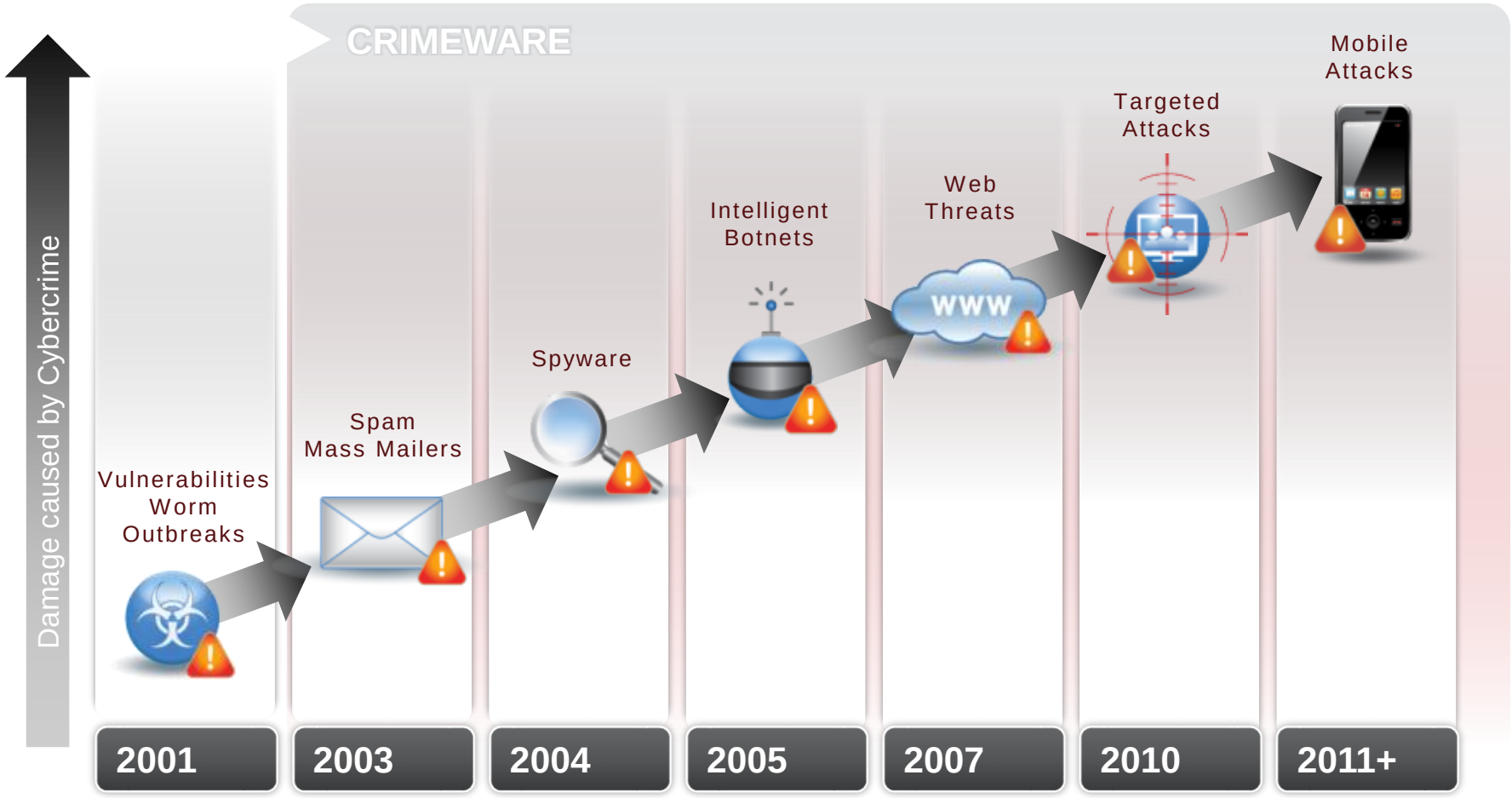
Detect and Respond:
Simplified Strategies for Targeted attacks

Raimund Genes, CTO

The Threat Landscape Evolution

Evolution to Cybercrime



South Korea – Hacktivism, Cyber Sabotage, or Cyberterrorism?

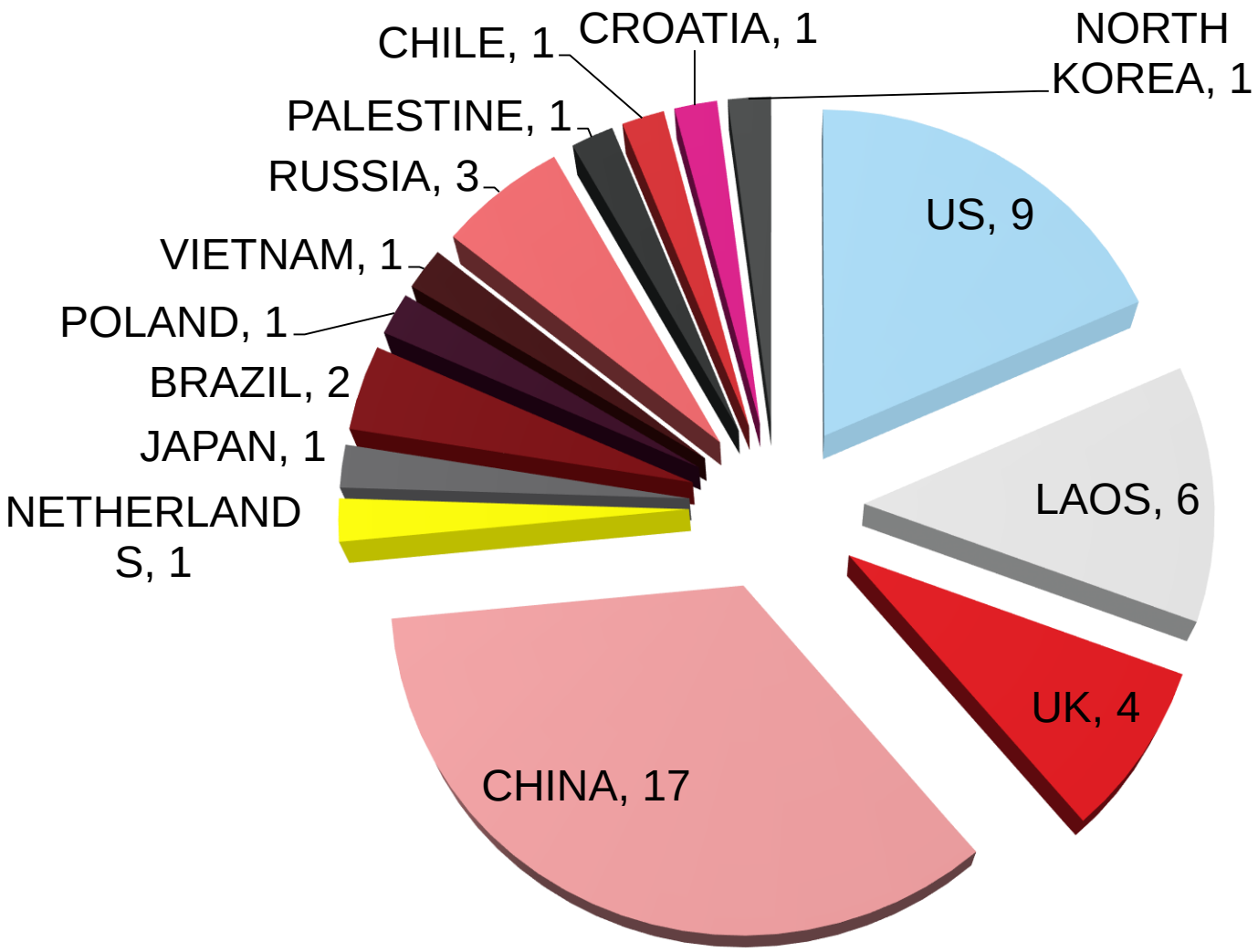
ICS targets

TREND MICRO

Let’s simulate a Water Pressure Control station

- In a small city in US with 8000 citizens
- It has to look like a real system
- And by “accident” the system has a link to the Internet

Attacks from



AP Twitter hack causes panic on Wall Street and sends Dow plunging

Market recovers after hackers tweeted from the official AP feed that two explosions had hit the White House

Heidi Moore in New York and **Dan Roberts** in Washington
guardian.co.uk, Tuesday 23 April 2013 20.41 BST

Jump to comments (62)

The panic, however brief, demonstrates how tightly intertwine become with Twitter. Photograph: Spencer Platt/Getty Image

Wall Street collided with social media on Tuesday, w from a trusted news organization sent the US stock

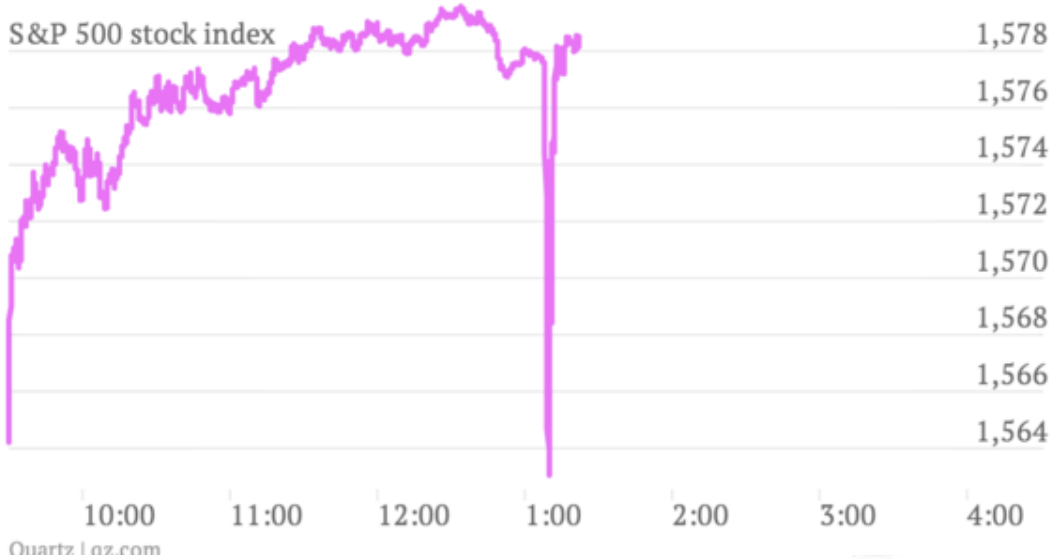
The 143-point fall in the Dow Jones industrial averag sent a message from the Twitter feed of the Associa White House had been hit by two explosions and tha injured. The fake tweet, which was immediately corr Press employees, caused a sensation on Twitter an

What Happened to Stock Markets When the AP's Twitter Account Was Hacked

Spoiler: They plunged, dramatically.

