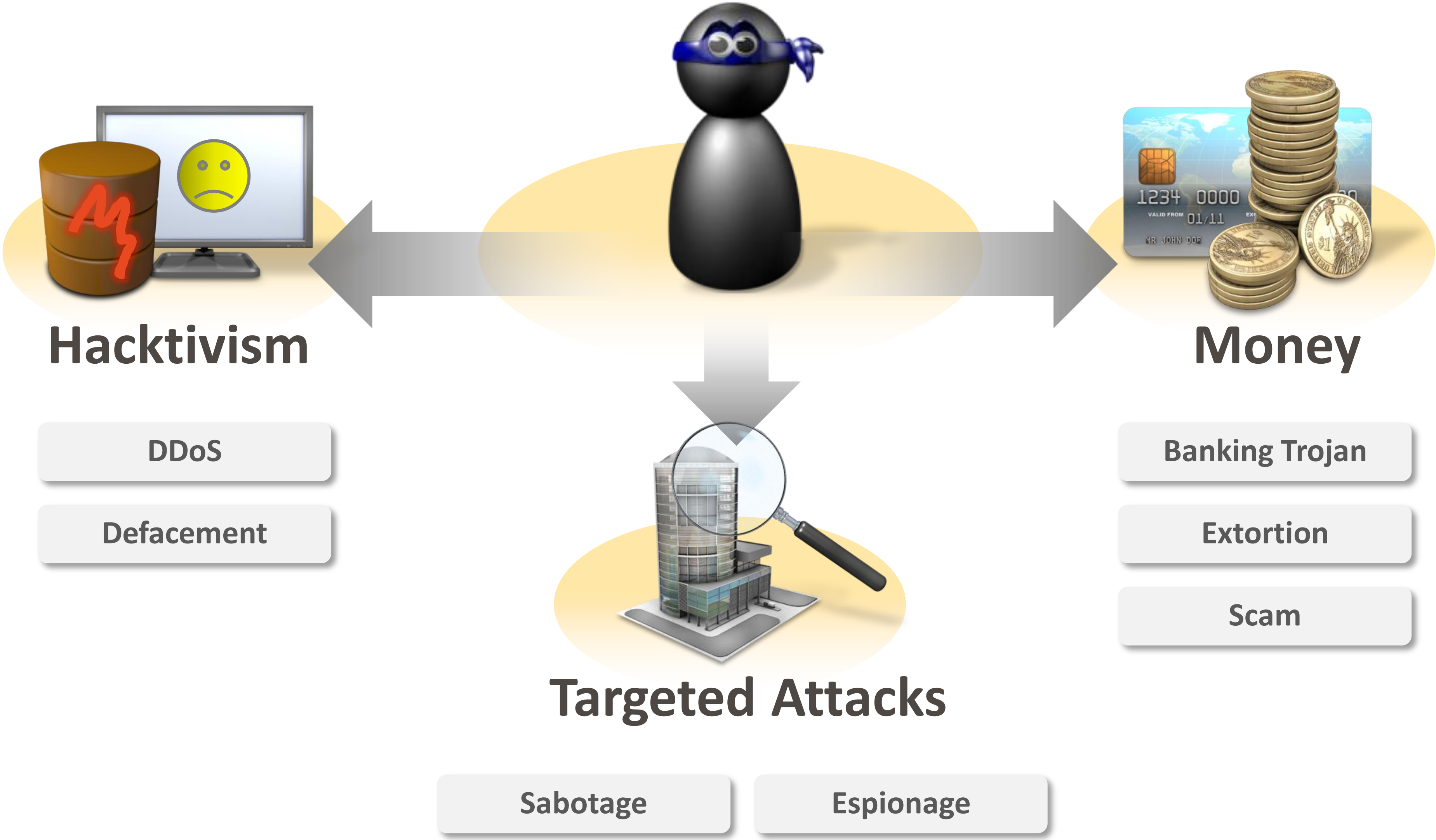
GRIFES

Threat Landscape

Antonio Sirera

Managing Director, Symantec Suisse

Different Motivation – Different Attacks



Hacktivism

- DDoS
- Defacement

Money

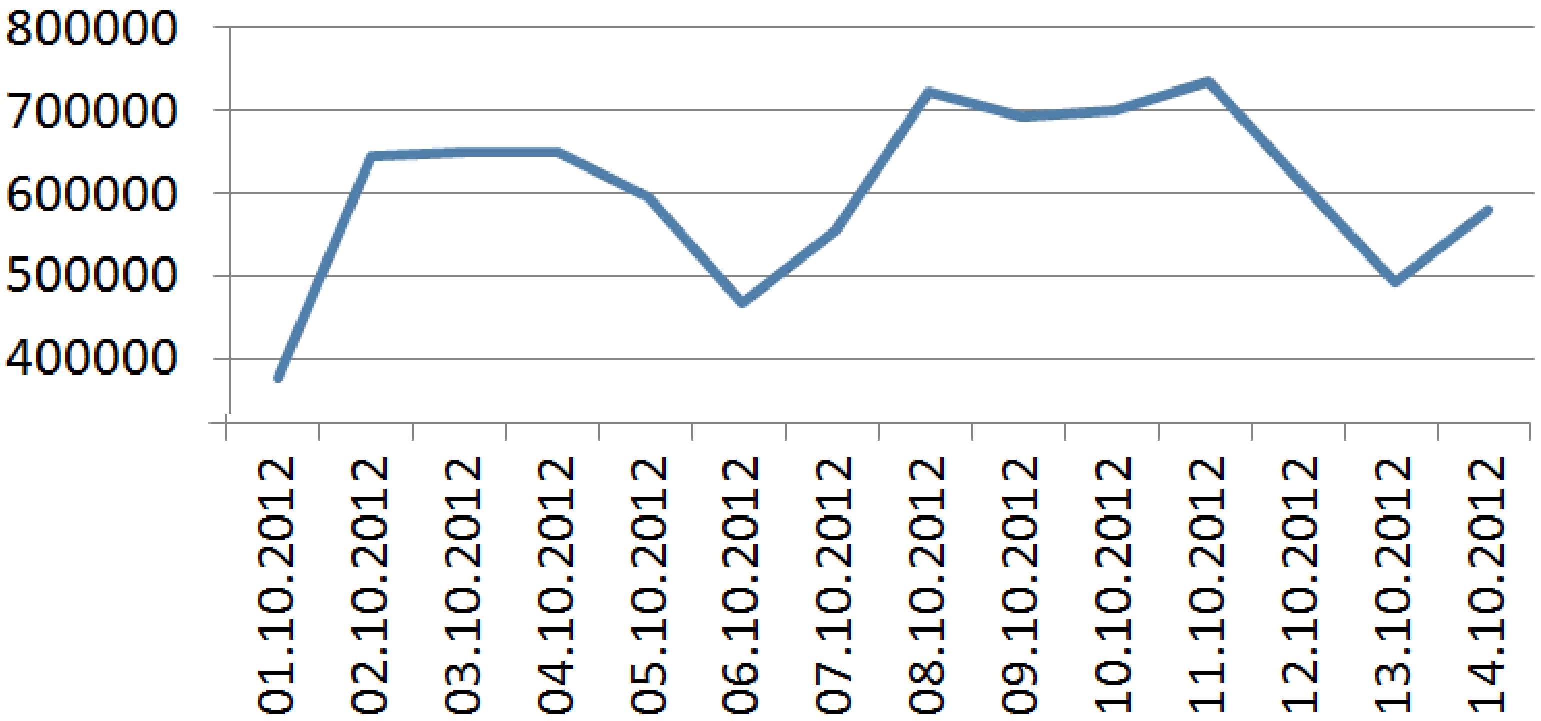
- Banking Trojan
- Extortion
- Scam

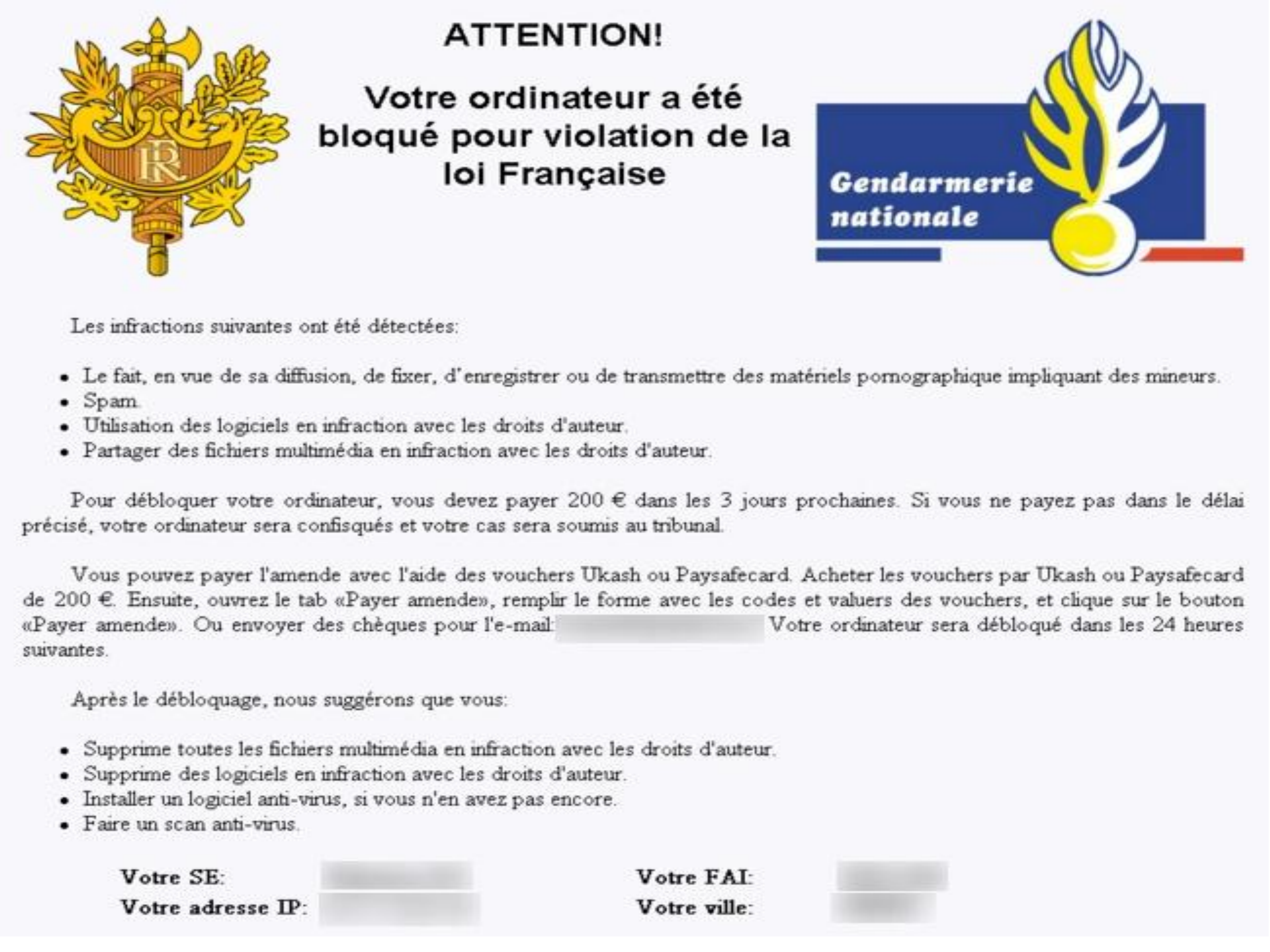
Targeted Attacks

- Sabotage
- Espionage

New malware variants per day (globally)

- On average 600’000 new variants / day at end of 2012
- A lot due to polymorphic runtime packers and file infectors





ATTENTION!

Votre ordinateur a été bloqué pour violation de la loi Française

Les infractions suivantes ont été détectées:

- Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre des matériels pornographique impliquant des mineurs.
- Spam.
- Utilisation des logiciels en infraction avec les droits d'auteur.
- Partager des fichiers multimédia en infraction avec les droits d'auteur.

Pour débloquer votre ordinateur, vous devez payer 200 € dans les 3 jours prochaines. Si vous ne payez pas dans le délai précisé, votre ordinateur sera confisqués et votre cas sera soumis au tribunal.

Vous pouvez payer l'amende avec l'aide des vouchers Ukash ou Paysafecard. Acheter les vouchers par Ukash ou Paysafecard de 200 €. Ensuite, ouvrez le tab «Payer amende», remplir le forme avec les codes et valuers des vouchers, et clique sur le bouton «Payer amende». Ou envoyer des chèques pour l'e-mail: [redacted] Votre ordinateur sera débloqué dans les 24 heures suivantes.

