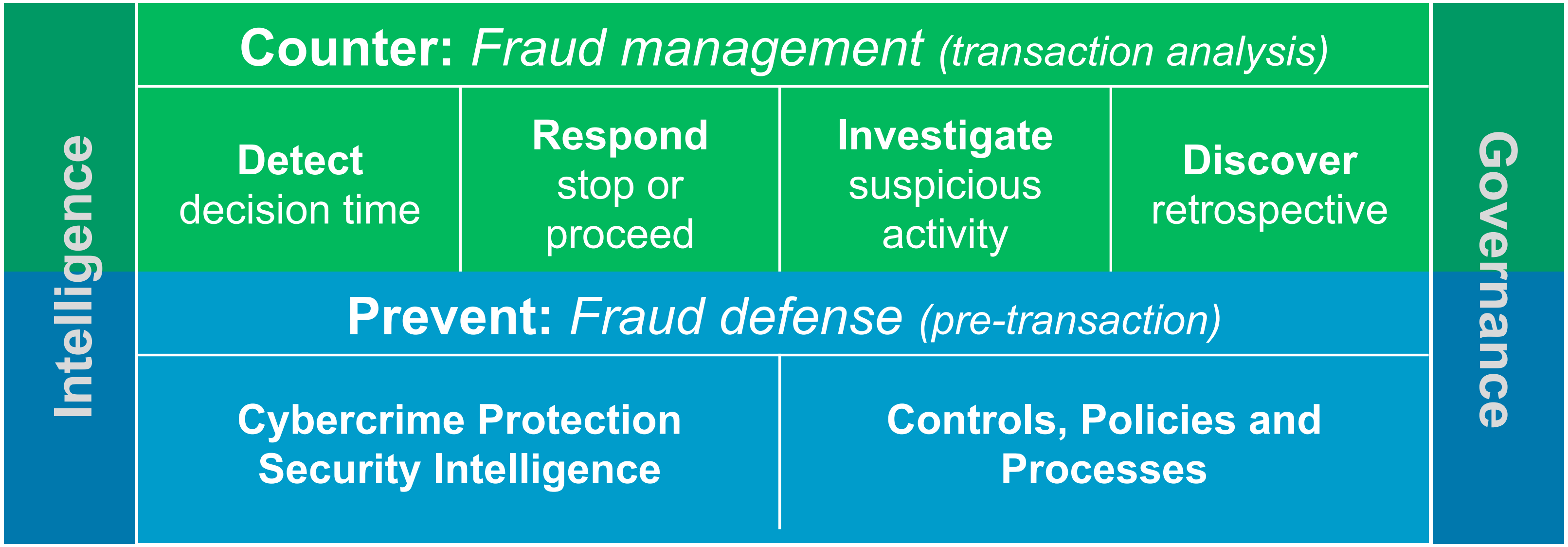
Improve Your Customer Experience

- Reduce unnecessary authentication challenges, transaction verifications and other interruptions
- Offer a more secure transaction and proactive remediation for compromised accounts

Utilize Real-time Intelligence Service

- Gather intelligence from 270M+ endpoints
- Adapt protection automatically without customer interaction
- Research and investigate industry and customer-specific threats

IBM Smarter Counter Fraud Framework



Intelligence

Counter: *Fraud management (transaction analysis)*

Detect decision time

Respond stop or proceed

Investigate suspicious activity

Discover retrospective

Prevent: *Fraud defense (pre-transaction)*

Cybercrime Protection Security Intelligence

Controls, Policies and Processes

Governance

Recognized fraud leader

Web Fraud Detection

Trusteer ranked as a leader in the Gartner 2013 Magic Quadrant for Web Fraud Detection

second year in a row!

> *"Customers report solid success using Trusteer Rapport and Trusteer Pinpoint Malware Detection"*
>
> *"Products have been used to successfully reduce malware-based fraud losses"*
>
> *"Products are very easy to install"*

Gartner
2013 Magic Quadrant Report

IBM Trusteer delivers quantifiable results

30%	Reduction in *Cross Channel Fraud* in 6 months	**Top 5 U.S. Bank**
50%	Reduction in *Risk Engine False Positives*	**Top 5 U.K. Bank**
80%	Reduction in *Phone Channel Fraud* in 2 weeks	**Top 10 U.K. Bank**

Client example: One of the world’s largest banks

Protecting against online and cross-channel fraud

Cross-channel Fraud Prevention

Reduced phishing attacks by

90%

2,000 a week to less than 10 a week

Reduced phone fraud to near

$0

Business challenge

The financial organization was experiencing high volumes of phishing attacks and phone fraud. Much of the information that was being stolen via phishing attacks was being used to perpetrate phone fraud.

IBM Security Solution *(Trusteer Rapport and Trusteer Pinpoint Criminal Detection)*

Reduced operational impact to organization, allowed resources to focus on legitimate business functions

- Reduced the number of phishing attacks the bank sees by 90%
- Reduced phone fraud to almost zero
- Free up call center resources to focus on legitimate calls; fraudulent calls made up 20% of their call center volume, so savings in time spent servicing and investigating fraudulent calls / attacks

Client example: Large Retail Bank

Strengthening security for mobile money transfers and banking applications

Mobile Fraud Protection

$1 million

in fraud stopped in the **first week**

$60 million

in fraud stopped in the **first year**

Business challenge

A retail bank in the EU sought a secure means to allow its users to perform the same functions they performed online with their mobile devices.

IBM Security Solution *(Trusteer Mobile SDK)*

Helped protect the organizations' existing mobile banking application by adding device risk analysis and providing a persistent mobile device ID

- Detects high risk access from compromised or vulnerable devices
- Generates a persistent mobile device ID for unique device identification

Client example: Large international bank in the U.K.

Reduce risk engine false positives with malware detection

Fraud and Malware Detection

90% reduction in false positives

Business challenge

The financial institution was wasting valuable resources investigating alerts generated by their risk engine that turned out to be nothing (false positives).