SIMONE FOXMAN AND MATT PHILLIPS | APR 23 2013, 2:35 PM ET

37 Like
78 Tweet
1 +1
10 Share



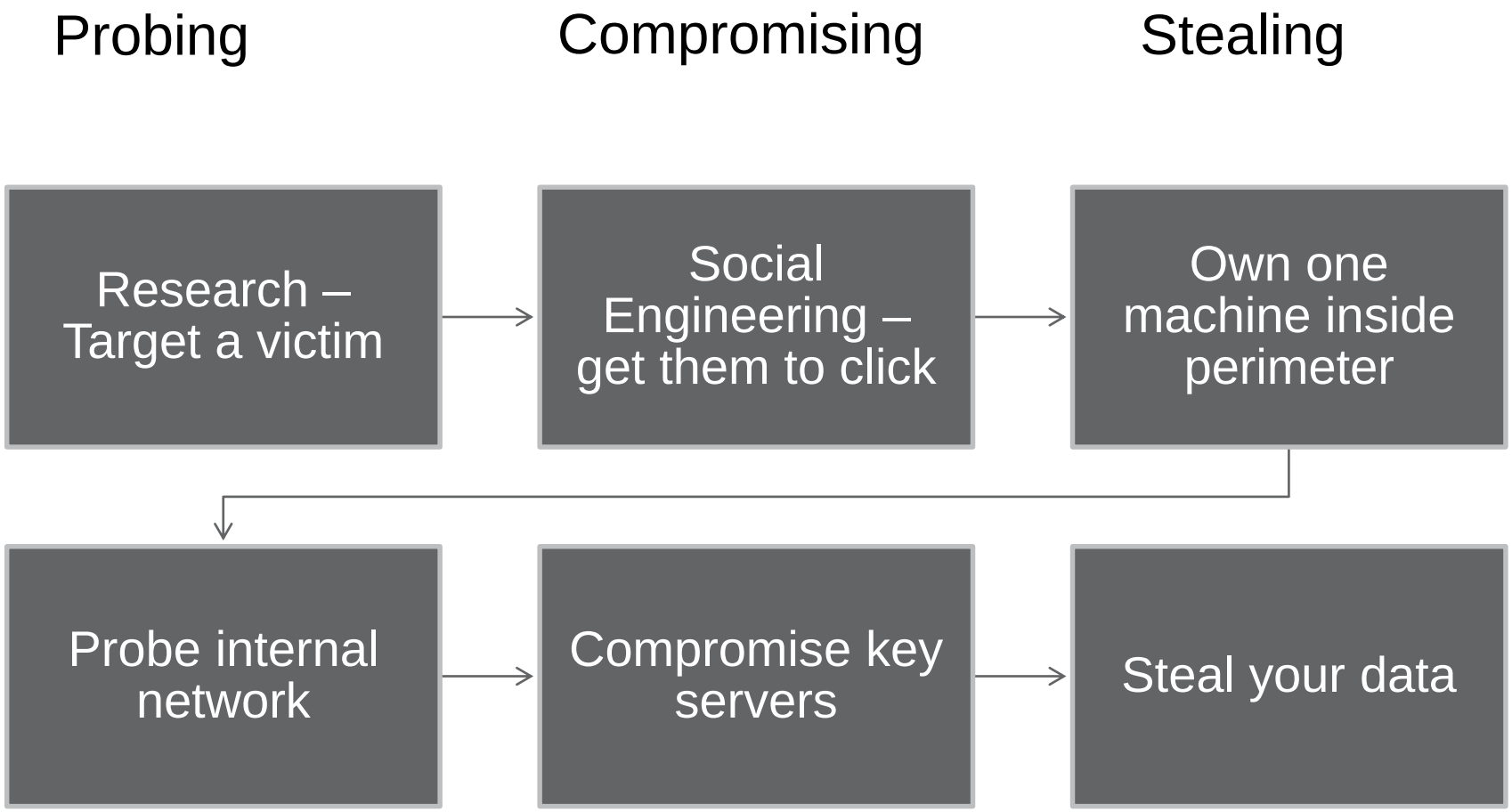
Hackers stole 45 million dollars in ATM cyber-heist

Posted on May 10, 2013 | By AP | Technology

In this undated photo provided by the United States Attorney's Office for the Southern District of New York, Elvis Rafael Rodriguez, left, and Emir Yasser Yeje, pose with bundles of cash allegedly stolen using bogus magnetic swipe cards at cash machines throughout New York. Prosecutors in New York on Thursday, May 9, 2103 said that they are members of worldwide gang of criminals who stole $45 million in hours by hacking into a database of prepaid debit cards and draining cash machines around the globe. (AP Photos/U.S. Attorney's Office for the Southern District of New York)

NEW YORK (AP) — A worldwide gang of criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe, federal prosecutors said Thursday — and outmoded U.S. card technology may be partly to blame.

How to get your prey



Trustwave 2013 Global Security Report:

Average time from initial breach to detection was 210 days, more than 35 days longer than in 2011.

The attacker knows what he's looking for!

TREND MICRO

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012 | 360 Comments

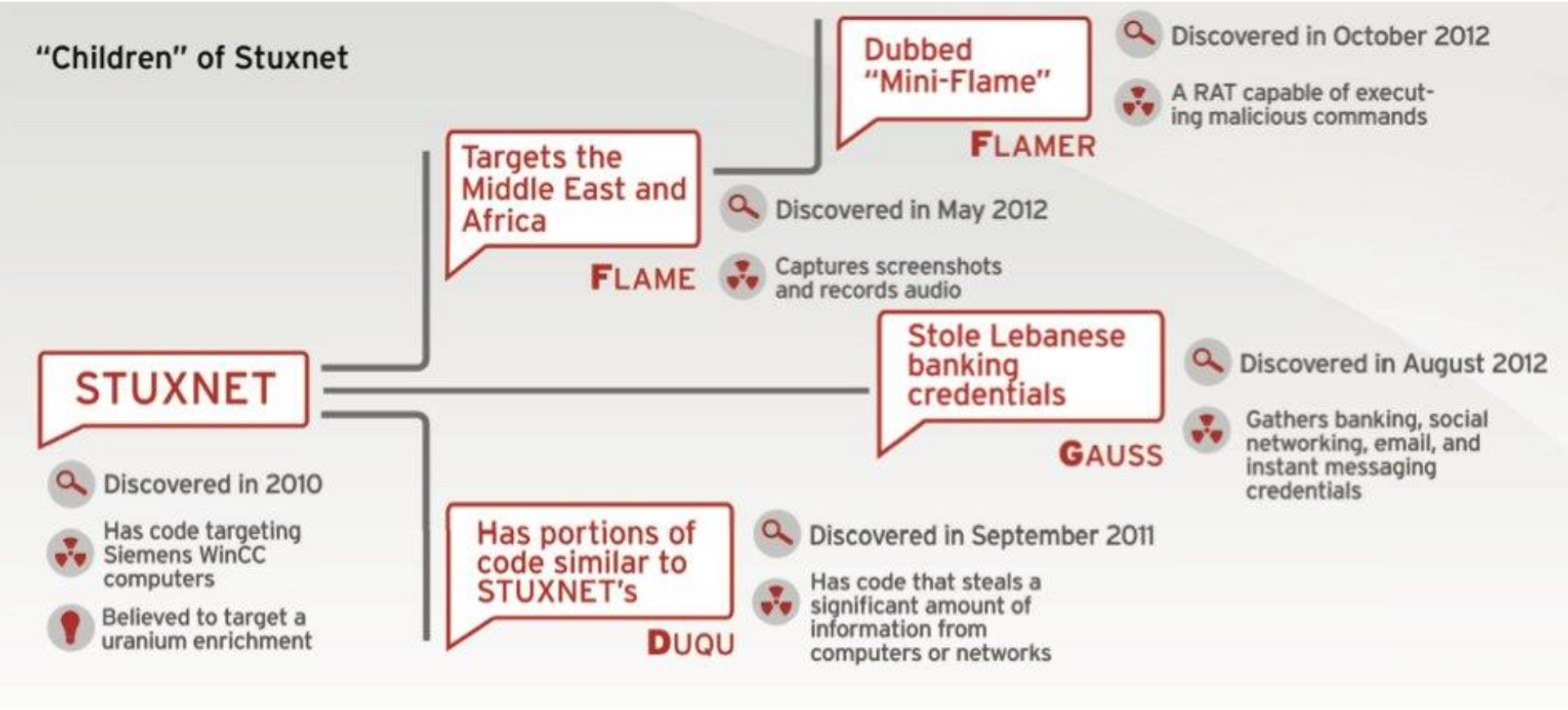
WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

FACEBOOK
TWITTER
GOOGLE+
E-MAIL
SHARE
PRINT
REPRINTS

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice

TREND MICRO


"Children" of Stuxnet
STUXNET
Discovered in 2010
Has code targeting Siemens WinCC computers
Believed to target a uranium enrichment
Targets the Middle East and Africa
FLAME
Discovered in May 2012
Captures screenshots and records audio
Dubbed "Mini-Flame"
FLAMER
Discovered in October 2012
A RAT capable of executing malicious commands
Stole Lebanese banking credentials
GAUSS
Discovered in August 2012
Gathers banking, social networking, email, and instant messaging credentials
Has portions of code similar to STUXNET's
DUQU
Discovered in September 2011
Has code that steals a significant amount of information from computers or networks

TREND MICRO

Targeted!