Après le débloquage, nous suggérons que vous:

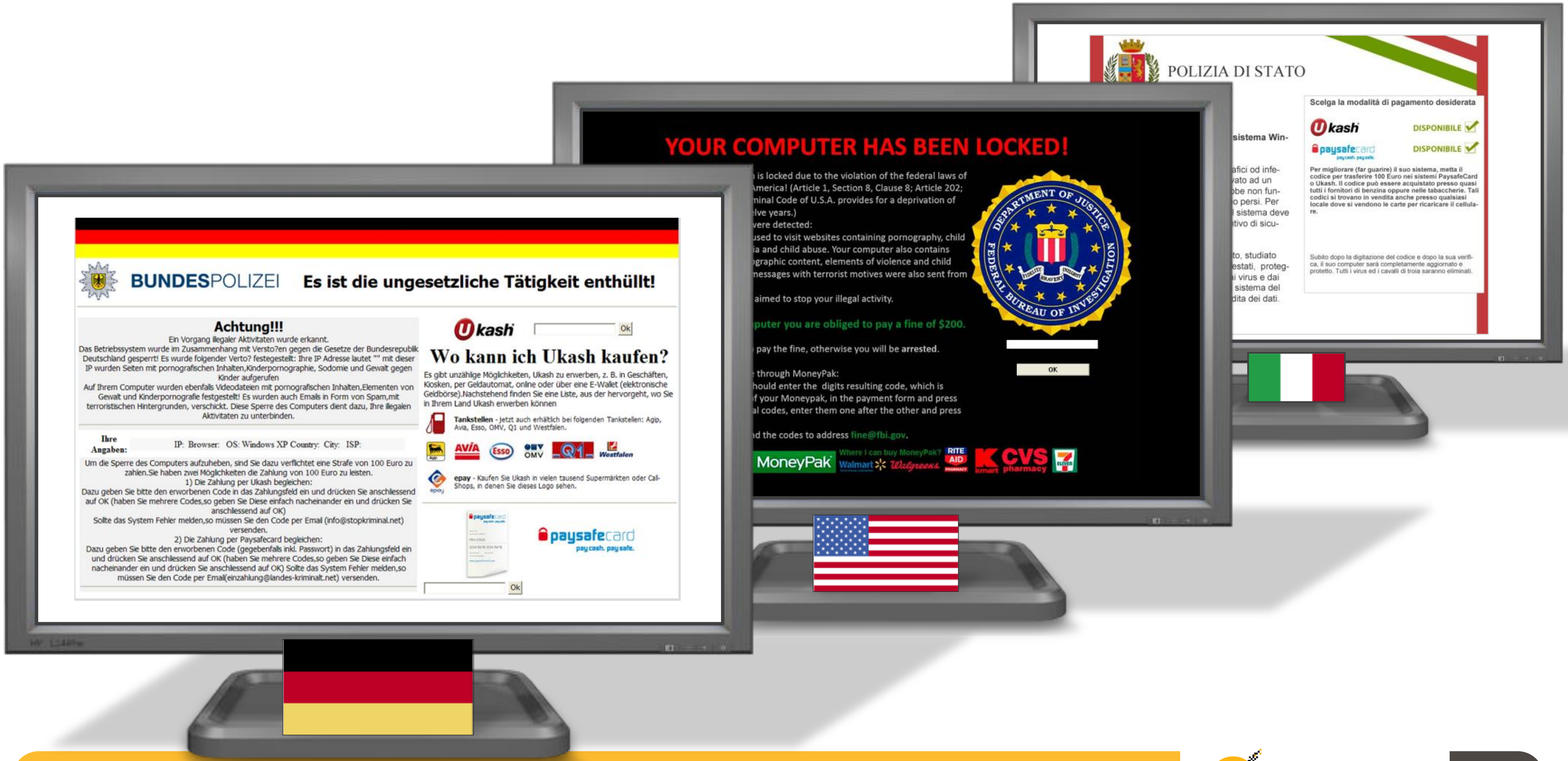
- Supprime toutes les fichiers multimédia en infraction avec les droits d'auteur.
- Supprime des logiciels en infraction avec les droits d'auteur.
- Installer un logiciel anti-virus, si vous n'en avez pas encore.
- Faire un scan anti-virus.

Votre SE:	[redacted]	**Votre FAI:**	[redacted]
Votre adresse IP:	[redacted]	**Votre ville:**	[redacted]

A GROWING MENACE Ransomware

Ransomware

- Blocks a user’s PC and demands money
- Usually masked as a legal police action



BUNDESPOLIZEI Es ist die ungesetzliche Tätigkeit enthüllt!

Achtung!!!

Ein Vorgang illegaler Aktivitaten wurde erkannt.
Das Betriebssystem wurde im Zusammenhang mit Versto?en gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verto? festegestelt: Ihre IP Adresse lautet "" mit dieser IP wurden Seiten mit pornografischen Inhalten,Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen
Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten,Elementen von Gewalt und Kinderpornografie festgestelt! Es wurden auch Emails in Form von Spam,mit terroristischen Hintergrunden, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitaten zu unterbinden.

Ihre Angaben: IP: Browser: OS: Windows XP Country: City: ISP:

Um die Sperre des Computers aufzuheben, sind Sie dazu verfichtet eine Strafe von 100 Euro zu zahlen.Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.
1) Die Zahlung per Ukash begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschlessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK)
Solte das System Fehler melden,so müssen Sie den Code per Email (info@stopkriminal.net) versenden.
2) Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK) Solte das System Fehler melden,so müssen Sie den Code per Email(einzahlung@landes-kriminalt.net) versenden.

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

YOUR COMPUTER HAS BEEN LOCKED!

is locked due to the violation of the federal laws of
America! (Article 1, Section 8, Clause 8; Article 202;
minal Code of U.S.A. provides for a deprivation of
lve years.)
vere detected:
used to visit websites containing pornography, child
ia and child abuse. Your computer also contains
graphic content, elements of violence and child
messages with terrorist motives were also sent from

aimed to stop your illegal activity.

puter you are obliged to pay a fine of $200.

pay the fine, otherwise you will be **arrested**.

through MoneyPak:
hould enter the digits resulting code, which is
f your Moneypak, in the payment form and press
al codes, enter them one after the other and press

d the codes to address fine@fbi.gov.

Where I can buy MoneyPak?