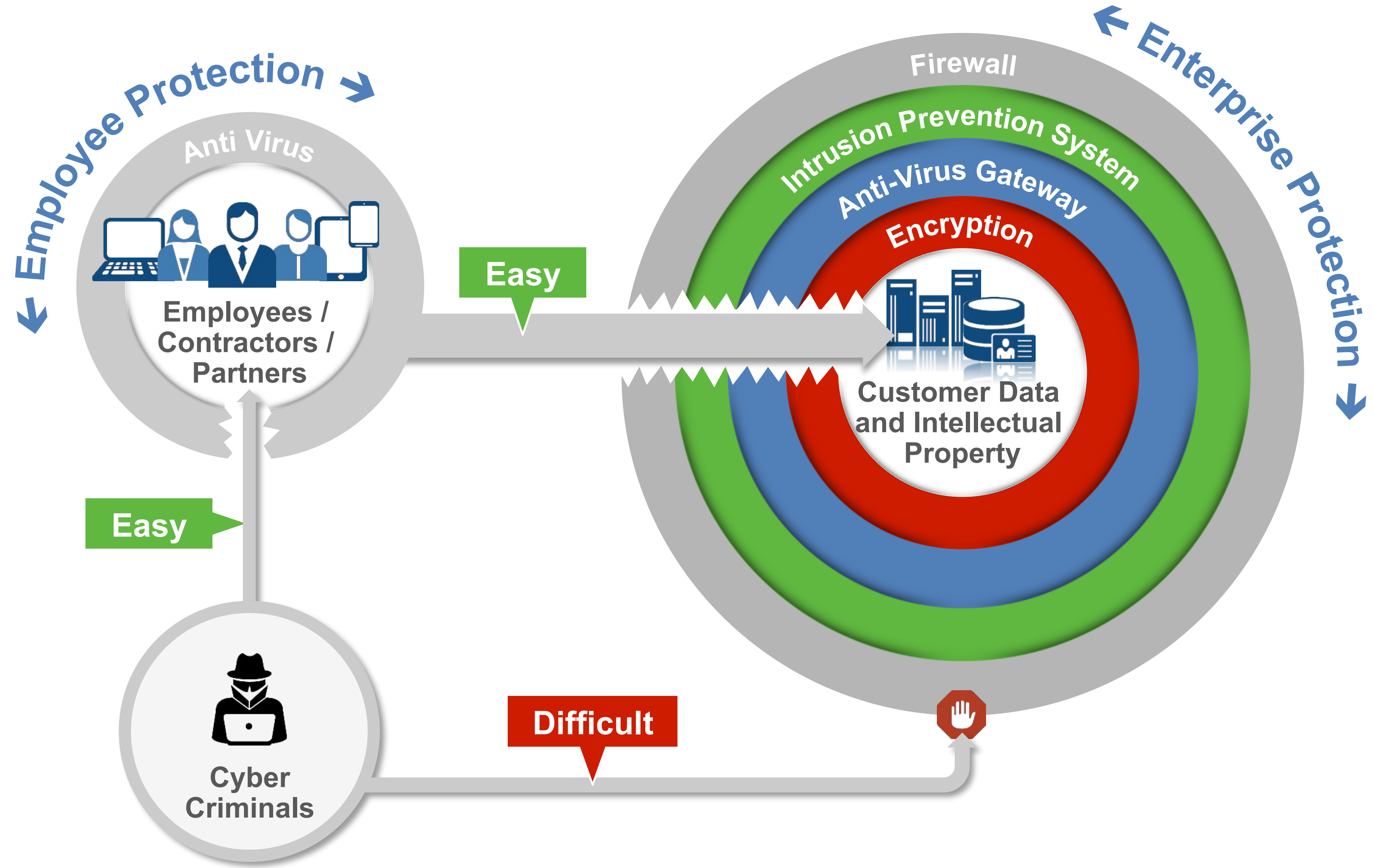
IBM Security Solution *(Trusteer Pinpoint Malware Detection)*

Helped the bank with malware detection and risk engine integration

- Reduced the false positive rate of their risk engine by 90%
- Helped focus resources on protecting the truly high risk transactions and not chasing false positives

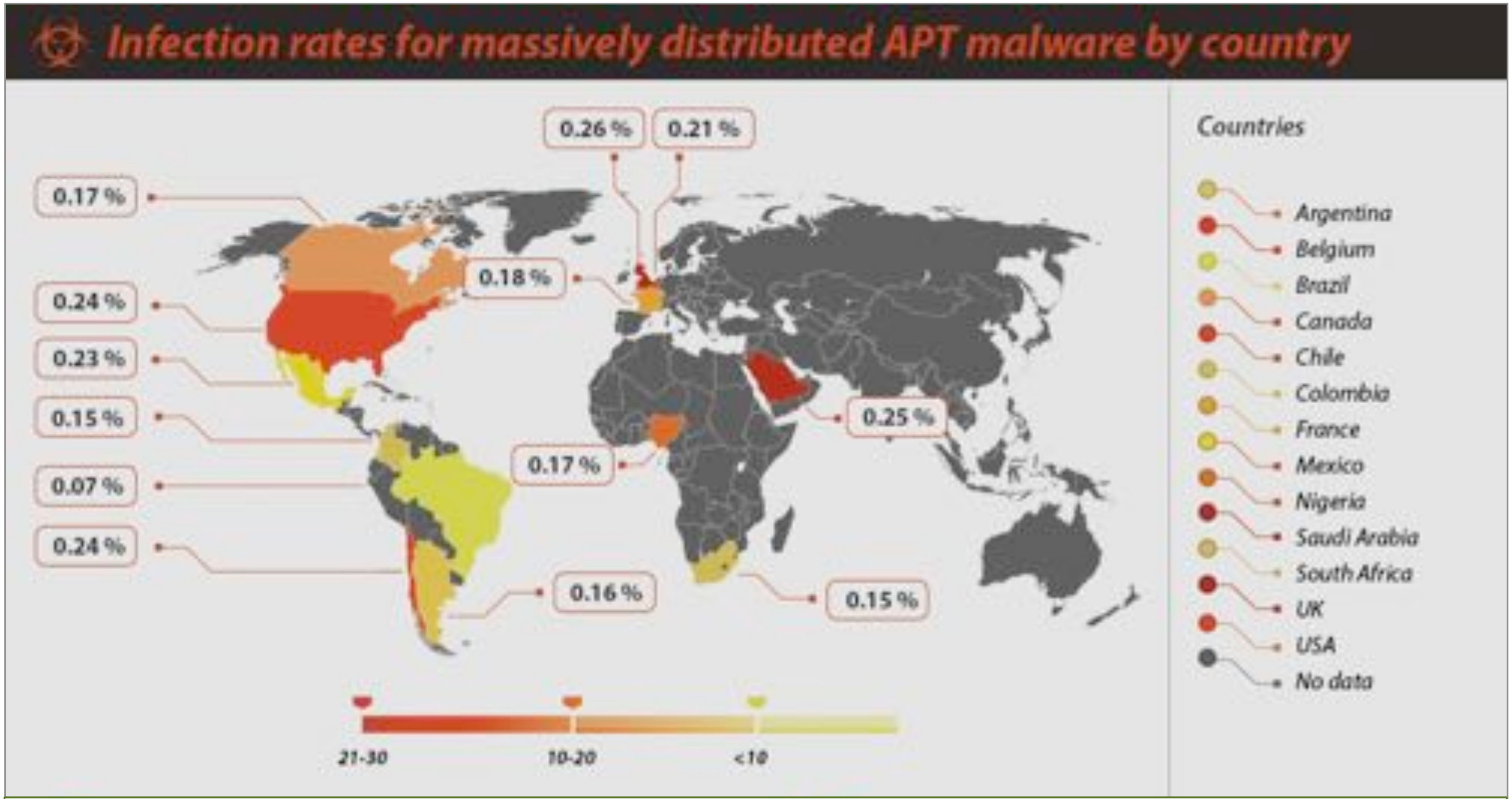
Enterprise Fraud

Criminals attack the weak link



Massively Distributed APTs

Large-scale infections create large surface area for new APT style attacks

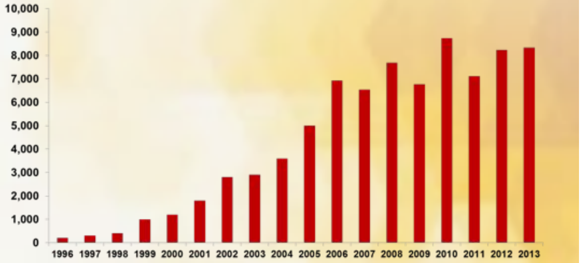


New APT attack that can evade AV and standard controls
Attack attempts to set up remote control or steal corporate credentials