Name	Typ	Wert
(Standard)	REG_SZ	(Wert nicht gesetzt)
Company	REG_SZ	Trend Micro
CompanyName	REG_SZ	Trend Micro
UserInitials	REG_SZ	RG
UserName	REG_SZ	Raimund Genes

TREND MICRO

Spear Phishing

CVE-2009-3129
CVE-2010-3333
CVE-2011-1980
CVE-2009-3129
CVE-2012-0754

Normally has exploits as attachments in the guise of documents

Displays normal files

Malicious C&C servers

Waterholing

TREND MICRO

Bits

FEBRUARY 19, 2013, 4:35 PM | 5 Comments

Apple Computers Hit by Sophisticated Cyberattack

By NICOLE PERLROTH

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL
SHARE
PRINT

Cyberattacks, apparently, happen in threes.

Karen Bleier/Agence France-Presse — Getty Images

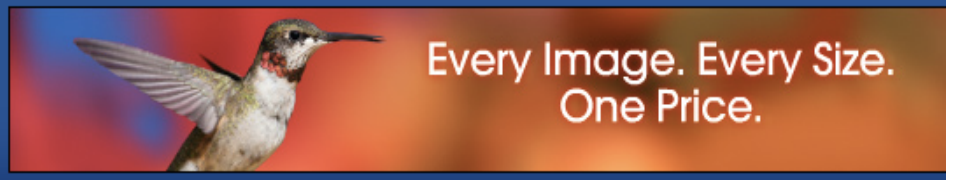
After Facebook and Twitter announced that they were breached by sophisticated hackers in recent weeks, Apple said it had been attacked, too, in a rare admission for the technology giant.

In a statement to reporters Tuesday, Apple said some of its computers were infected with the same malware that hit Twitter and Facebook. Like Facebook, Apple confirmed that its employees' computers were infected with malware when they visited a Web site for software developers. Neither company has named the Web site. But according to a person with knowledge of Facebook's investigation, the compromised site, iPhonedevsdk, an online forum for software developers, is still infected. (In other words, unless you want to be owned by hackers, *do not visit the site.*)

"We identified a small number of systems within Apple that were infected and isolated them from our network," Apple said in a statement. "There is no evidence that any data left Apple. We are working closely with law enforcement to find the source of the malware."

Twitter said attackers may have briefly gained access to data for 250,000 user accounts and that it reset passwords for and alerted users whose data may have been vulnerable. Facebook said that no user data was taken in its

TREND MICRO



iPhoneDevSDK has learned it was used as part of an attack whose victims included large internet companies. We have no reason to believe user data was compromised, but to be safe, we've reset all user passwords. **Please read more on this thread.**

iPhoneDevSDK compromised: What happened and how we are dealing with it

iseff Posts: **22** Administrators

5:16AM in Site News & Announcements

Today, we were alerted that our site was part of an elaborate and sophisticated attack whose victims included large internet companies. We were alerted through the press, via an AllThingsD article, which cited Facebook. Prior to this article, we had no knowledge of this breach and hadn't been contacted by Facebook, any other company, or any law enforcement about the potential breach. You can read more about the attack via Facebook's blog post.

As the most widely read dedicated iOS developer forum, we're targeted for attacks frequently. Security is a top priority for us, which is one reason why we switched to Vanilla Forums to host our site last year. Vanilla manages security like pros, and I should be clear that -- as best we can tell right now -- this attack has nothing to do with their software.

Immediately, we were in contact with Facebook's security team, including Joe Sullivan, Facebook's Chief Security Officer, and his team, to learn what they knew. We also contacted Vanilla, our amazing forum hosts, to ensure the problem was not with their software.

What we've learned is that it appears a single administrator account was compromised. The hackers used this account to modify our theme and inject JavaScript into our site. That JavaScript appears to have used a sophisticated, previously unknown exploit to hack into certain user's computers.

We're still trying to determine the exploit's exact timeline and details, but it appears as though it was ended (by the hacker) on January 30, 2013.

As with Facebook, it's important to stress that we have no reason to believe user data was compromised.

Just to be sure, we've reset all users' passwords. Please use our Forgot Password feature the next time you log in to reset your password.

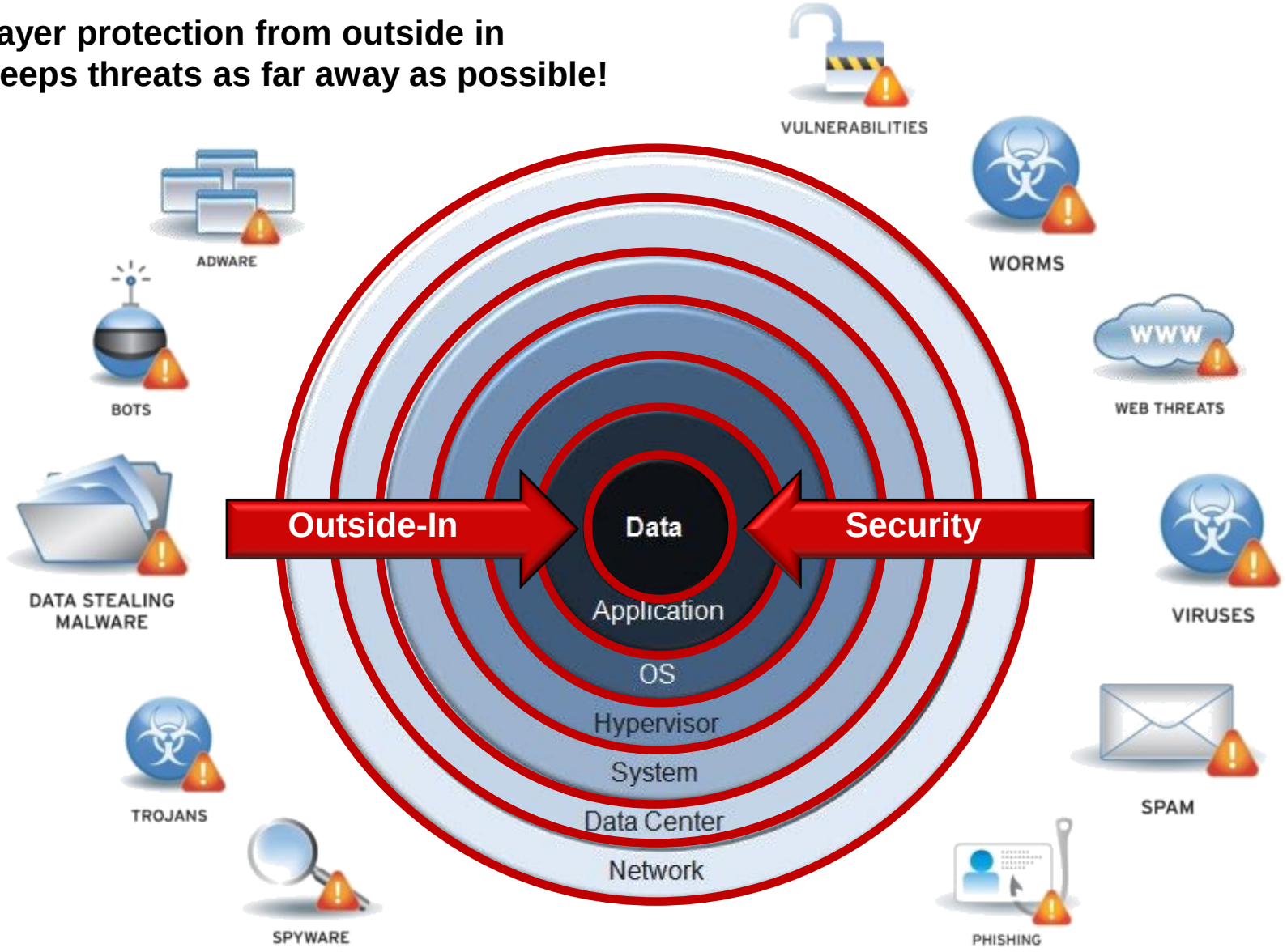
We're continuing to work with Facebook, Vanilla, other targeted companies, and law enforcement to find out who is behind this sophisticated attack.

If someone wants to get in, he get's in!