POLIZIA DI STATO

sistema Win-

afici od infe-
vato ad un
bbe non fun-
o persi. Per
l sistema deve
tivo di sicu-

to, studiato
estati, proteg-
i virus e dai
l sistema del
dita dei dati.

Scelga la modalità di pagamento desiderata

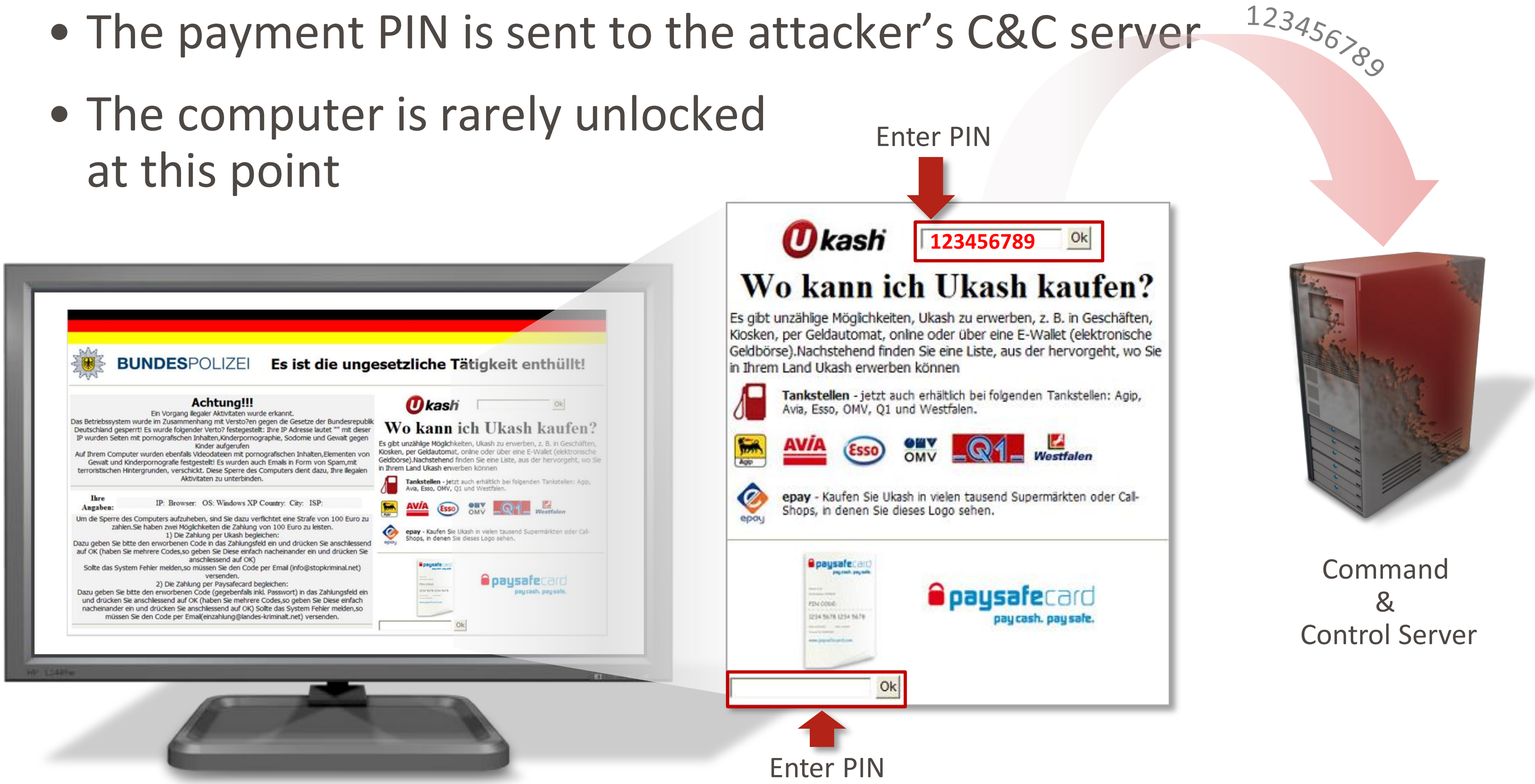
Ukash DISPONIBILE ✓
paysafecard DISPONIBILE ✓

Per migliorare (far guarire) il suo sistema, metta il codice per trasferire 100 Euro nei sistemi PaysafeCard o Ukash. Il codice può essere acquistato presso quasi tutti i fornitori di benzina oppure nelle tabaccherie. Tali codici si trovano in vendita anche presso qualsiasi locale dove si vendono le carte per ricaricare il cellulare.

Subito dopo la digitazione del codice e dopo la sua verifica, il suo computer sarà completamente aggiornato e protetto. Tutti i virus ed i cavalli di troia saranno eliminati.

Ransom Payment

- User needs to buy paysafe/UCash/MoneyPak for 50-200$
- The payment PIN is sent to the attacker’s C&C server
- The computer is rarely unlocked at this point



BUNDESPOLIZEI Es ist die ungesetzliche Tätigkeit enthüllt!

Achtung!!!

Ein Vorgang ilegaler Aktivitaten wurde erkannt.

Das Betriebssystem wurde im Zusammenhang mit Versto?en gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verto? festegestelt: Ihre IP Adresse lautet "" mit dieser IP wurden Seiten mit pornografischen Inhalten,Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen

Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten,Elementen von Gewalt und Kinderpornografie festgestellt! Es wurden auch Emails in Form von Spam,mit terroristischen Hintergrunden, verschickt. Diese Sperre des Computers dient dazu, Ihre ilegalen Aktivitaten zu unterbinden.

Ihre Angaben: IP: Browser: OS: Windows XP Country: City: ISP:

Um die Sperre des Computers aufzuheben, sind Sie dazu verfichtet eine Strafe von 100 Euro zu zahlen.Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten.

1) Die Zahlung per Ukash begleichen:

Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK)

Solte das System Fehler melden,so müssen Sie den Code per Email (info@stopkriminal.net) versenden.

2) Die Zahlung per Paysafecard begleichen:

Dazu geben Sie bitte den erworbenen Code (gegebenfalls inkl. Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK) Solte das System Fehler melden,so müssen Sie den Code per Email(einzahlung@landes-kriminalt.net) versenden.