By All Accounts, Prevention is Getting Harder

Increasing Number of Vulnerabilities

Growth in Vulnerabilities 1996 - 2013



- Vulnerabilities increasing
- Overall attack surface is growing
- Patches cannot be instantly implemented or do not exist

Zero-day Attacks and Constantly Mutating Threats

Designer Malware

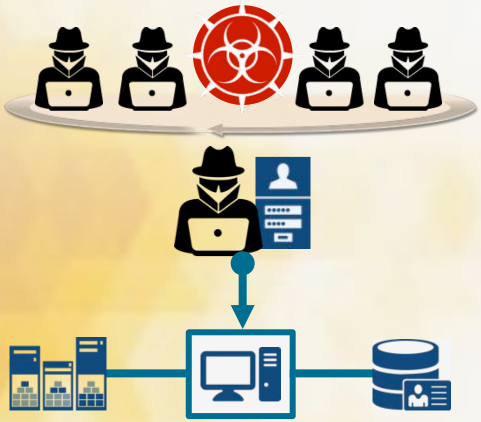
Spear Phishing

Persistence

Backdoors

- Attacks constantly mutating to evade signatures
- Increasing number of zero-day exploits

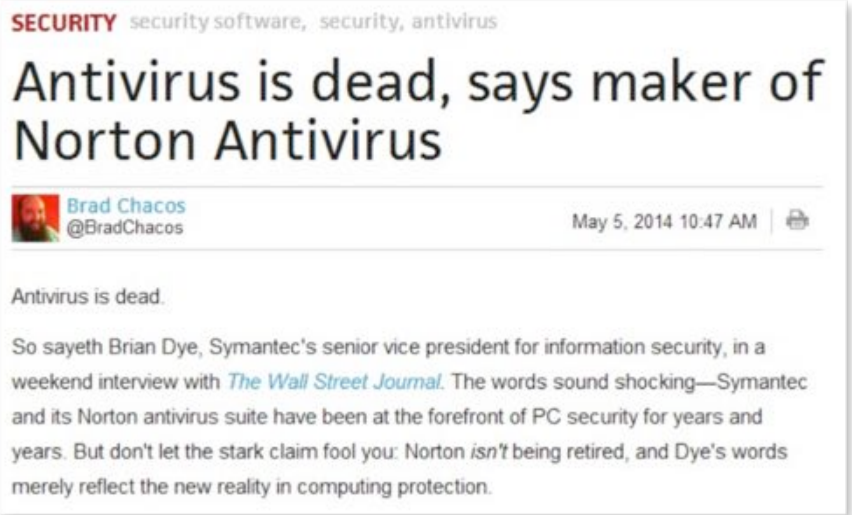
Multi-faceted Threats and APTs



- Well coordinated attacks by well coordinated teams
- Attackers exploiting users to gain access
- Traditional security tools unable to detect or assess the extent of the breach

Source: 2013 Cost of a Breach Report, Ponemon Institute

Traditional Tools are Failing to Stop Attacks and Advanced Malware



SECURITY security software, security, antivirus

Antivirus is dead, says maker of Norton Antivirus

Brad Chacos
@BradChacos

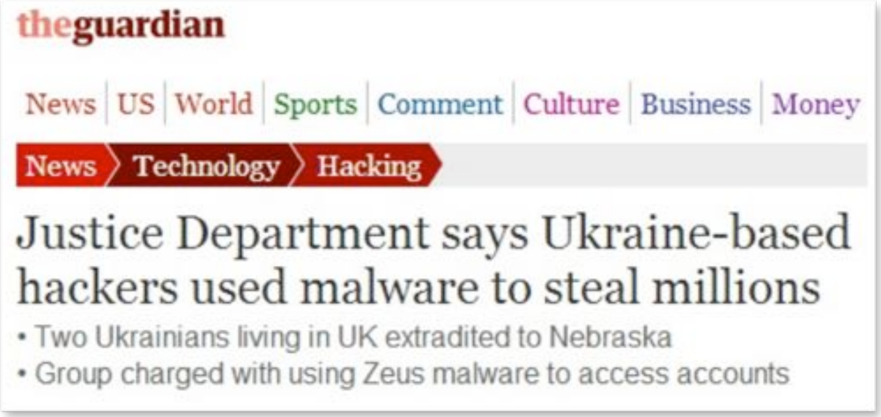
May 5, 2014 10:47 AM

Antivirus is dead.

So sayeth Brian Dye, Symantec's senior vice president for information security, in a weekend interview with *The Wall Street Journal*. The words sound shocking—Symantec and its Norton antivirus suite have been at the forefront of PC security for years and years. But don't let the stark claim fool you: Norton *isn't* being retired, and Dye's words merely reflect the new reality in computing protection.

Hackers steal data for 12 million customers at South Korean phone giant

By **Lina Yoon** and **Paul Armstrong,** CNN
March 6, 2014 -- Updated 1005 GMT (1805 HKT)



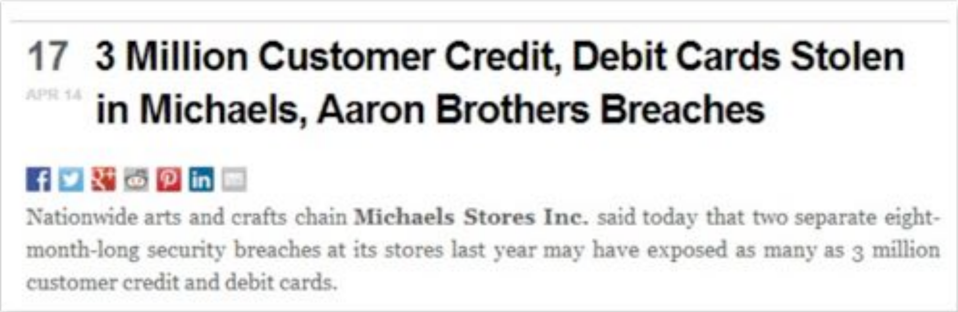
theguardian

News | US | World | Sports | Comment | Culture | Business | Money

News › Technology › Hacking

Justice Department says Ukraine-based hackers used malware to steal millions

- Two Ukrainians living in UK extradited to Nebraska
- Group charged with using Zeus malware to access accounts



17 APR 14

3 Million Customer Credit, Debit Cards Stolen in Michaels, Aaron Brothers Breaches

Nationwide arts and crafts chain **Michaels Stores Inc.** said today that two separate eight-month-long security breaches at its stores last year may have exposed as many as 3 million customer credit and debit cards.