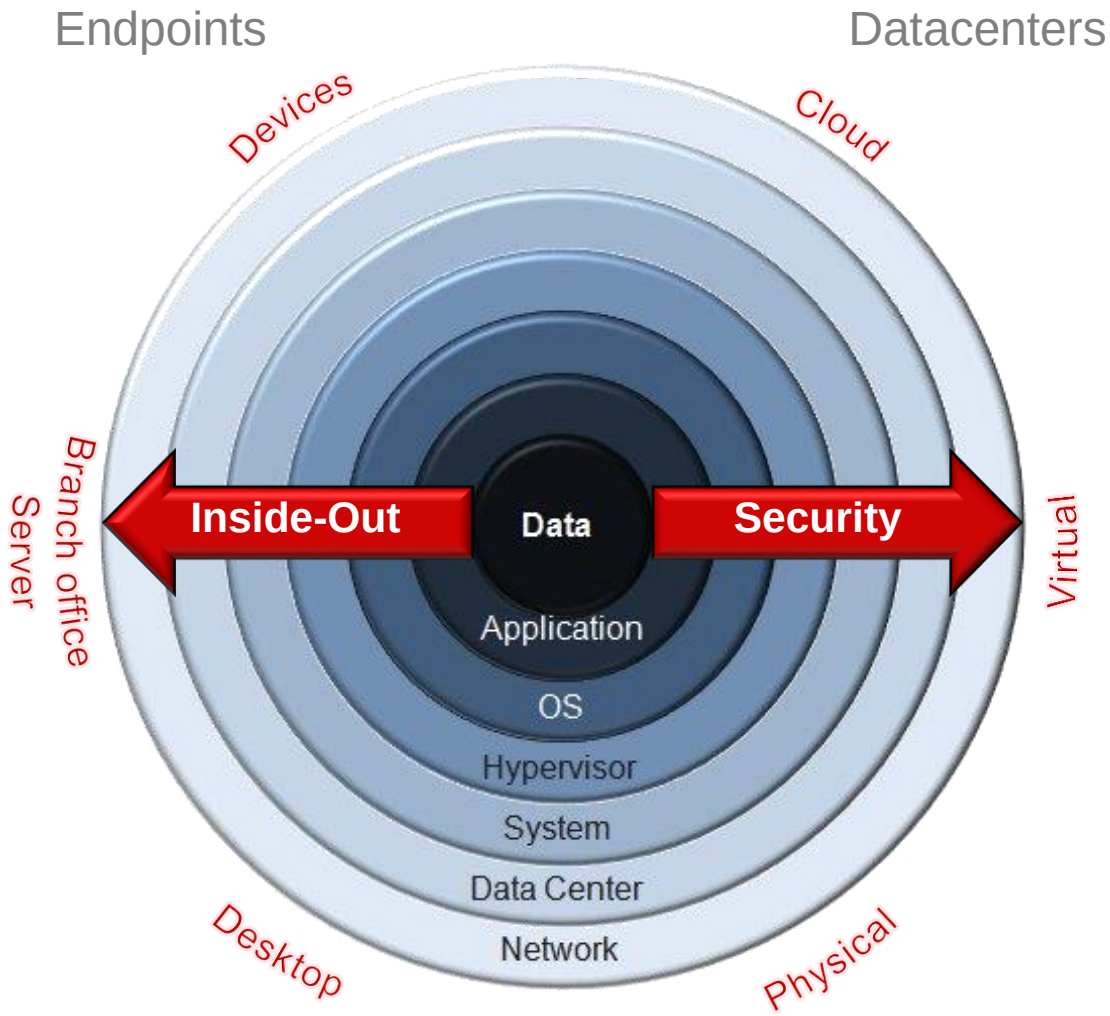
CHEWY DRAGEES
NATURAL MINT FLAVOUR
mentos
mint

Outside-in Model of Perimeter Defense

Layer protection from outside in
Keeps threats as far away as possible!



Inside-out Security



FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions face new **challenges** that can only be solved using active systems like FinSpy:
- Data not transmitted over any network
- Encrypted Communications
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION	
Usage:	· Strategic Operations · Tactical Operations
Capabilities:	· Remote Computer Monitoring · Monitoring of Encrypted Communications
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communication** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **Country Tracing** of Target
- **Silent extracting of Files** from Hard-Disk
- **Process-based Key-logger** for faster analysis
- **Live Remote Forensics** on Target System
- **Advanced Filters** to record only important information
- Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communication using **RSA 2048 and AES 256**
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

For a full feature list please refer to the Product Specifications.

Targeted!

Name	Typ	Wert
(Standard)	REG_SZ	(Wert nicht gesetzt)
Company	REG_SZ	Trend Micro
CompanyName	REG_SZ	Trend Micro
UserInitials	REG_SZ	RG
UserName	REG_SZ	Raimund Genes

TREND MICRO

PayPal Security <paypalhilfe@webgo24.de>
An: RAIMUND GENES
Raimund Genes, Beschränkung Ihres Benutzerkontos - Ihre Mithilfe ist gefragt

---

PayPal™ Konfliktlösung

Guten Tag, Raimund Genes!

Bitte seien Sie uns dabei behilflich, Ihr Benutzerkonto wieder in Ordnung zu bringen.
Bis dahin haben wir den Zugang zu Ihrem Benutzerkonto vorübergehend eingeschränkt, um potenziellem Missbrauch vorzubeugen.

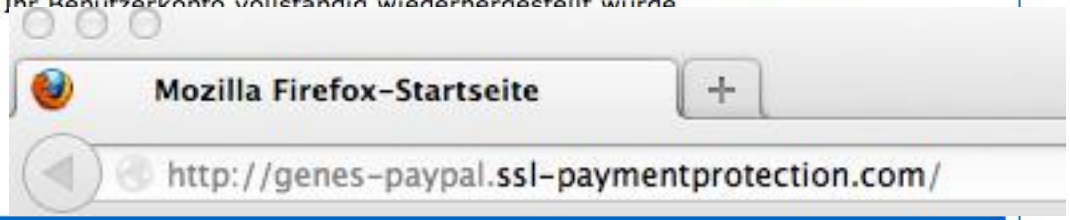
Wo liegt das Problem?

Laut unserem Sicherheitssystem wurde mehrfach erfolglos versucht sich in Ihr Benutzerkonto einzuloggen.

Bearbeitungsnummer: PP-039-962-815-130

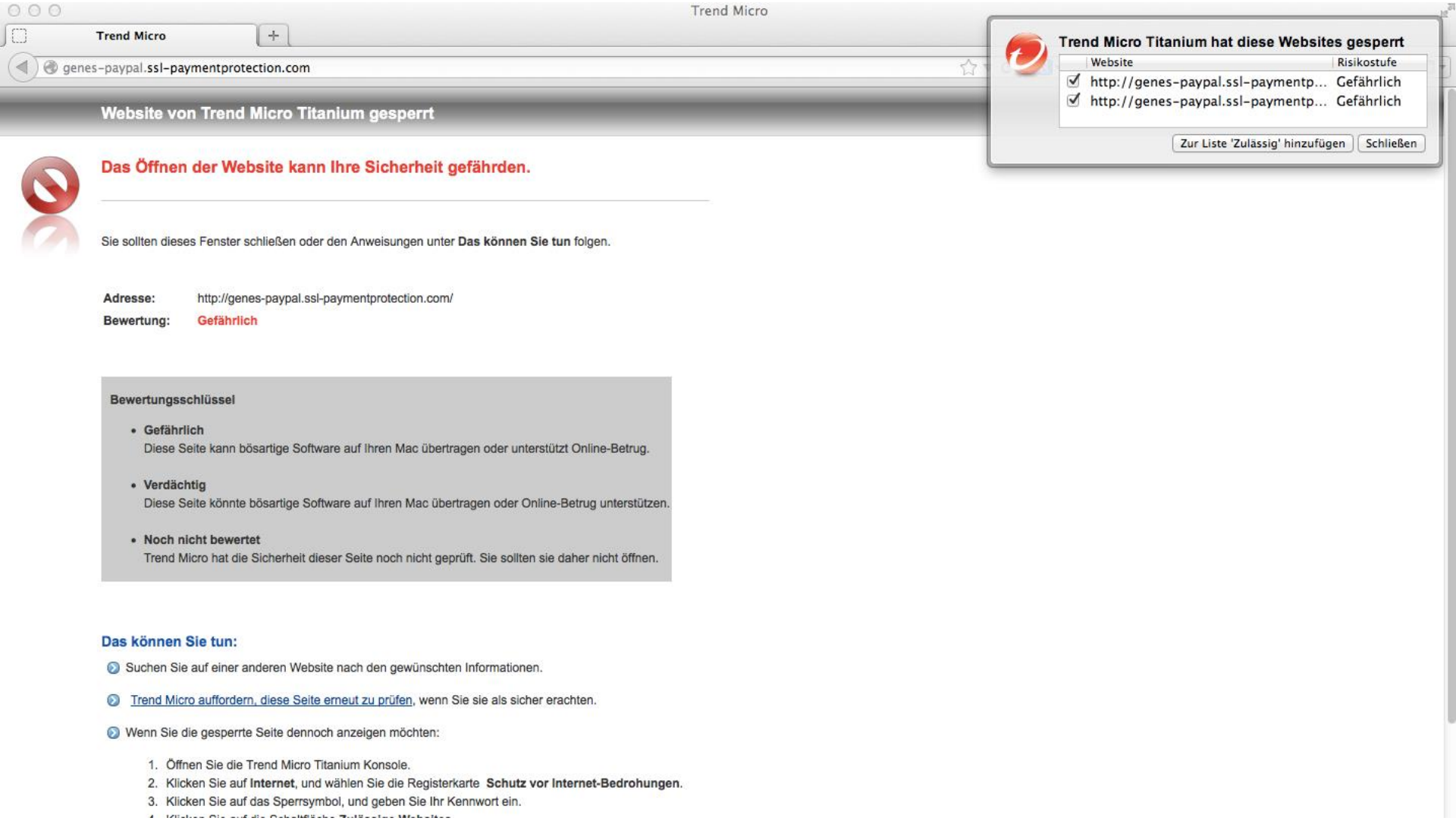
Was ist nun zu tun?