Ukash 123456789 Ok

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

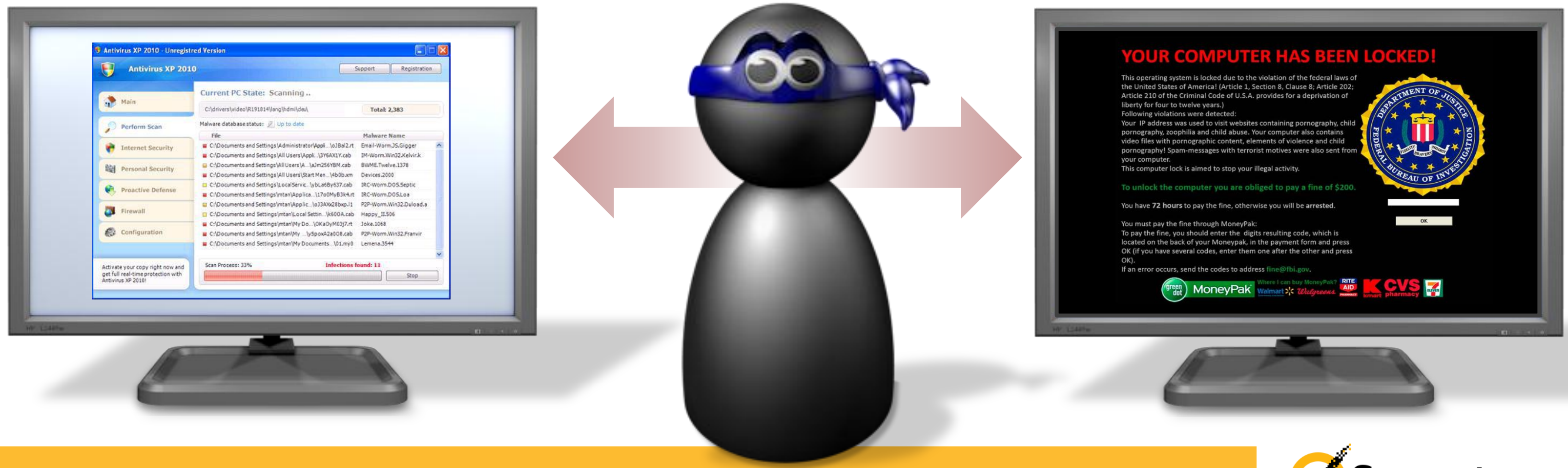
paysafecard pay cash. pay safe.

Ok

A GROWING MENACE Ransomware

Who’s Behind It?

- At least 16 separate gangs involved in the current campaigns
- Many of the gangs did also banking Trojans or Fake AV
- Some have earnings of over $500,000 per month
- In our analysis 2.9% of the users paid up



Current PC State: Scanning ..

C:\drivers\video\R191814\lang\hdmi\deu\ Total: 2,383

Malware database status: Up to date

File	Malware Name
C:\Documents and Settings\Administrator\Appli...\oJBal2.rt	Email-Worm.JS.Gigger
C:\Documents and Settings\All Users\Appl...\3Y6AX1Y.cab	IM-Worm.Win32.Kelvir.k
C:\Documents and Settings\All Users\A...\aJm256YBM.cab	BWME.Twelve.1378
C:\Documents and Settings\All Users\Start Men...\4b0b.xm	Devices.2000
C:\Documents and Settings\LocalServic...\ybLa6By637.cab	IRC-Worm.DOS.Septic
C:\Documents and Settings\mtan\Applica...\17o0MyB3k4.rt	IRC-Worm.DOS.Loa
C:\Documents and Settings\mtan\Applic...\oJ3AXx28bxp.l1	P2P-Worm.Win32.Duload.a
C:\Documents and Settings\mtan\Local Settin...\k600A.cab	Happy_II.506
C:\Documents and Settings\mtan\My Do...\0KaOyM03j7.rt	Joke.1068
C:\Documents and Settings\mtan\My ...\ySpoxA2a0O8.cab	P2P-Worm.Win32.Franvir
C:\Documents and Settings\mtan\My Documents...\01.my0	Lemena.3544

Scan Process: 33% Infections found: 11

Activate your copy right now and get full real-time protection with Antivirus XP 2010!

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Smartphones

I bet you know someone who once lost his phone with important data on it!

Top mobile threats

Web- & Network-based Attacks

Launched by malicious websites or compromised legitimate sites

Attacking site exploits device's browser

Attempts to install malware or steal confidential data that flows through browser

Malware

Includes traditional computer viruses, computer worms and Trojan horse programs

Example: Ikee worm targeted iOS-based devices

Example: Pjapps enrolled infected Android devices in botnet

Social Engineering Attacks

Leverage social engineering to trick users

Attempts to get users to disclose sensitive info or install malware

Examples include phishing and targeted attacks

Resource Abuse

Attempt to misuse network, device or identity resources

Example: Sending spam from compromised devices

Example: Denial of service attacks using computing resources of compromised devices