Attackers are Exploiting Vulnerabilities to Deliver Advanced Malware

Latest X-Force Data shows key vulnerabilities as malware entry points

Exploitation of application vulnerabilities

from survey of 1 million Trusteer customers, December 2013

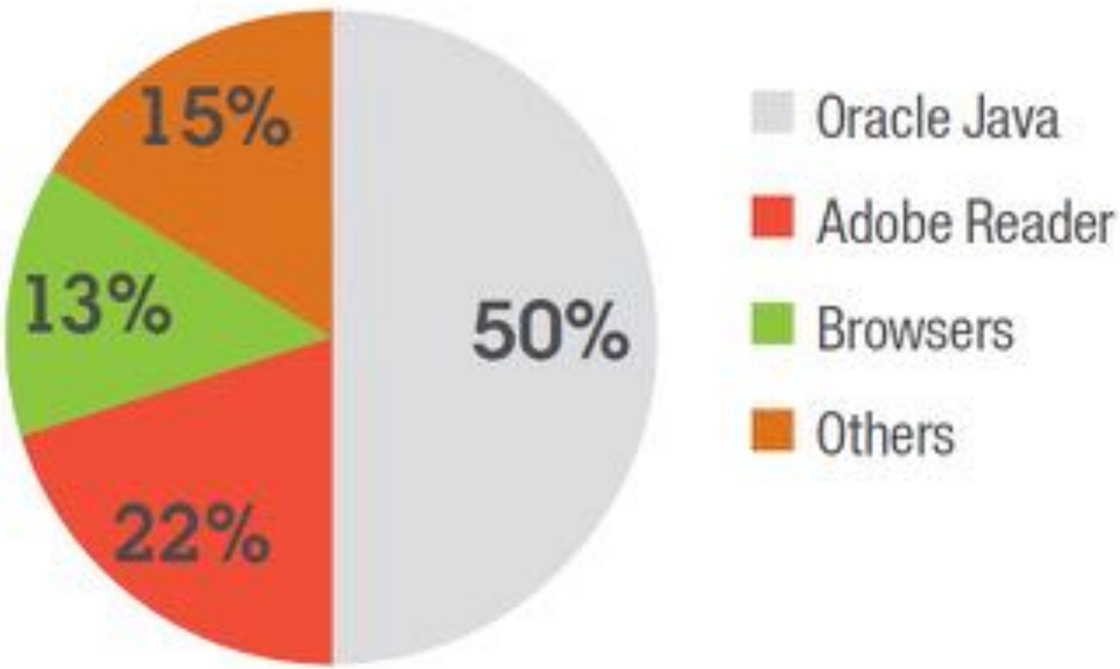
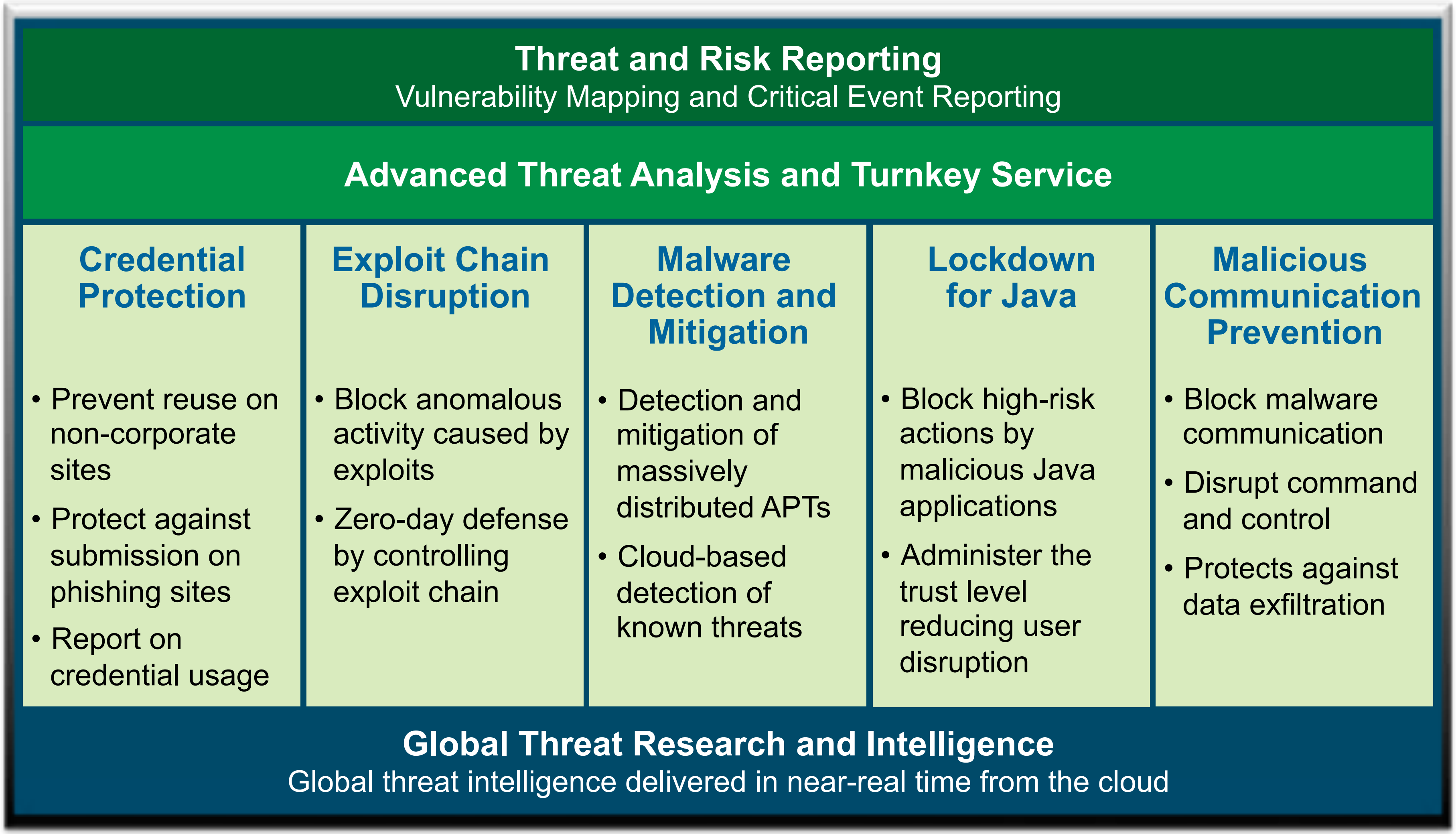


Figure 4. Exploitation of application vulnerabilities

Apex multi-layered defense architecture



Threat and Risk Reporting

Vulnerability Mapping and Critical Event Reporting

Advanced Threat Analysis and Turnkey Service

Credential Protection

- Prevent reuse on non-corporate sites
- Protect against submission on phishing sites
- Report on credential usage

Exploit Chain Disruption

- Block anomalous activity caused by exploits
- Zero-day defense by controlling exploit chain

Malware Detection and Mitigation

- Detection and mitigation of massively distributed APTs
- Cloud-based detection of known threats

Lockdown for Java

- Block high-risk actions by malicious Java applications
- Administer the trust level reducing user disruption