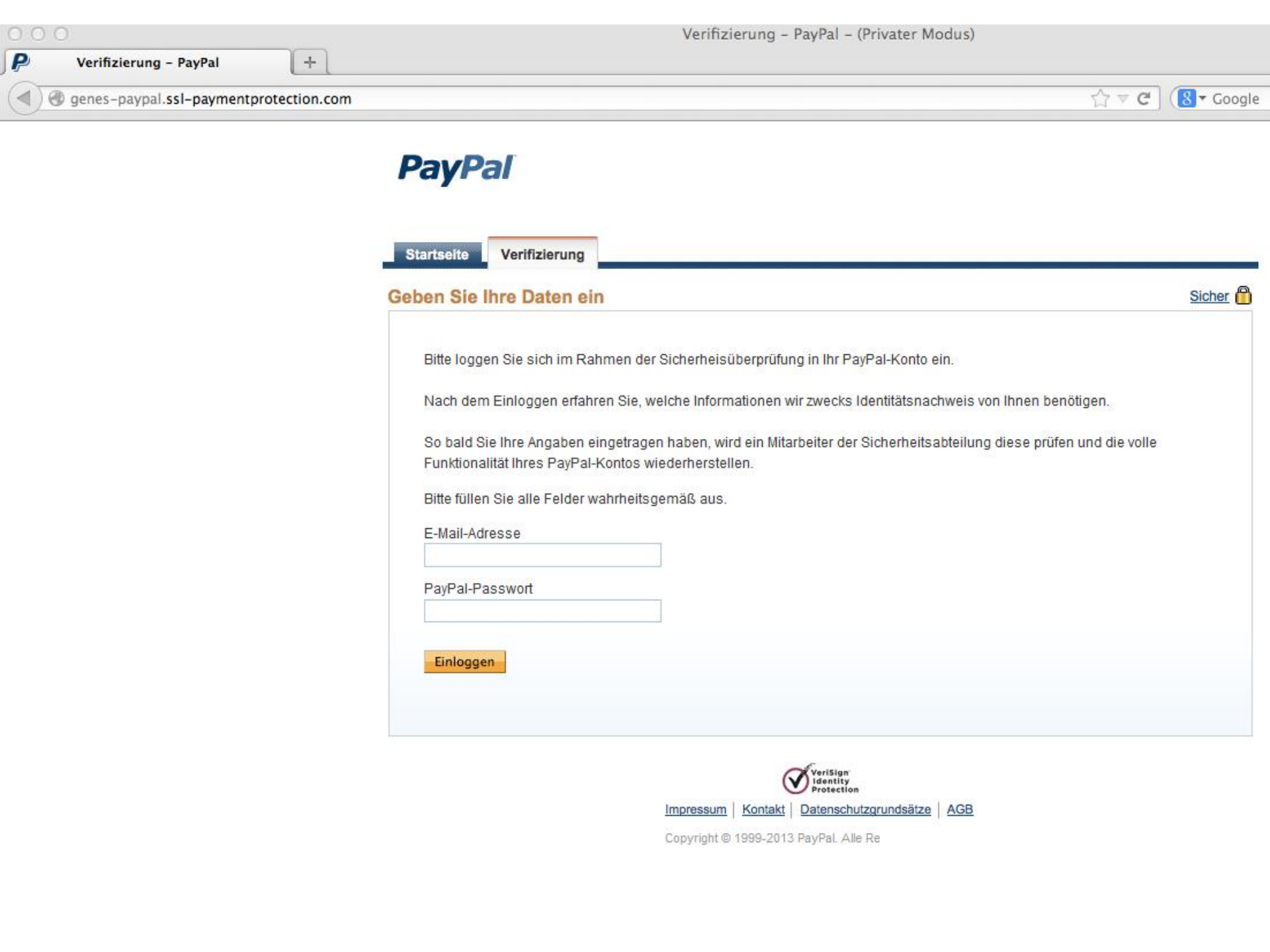
Bitte loggen Sie sich in Ihr Benutzerkonto ein und befolgen Sie die Anweisungen. Dort sehen Sie, welche Informationen benötigt werden - und können sie gleich einreichen. Und Sie sehen anschließend, dass Ihr Benutzerkonto vollständig wiederhergestellt wurde.



Copyright © 1999–2013 PayPal. Alle Rechte vorbehalten. PayPal (Europe) S.à r.l. et Cie, S.C.A., Société en Commandite par Actions. Eingetragener Firmensitz: 22-24 Boulevard Royal, L-2449 Luxembourg RCS Luxembourg B 118 349.

Signatur-Code: f8bd9a6f7e7d7079fffc995f08beb849


Trend Micro
Trend Micro
genes-paypal.ssl-paymentprotection.com
Website von Trend Micro Titanium gesperrt
Das Öffnen der Website kann Ihre Sicherheit gefährden.
Sie sollten dieses Fenster schließen oder den Anweisungen unter Das können Sie tun folgen.
Adresse: http://genes-paypal.ssl-paymentprotection.com/
Bewertung: Gefährlich
Bewertungsschlüssel
Gefährlich
Diese Seite kann bösartige Software auf Ihren Mac übertragen oder unterstützt Online-Betrug.
Verdächtig
Diese Seite könnte bösartige Software auf Ihren Mac übertragen oder Online-Betrug unterstützen.
Noch nicht bewertet
Trend Micro hat die Sicherheit dieser Seite noch nicht geprüft. Sie sollten sie daher nicht öffnen.
Das können Sie tun:
Suchen Sie auf einer anderen Website nach den gewünschten Informationen.
Trend Micro auffordern, diese Seite erneut zu prüfen, wenn Sie sie als sicher erachten.
Wenn Sie die gesperrte Seite dennoch anzeigen möchten:
1. Öffnen Sie die Trend Micro Titanium Konsole.
2. Klicken Sie auf Internet, und wählen Sie die Registerkarte Schutz vor Internet-Bedrohungen.
3. Klicken Sie auf das Sperrsymbol, und geben Sie Ihr Kennwort ein.
Trend Micro Titanium hat diese Websites gesperrt
Website
Risikostufe
http://genes-paypal.ssl-paymentp... Gefährlich
http://genes-paypal.ssl-paymentp... Gefährlich
Zur Liste 'Zulässig' hinzufügen
Schließen


Verifizierung – PayPal – (Privater Modus)
Verifizierung – PayPal
genes-paypal.ssl-paymentprotection.com
Google
PayPal
Startseite
Verifizierung
Geben Sie Ihre Daten ein
Sicher
Bitte loggen Sie sich im Rahmen der Sicherheisüberprüfung in Ihr PayPal-Konto ein.
Nach dem Einloggen erfahren Sie, welche Informationen wir zwecks Identitätsnachweis von Ihnen benötigen.
So bald Sie Ihre Angaben eingetragen haben, wird ein Mitarbeiter der Sicherheitsabteilung diese prüfen und die volle Funktionalität Ihres PayPal-Kontos wiederherstellen.
Bitte füllen Sie alle Felder wahrheitsgemäß aus.
E-Mail-Adresse
PayPal-Passwort
Einloggen
VeriSign Identity Protection
Impressum | Kontakt | Datenschutzgrundsätze | AGB
Copyright © 1999-2013 PayPal. Alle Re

PayPal

Startseite | Verifizierung

Geben Sie Ihre Daten ein

Sicher

Vorname
Donald

Nachname
Duck

Geburtsdatum

TT MM JJJJ

01 . 01 . 1999

Straße und Hausnummer
Donaldigasse 1

Zusatzinformationen (optional)

PLZ
81111

Ort
Donaldsville

Weiter

VeriSign Identity Protection

Impressum | Kontakt | Datenschutzgrundsätze | AGB

Copyright © 1999-2013 PayPal. Alle Rechte vorbehalten.

Startseite | Verifizierung

Geben Sie Ihre Daten ein

Sicher

Kontoinhaber
(Nicht Name der Bank)

Kontonummer
(1-11 Ziffern)

Bankleitzahl (BLZ)
(8 Ziffern)

Kreditkarteninhaber
(Wie auf der Karte angegeben)

Kreditkartennummer
(12-16 Ziffern)

Kartenprüfnummer (CVV/CVV2)
(3 Ziffern, Rückseite der Kreditkarte)