Data Loss

Employee or hacker exfiltrates sensitive info from device or network

Can be unintentional or malicious

Remains biggest threat to mobile devices

Data Integrity Threats

Attempts to corrupt or modify data

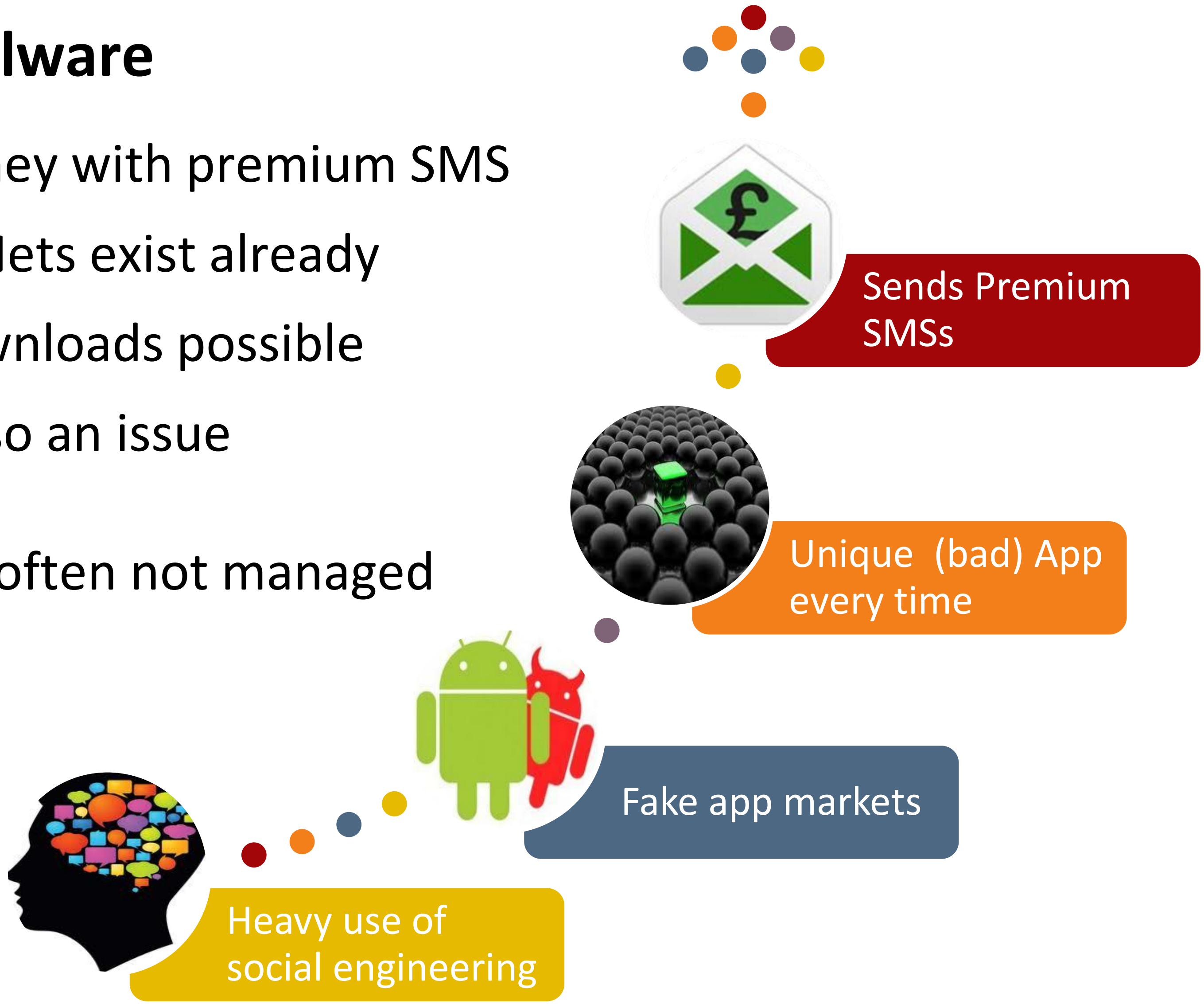
Purpose is to disrupt operations of an enterprise or for financial gain

Can also occur unintentionally

Android Malware

- Making money with premium SMS
- Mobile BotNets exist already
- DriveBy Downloads possible
- Privacy is also an issue