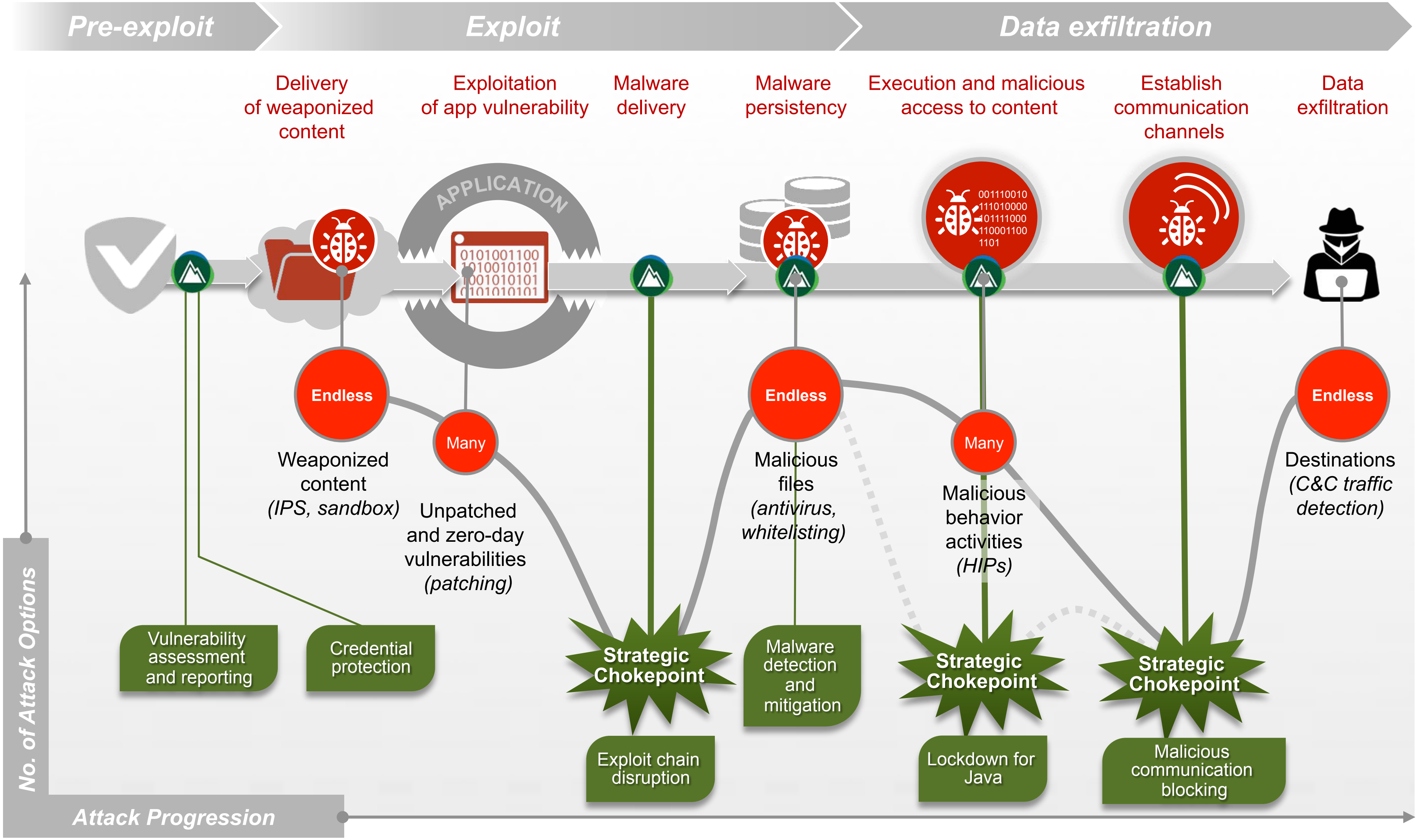
Malicious Communication Prevention

- Block malware communication
- Disrupt command and control
- Protects against data exfiltration

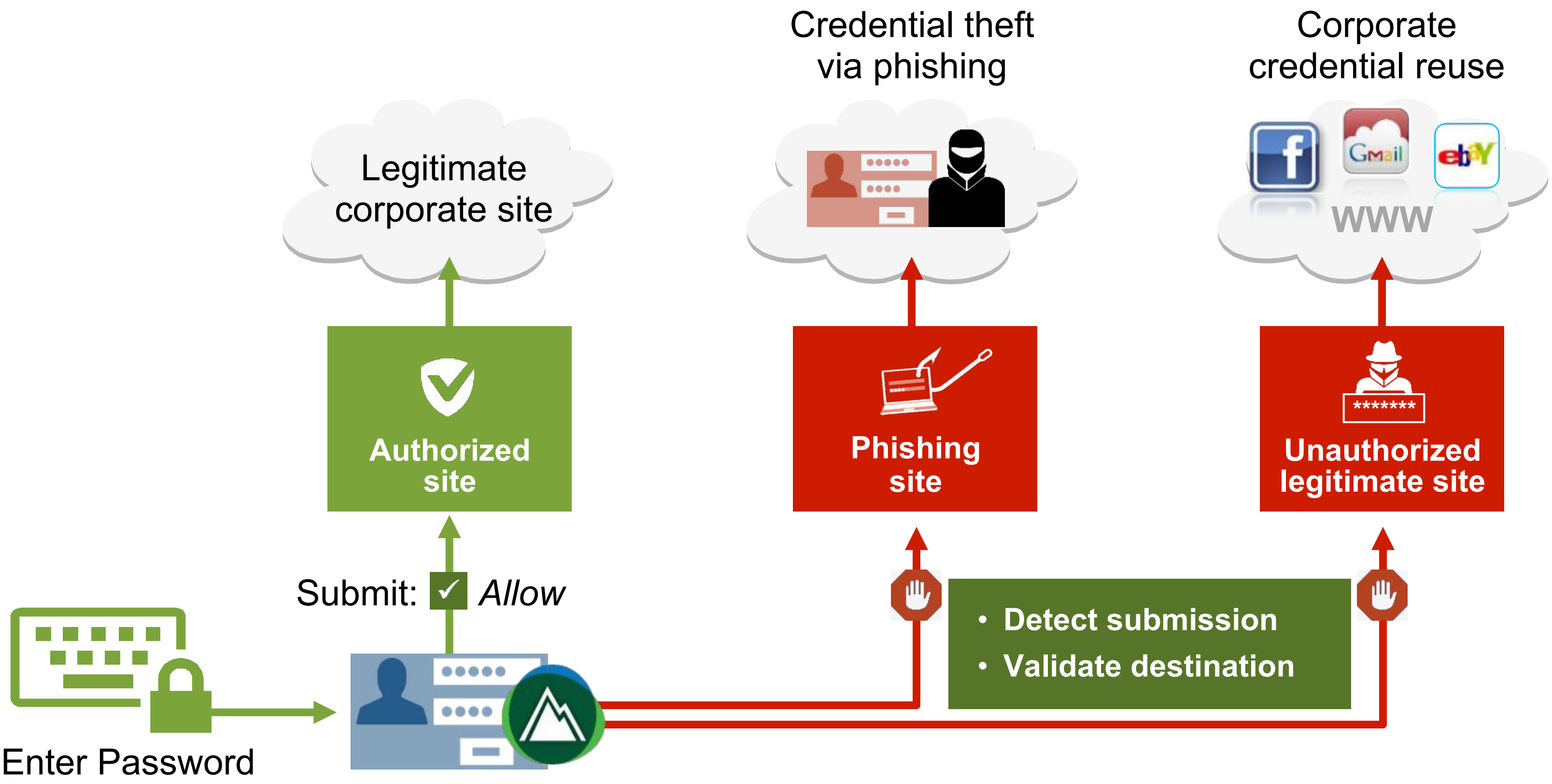
Global Threat Research and Intelligence

Global threat intelligence delivered in near-real time from the cloud

Controlling exploit-chain chokepoints


Pre-exploit
Exploit
Data exfiltration
Delivery of weaponized content
Exploitation of app vulnerability
Malware delivery
Malware persistency
Execution and malicious access to content
Establish communication channels
Data exfiltration
APPLICATION
0101001100
1010010101
1001010101
0101010101
001110010
111010000
101111000
110001100
1101
Endless
Weaponized content (IPS, sandbox)
Many
Unpatched and zero-day vulnerabilities (patching)
Endless
Malicious files (antivirus, whitelisting)
Many
Malicious behavior activities (HIPs)
Endless
Destinations (C&C traffic detection)
Vulnerability assessment and reporting
Credential protection
Strategic Chokepoint
Exploit chain disruption
Malware detection and mitigation
Strategic Chokepoint
Lockdown for Java
Strategic Chokepoint
Malicious communication blocking
No. of Attack Options
Attack Progression