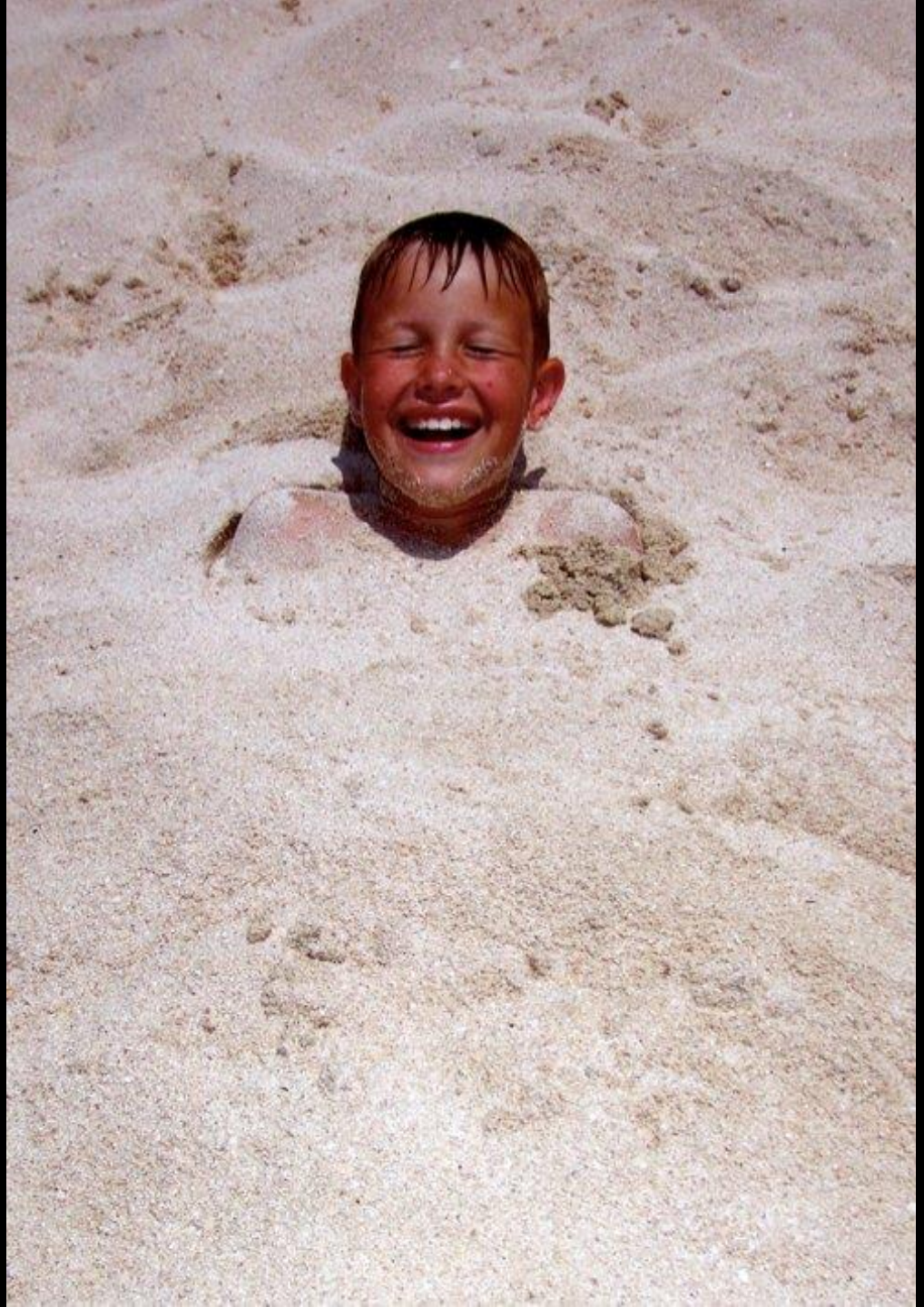
Verfallsdatum
MM JJJJ

Kartenlimit
(Aktuelles Kreditkartenlimit. Zu finden auf Ihrer Kreditkartenabrechnung)

Verified by Visa / MasterCard Secure Code
(Einzutragen, falls Ihre Karte für eines der Verfahren registriert ist.)

VERIFIED by VISA MasterCard SecureCode

Abschließen der Verifizierung

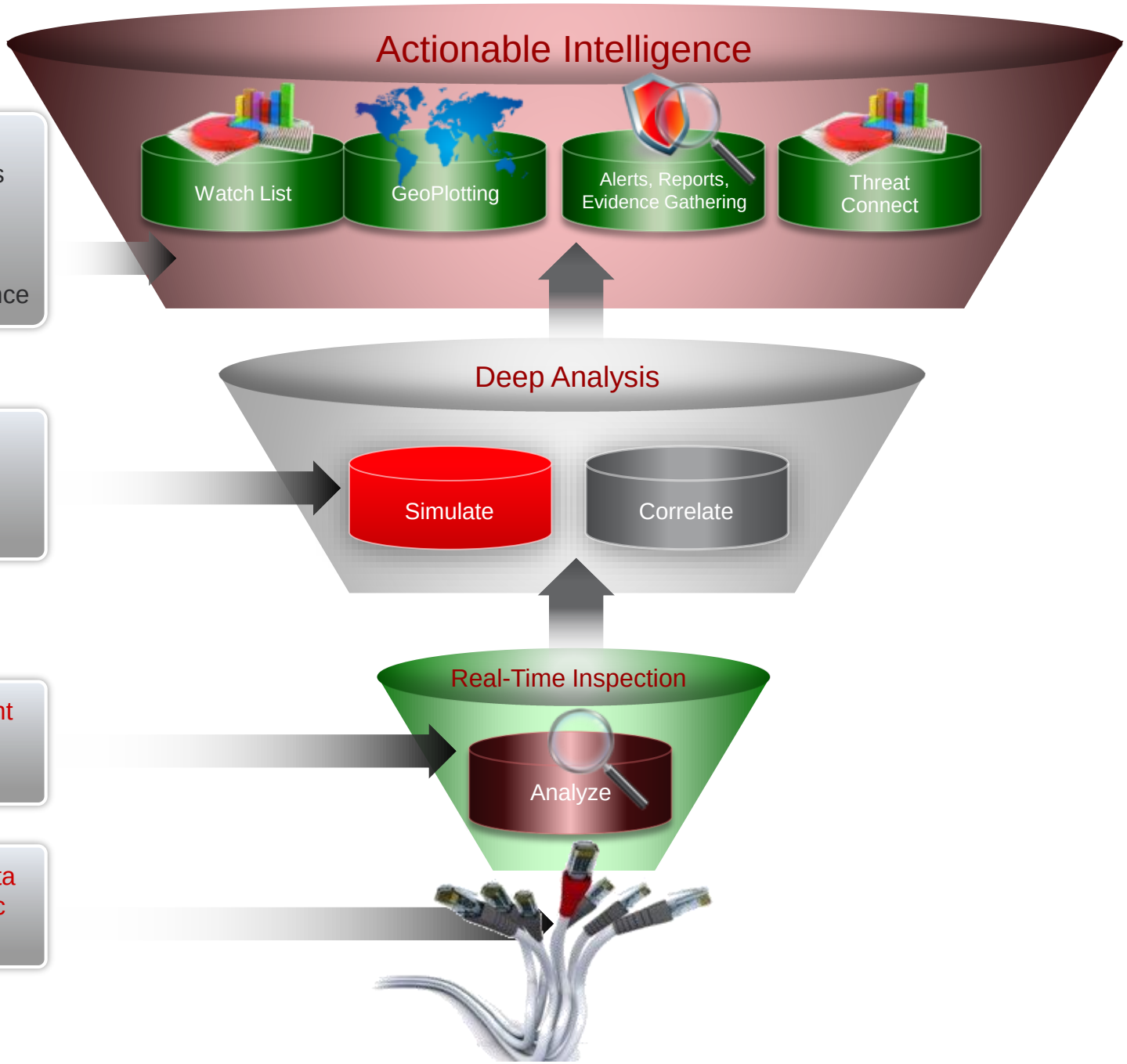


Visibility
– Real-time Dashboards
Insight
– Risk-based Analysis
Action
– Remediation Intelligence