- Devices are often not managed



Sends Premium SMSs

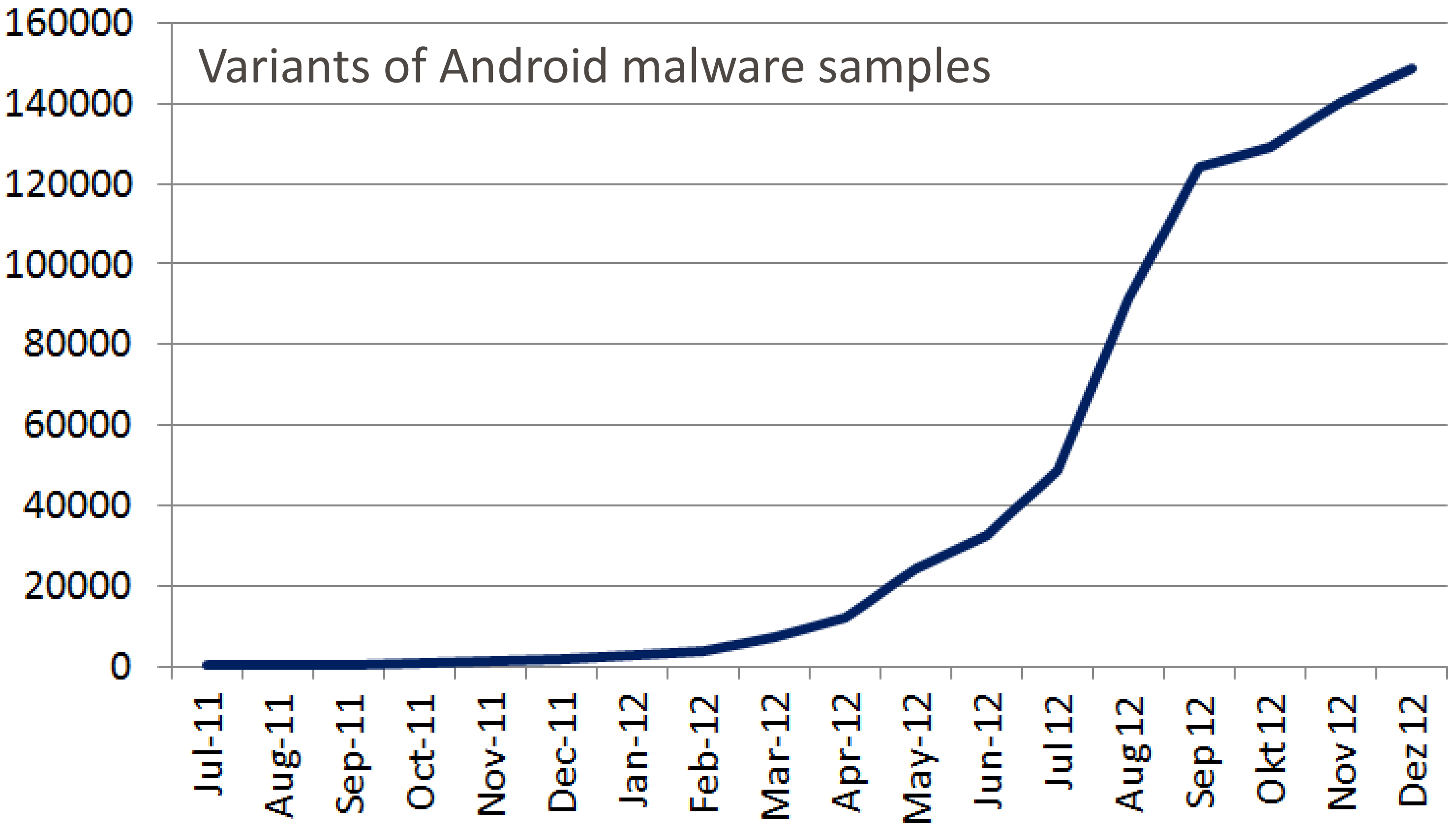
Unique (bad) App every time

Fake app markets

Heavy use of social engineering

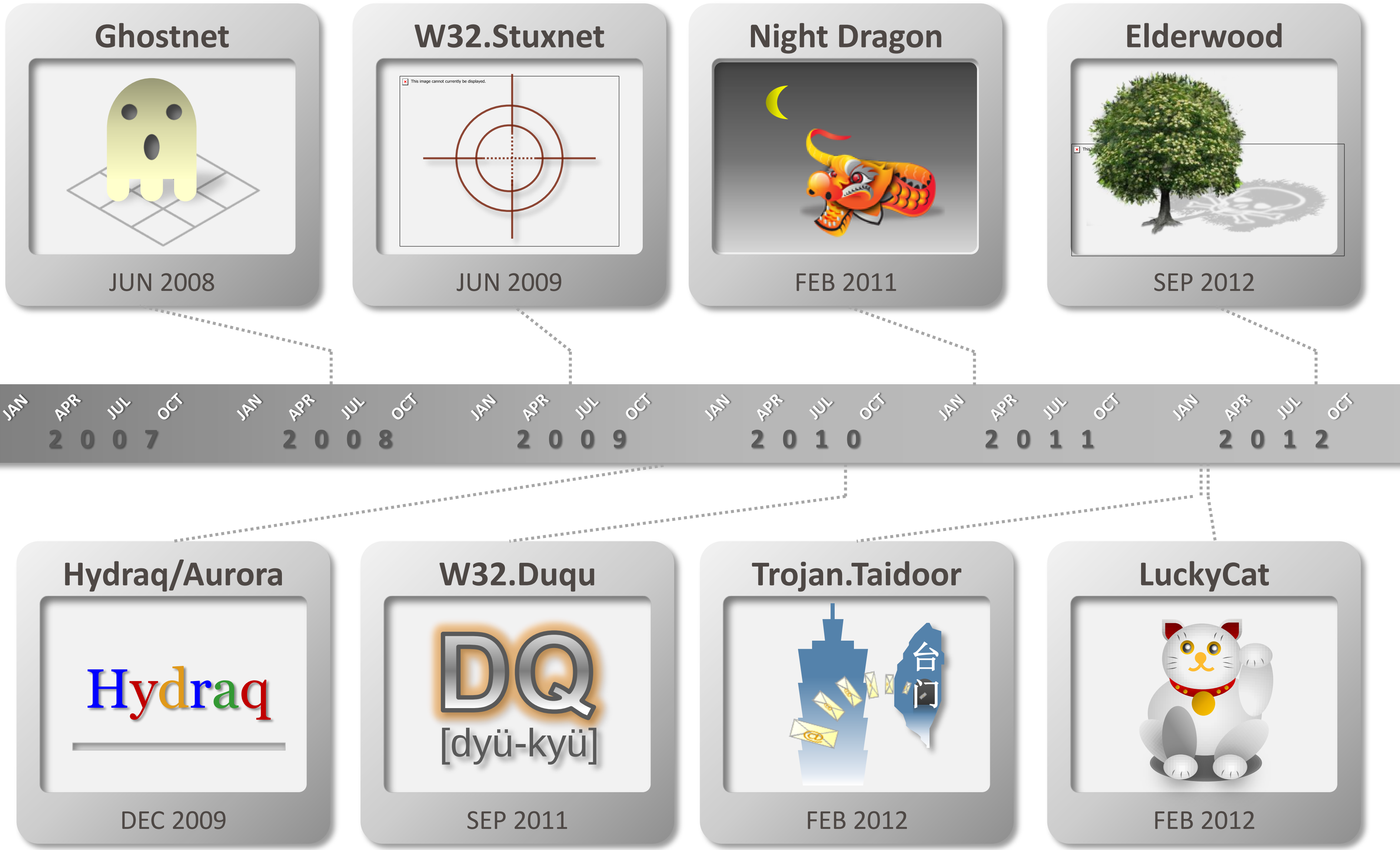
Android Malware statistics

- 224 Android malware families in December 2012
- 150‘000 different sample variants



Where is your critical data and who can access it?

Examples of targeted attacks



Ghostnet
JUN 2008

W32.Stuxnet
JUN 2009

Night Dragon
FEB 2011

Elderwood
SEP 2012

Hydraq/Aurora
DEC 2009

W32.Duqu
SEP 2011

Trojan.Taidoor
FEB 2012

LuckyCat
FEB 2012

Symantec.