Corporate Credentials Protection



Credential theft via phishing

Corporate credential reuse

Legitimate corporate site

Authorized site

Phishing site

Unauthorized legitimate site

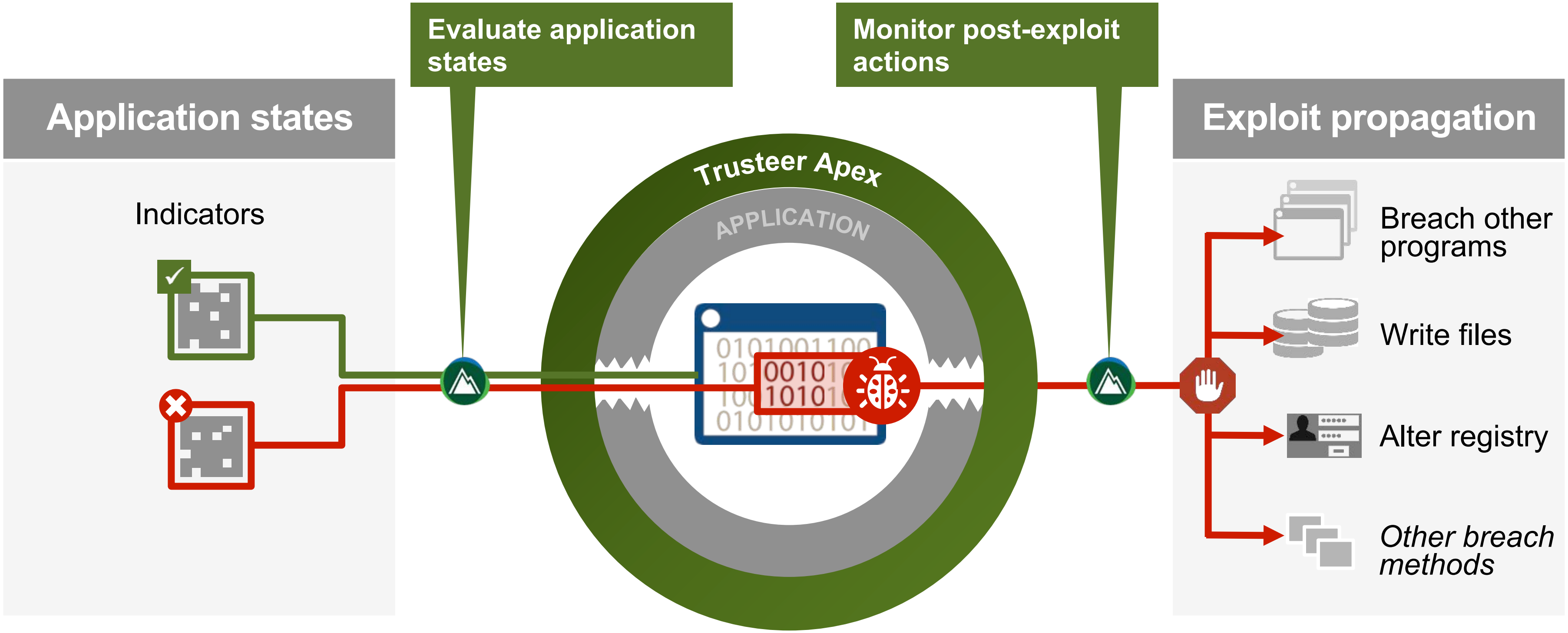
Submit: ✓ *Allow*

- Detect submission
- Validate destination

Enter Password

Exploit chain disruption

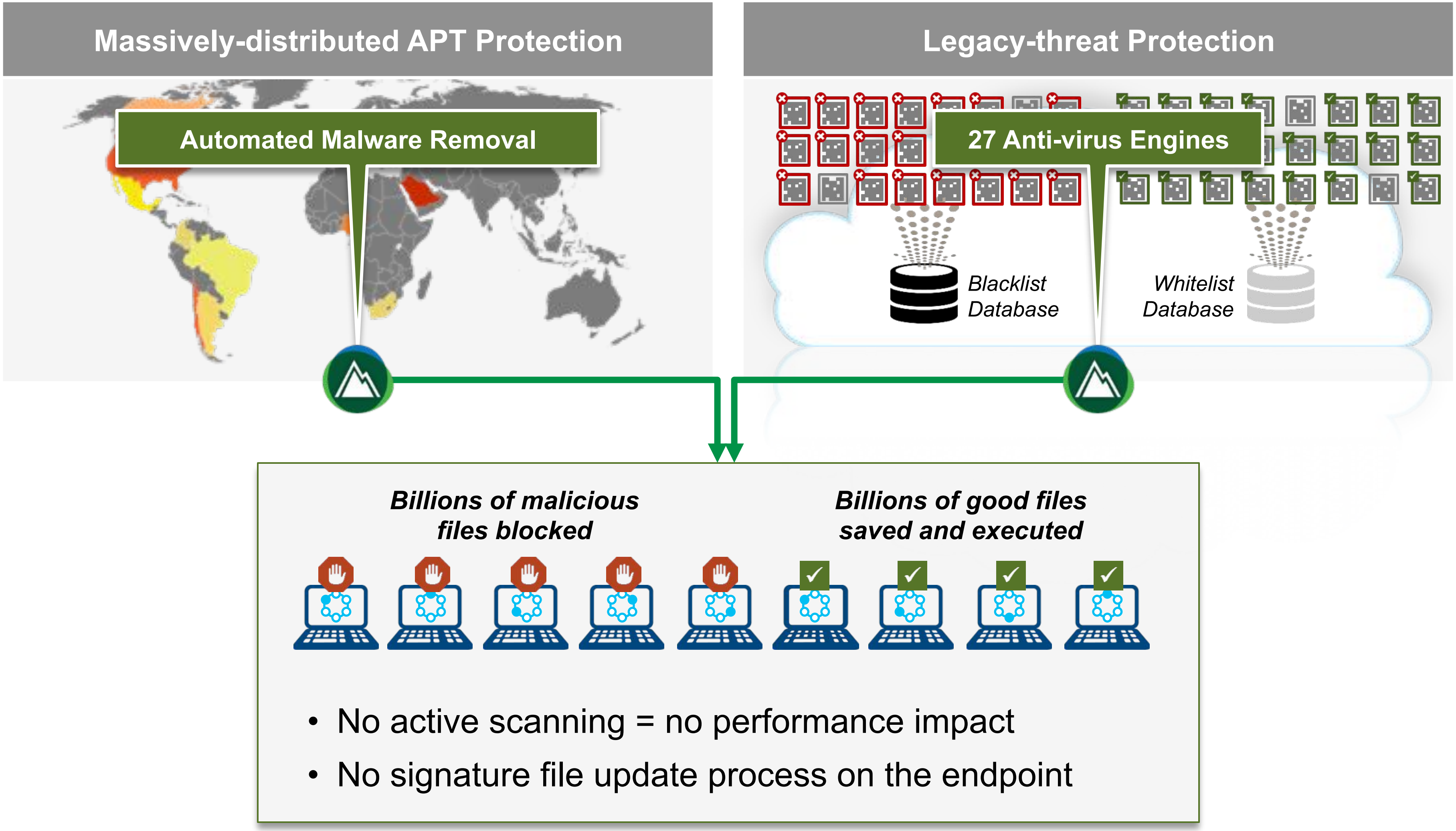
Disrupt zero day attacks without prior knowledge of the exploit or vulnerability