Identify Attack Behavior & Reduce False Positives

Detect Malicious Content and Communication

Out of band network data feed of all network traffic



Disabled 48,700 computers in S. Korea

NH Bank NongHyup

제주은행 JEJU BANK

신한은행 SHINHAN BANK

KBS

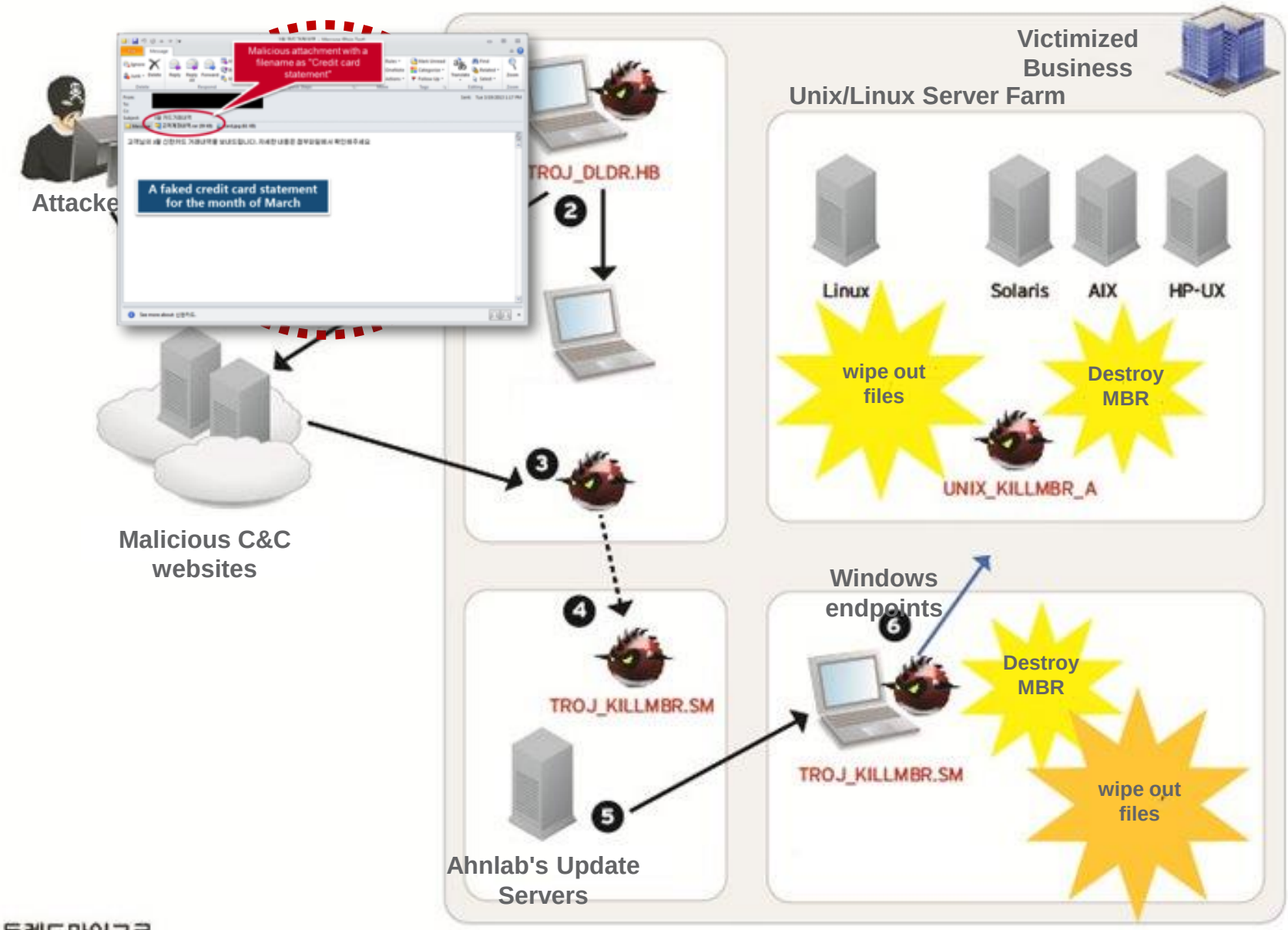
MBC

YTN

Impact

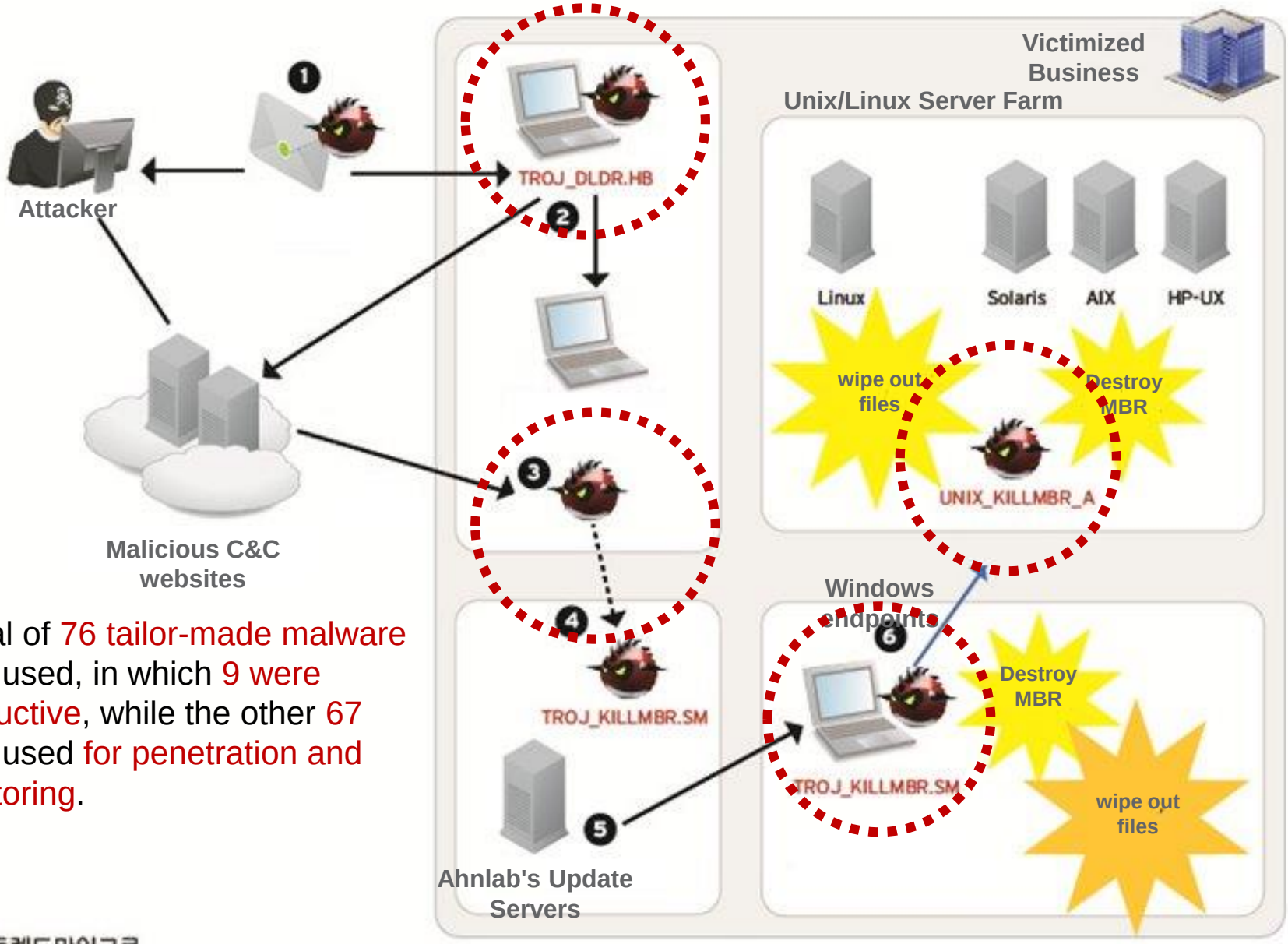
- Disruption in business continuity
  - Banking: ATM, banking operations, and online banking came to a halt.
  - TV/Media: media contents to be broadcasted couldn't be updated. Public facing websites taken down.
- Data loss
  - Data on compromised systems couldn't be recovered
- Public
  - Unable to withdraw from ATM
  - Unable to process credit card transactions

Penetration with phishing email



출처 - 트렌드마이크로

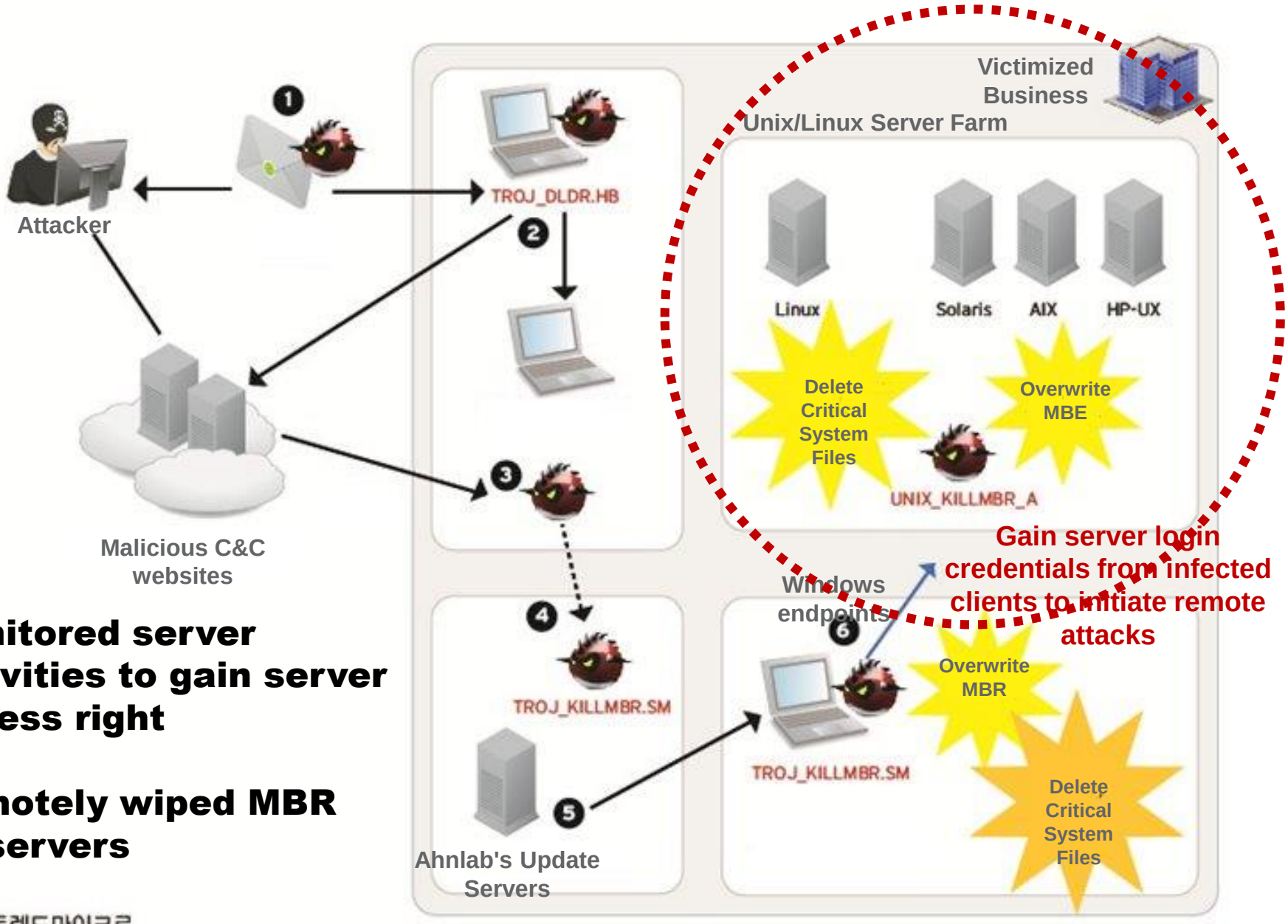
Evade detection with customized malware



A total of 76 tailor-made malware were used, in which 9 were destructive, while the other 67 were used for penetration and monitoring.

출처 – 트렌드마이크로

Servers breached after credentials compromised



Monitored server activities to gain server access right

Remotely wiped MBR on servers

출처 – 트렌드마이크로

How a Bank Averted this attack with Trend Micro

- Deep Discovery Inspector (DDI) intercepted potentially malicious content in SMTP traffic
- Content was ‘detonated’ in a sandbox
- C&C communication and sample files were identified
- Administrator applied custom blacklist to other security control
- Customized signatures were deployed to endpoints for immediate cleanup

An spear-phishing email was sent to an employee. The email contained a malicious attachment.

Trend Micro Deep Discovery detected potential malicious content in SMTP traffic as HEUR_NAMETRICK.B

Attachment was sent to sandbox for real-time analysis.

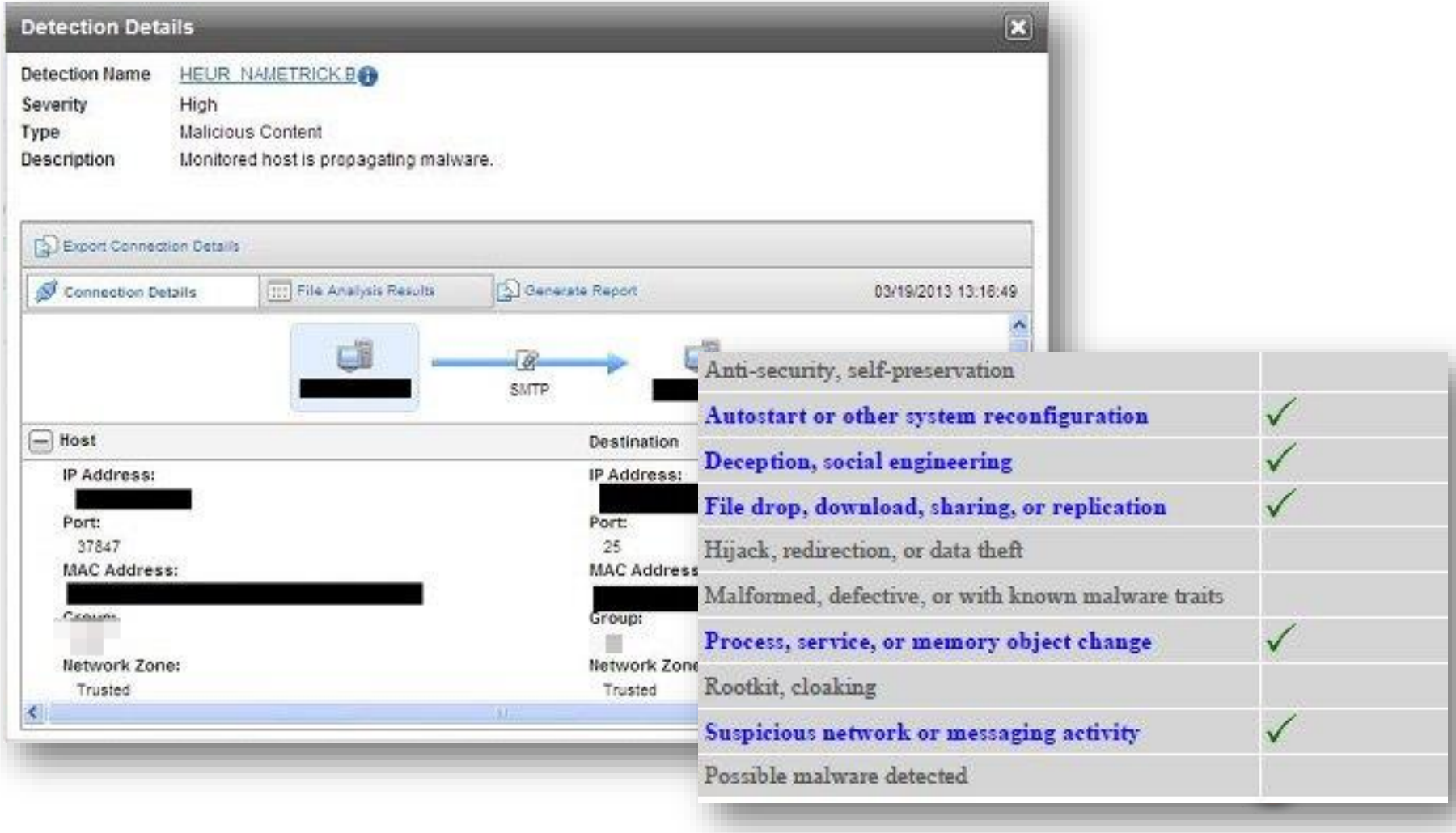
IT admin obtained results from sandbox, performs necessary steps (URL blocking, etc.). THREAT AVERTED.

DEEP DISCOVERY INSPECTOR (DDI)

TREND MICRO

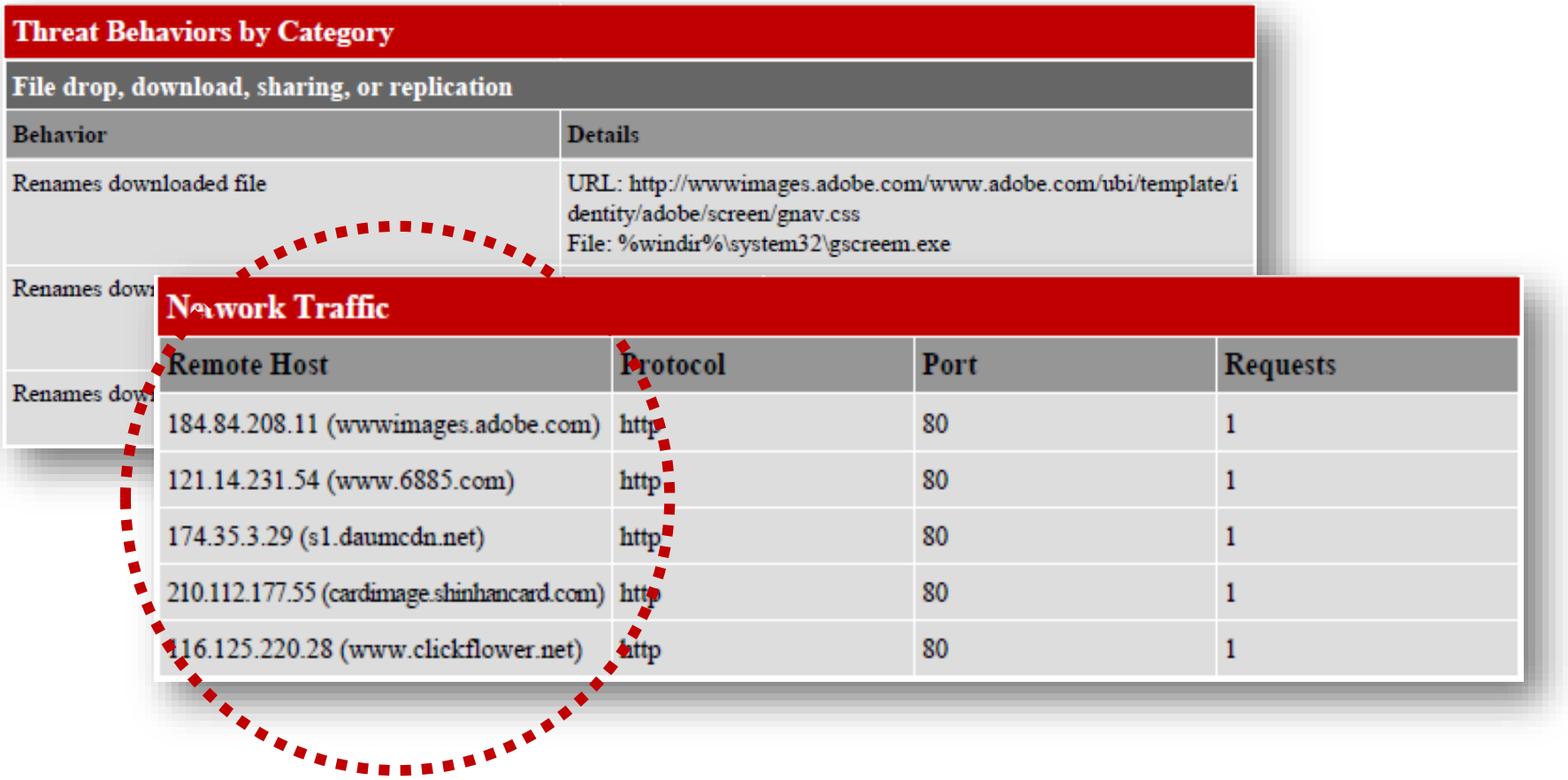
Early detection of spear-phishing email

With sandbox analysis, DDI detected the suspicious email and identified its attachment as a Trojan downloader



Sandbox Analysis Provided Actionable Intelligence

The sandbox analysis exposed malicious behaviors embedded and C&C communications the bad URL and IP. Administrator updated firewall/IPS rules to terminate C&C communications.



Threat Behaviors by Category

File drop, download, sharing, or replication

Behavior	Details
Renames downloaded file	URL: http://wwwimages.adobe.com/www.adobe.com/ubi/template/identity/adobe/screen/gnav.css File: %windir%\system32\gscreem.exe
Renames dow	
Renames dow	

Network Traffic

Remote Host	Protocol	Port	Requests
184.84.208.11 (wwwimages.adobe.com)	http	80	1
121.14.231.54 (www.6885.com)	http	80	1
174.35.3.29 (s1.daumcdn.net)	http	80	1
210.112.177.55 (cardimage.shinhancard.com)	http	80	1
116.125.220.28 (www.clickflower.net)	http	80	1