- Correlate application state with post-exploit actions
- Apply allow / block controls across the exploit chain

Malware Detection and Mitigation

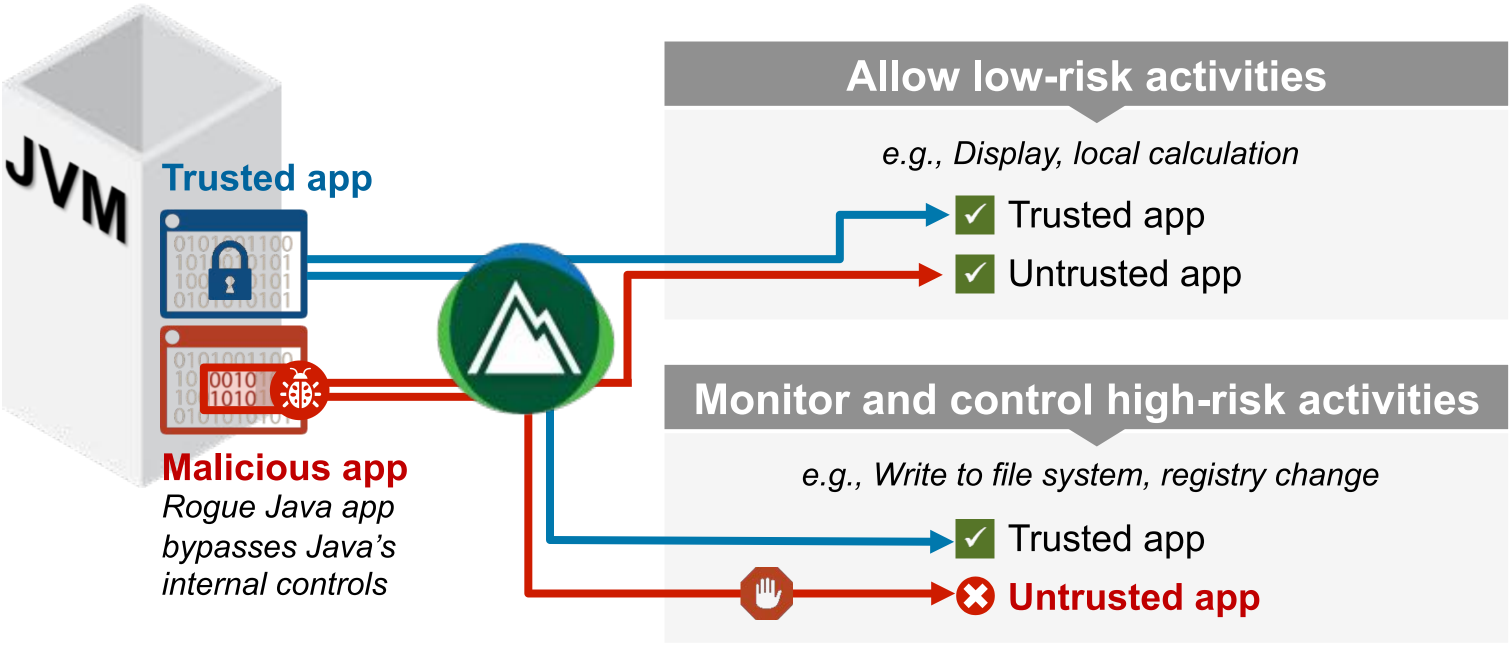
Transparent removal of malware infections


Massively-distributed APT Protection
Automated Malware Removal
Legacy-threat Protection
27 Anti-virus Engines
Blacklist Database
Whitelist Database
Billions of malicious files blocked
Billions of good files saved and executed

- No active scanning = no performance impact
- No signature file update process on the endpoint

Lockdown for Java

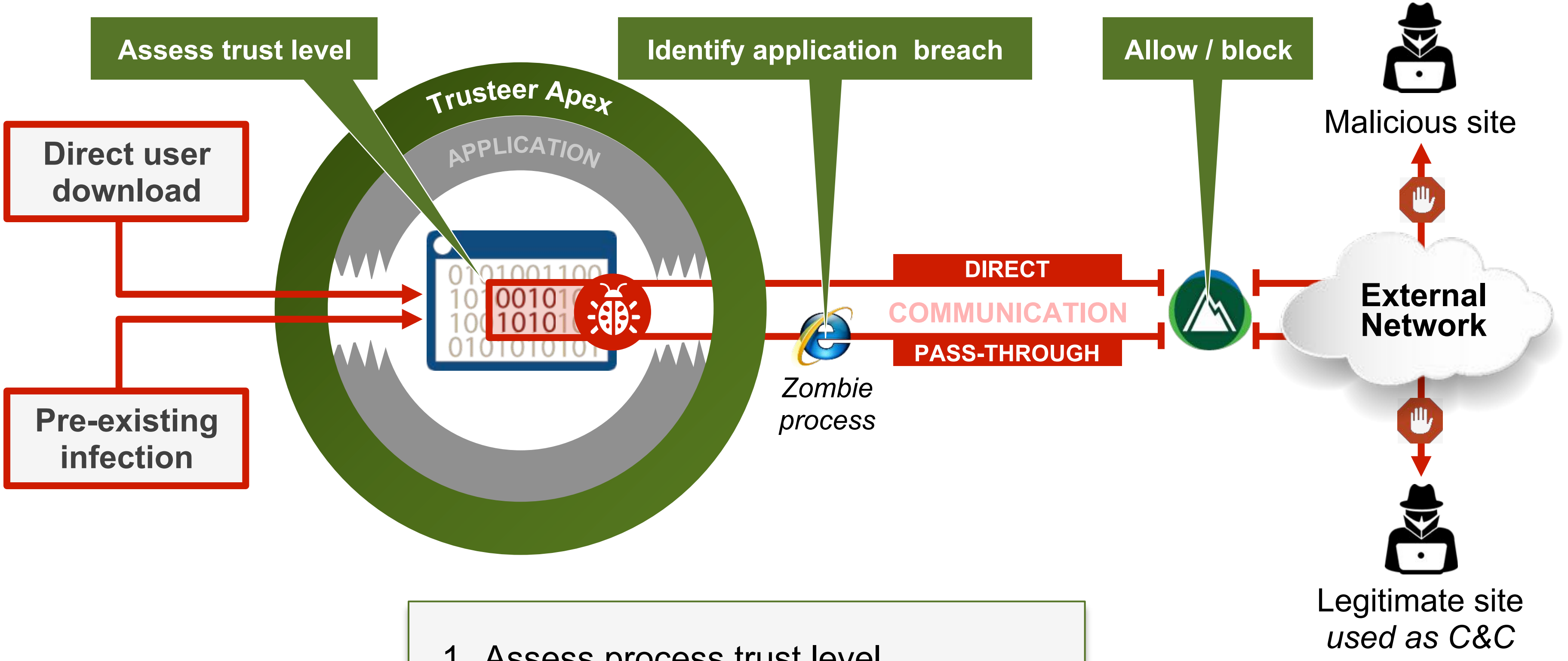
Monitor and control high risk Java application actions


JVM
Trusted app
Malicious app
Rogue Java app bypasses Java's internal controls
Allow low-risk activities
e.g., Display, local calculation
✓ Trusted app
✓ Untrusted app
Monitor and control high-risk activities
e.g., Write to file system, registry change
✓ Trusted app
☒ Untrusted app

- Malicious activity is blocked while legitimate Java applications are allowed
- Trust for specific Java apps is granted by Trusteer / IT administrator

Malicious communication blocking

Block suspicious executables that attempt to compromise other applications or open malicious communication channels



1. Assess process trust level
2. Identify process breach
3. Allow / block external communication

Client example: Major heavy equipment manufacturer

Protecting endpoints against advanced threats and malware

Discovered

32 threats

and

100 suspicious activities

within weeks of deployment despite other security products

Business challenge

- Protect 10,000 endpoints in multiple international locations
- Provide Remote Access to Suppliers, Contractors and Employees
- Prevent IP and Technology Data Theft

IBM Security Solution: Trusteer Apex

Trusteer Apex protects endpoints throughout the threat lifecycle by applying an integrated, multi-layered defense to prevent endpoint compromise for both managed and remote endpoints. Threats are continually analyzed and protections provided by Trusteer's turnkey service.

Client example: Major health care provider

Protecting endpoints against advanced threats and malware

Protecting

>25,000 Endpoints

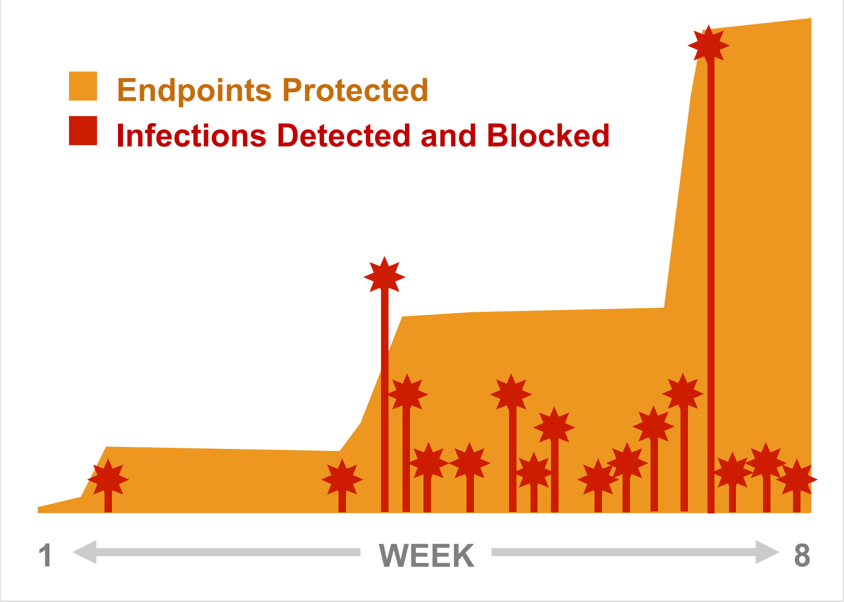
Business challenge

- Protect sensitive patient data
- Protect mission critical medical application
- Advanced malware infections despite Anti-Virus and Next Generation Firewall

IBM Security Solution: Trusteer Apex

- **200+** high risk infections detected and blocked despite deployments of traditional network and endpoint protection products
- Majority of infections included remote control capability

200 High-Risk Infections Detected During First 8 Weeks



Smarter Prevention on the Network and Endpoint to Break the Chain

1 Smarter Prevention

Trusteer Apex Endpoint Exploit Chain Disruption

NEW *Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration*

IBM Security Network Protection XGS

NEW *Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS*

2 Security Intelligence

IBM Security QRadar Security Intelligence

NEW *Data Node appliance, new flow and event APIs, and QRadar Vulnerability Manager scanning improvements*

Continuous Response 3

IBM Security QRadar Incident Forensics

NEW *Integrated forensics module with full packet search and visual reconstruction of relationships*

IBM Emergency Response Services

NEW *Increased global coverage and expertise related to malware analysis and forensics*

Global Threat Intelligence 4

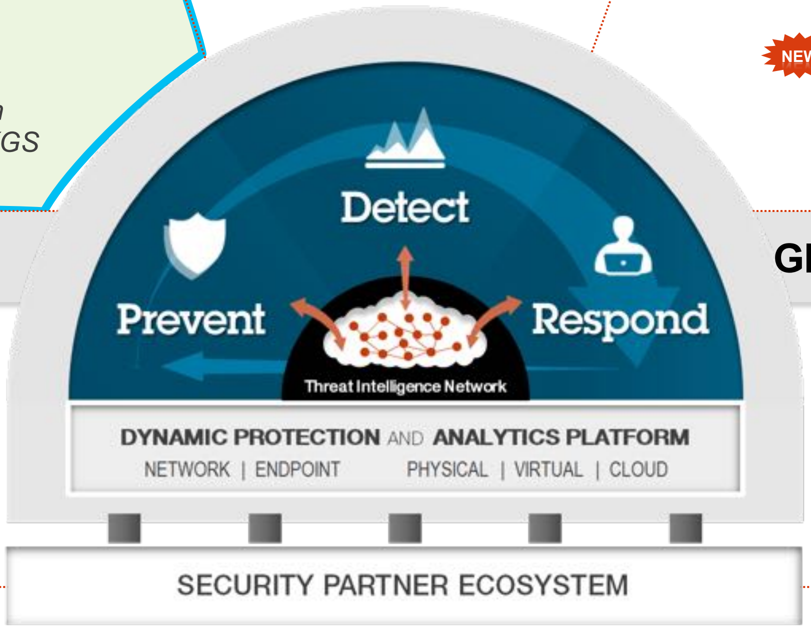
IBM X-Force Threat Intelligence

NEW *New real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force*

5 Open Integrations

Ready for IBM Security Intelligence Ecosystem

NEW *New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors*


Detect
Prevent
Respond
Threat Intelligence Network
DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT
PHYSICAL | VIRTUAL | CLOUD
SECURITY PARTNER ECOSYSTEM

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security