Information Theft

Types of Info

- Designs
- Business Plans
- Financial Info
- Personnel Info

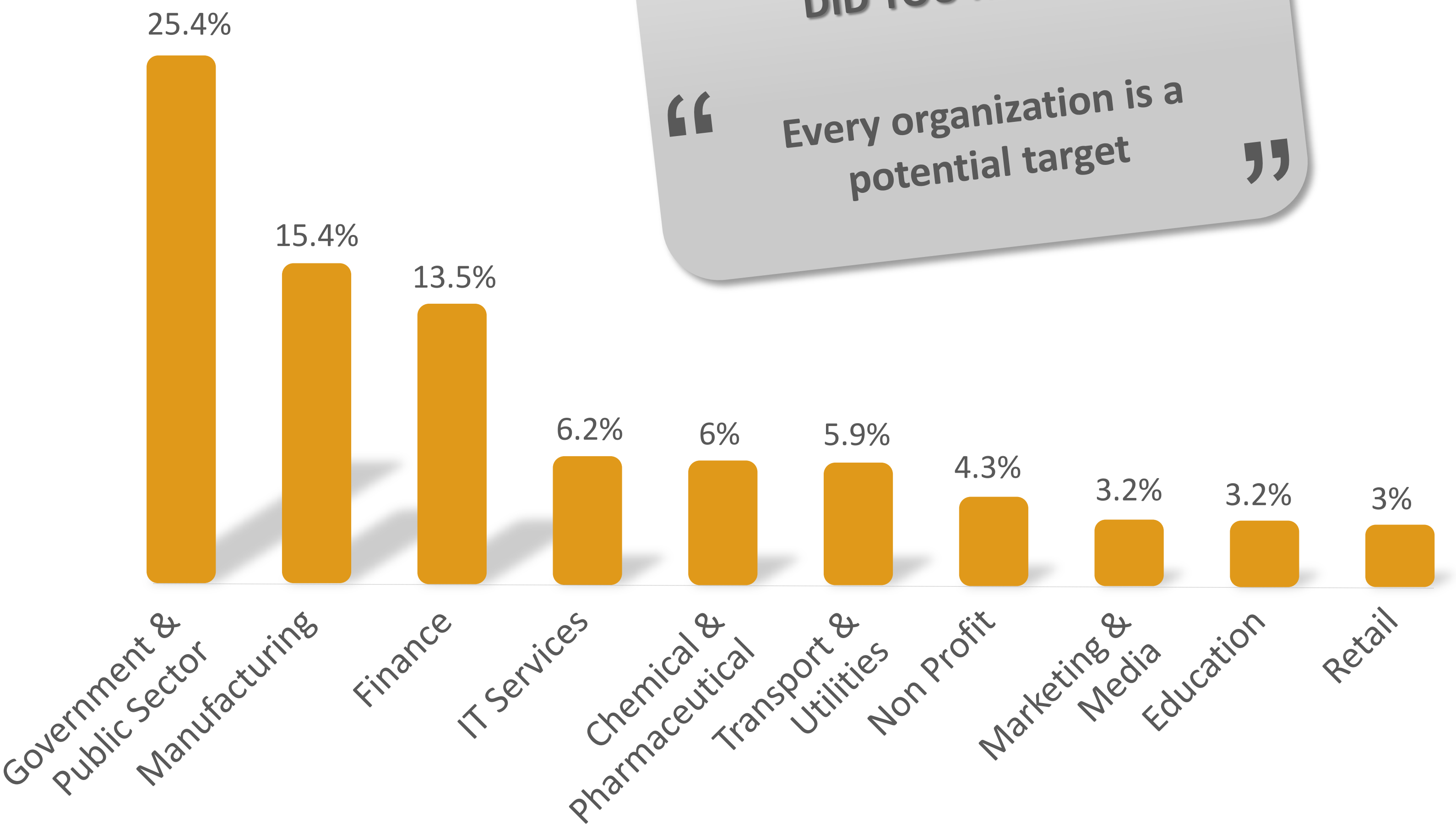
Information is

source of wealth
&
power

Information is

a key asset of
any organization

Top 10 sectors of targeted attacks

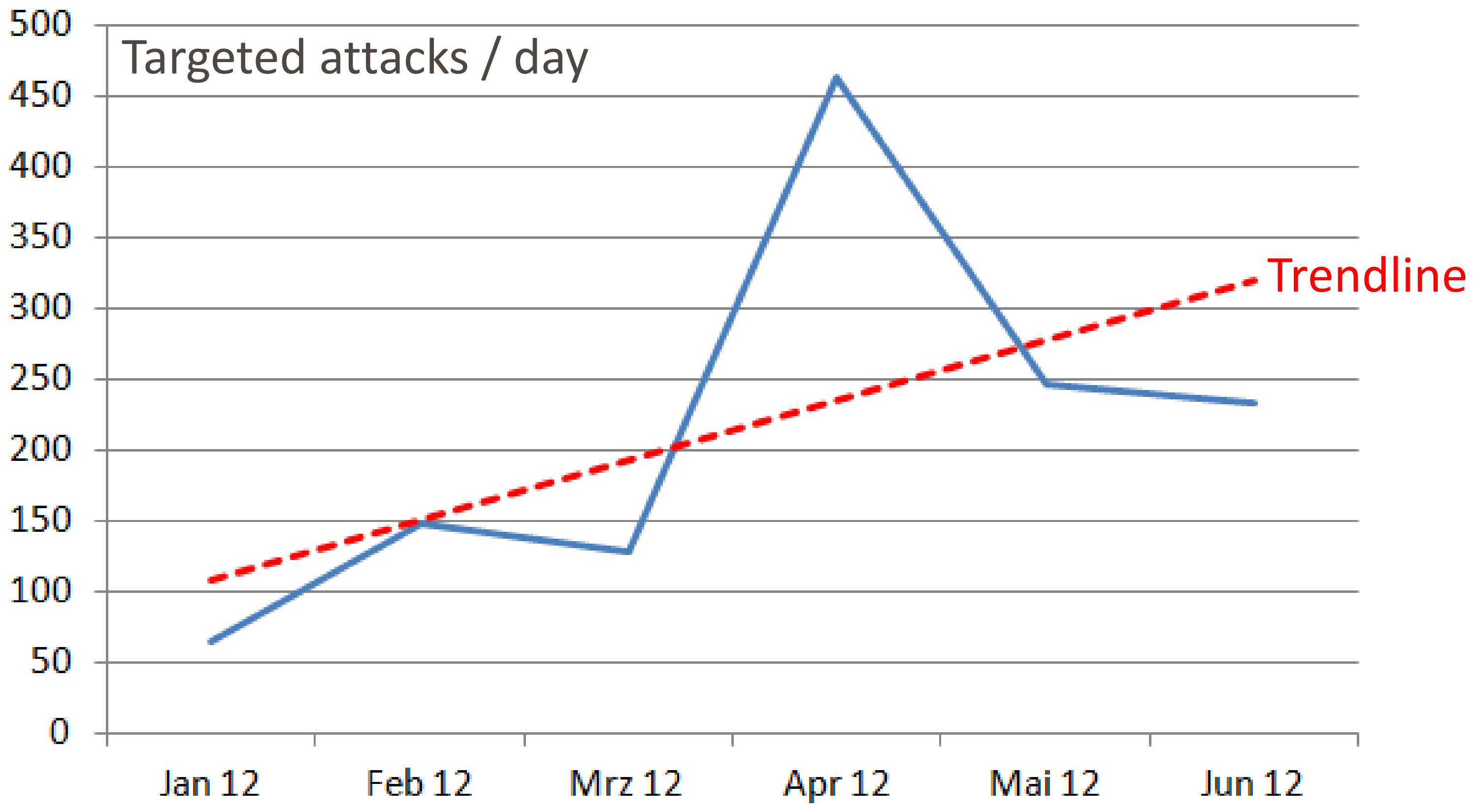


DID YOU KNOW?

“ Every organization is a potential target ”

Targeted attacks do happen daily

- Small business often targeted, because not well protected, but connected to others



How Are The Attacks Carried Out?

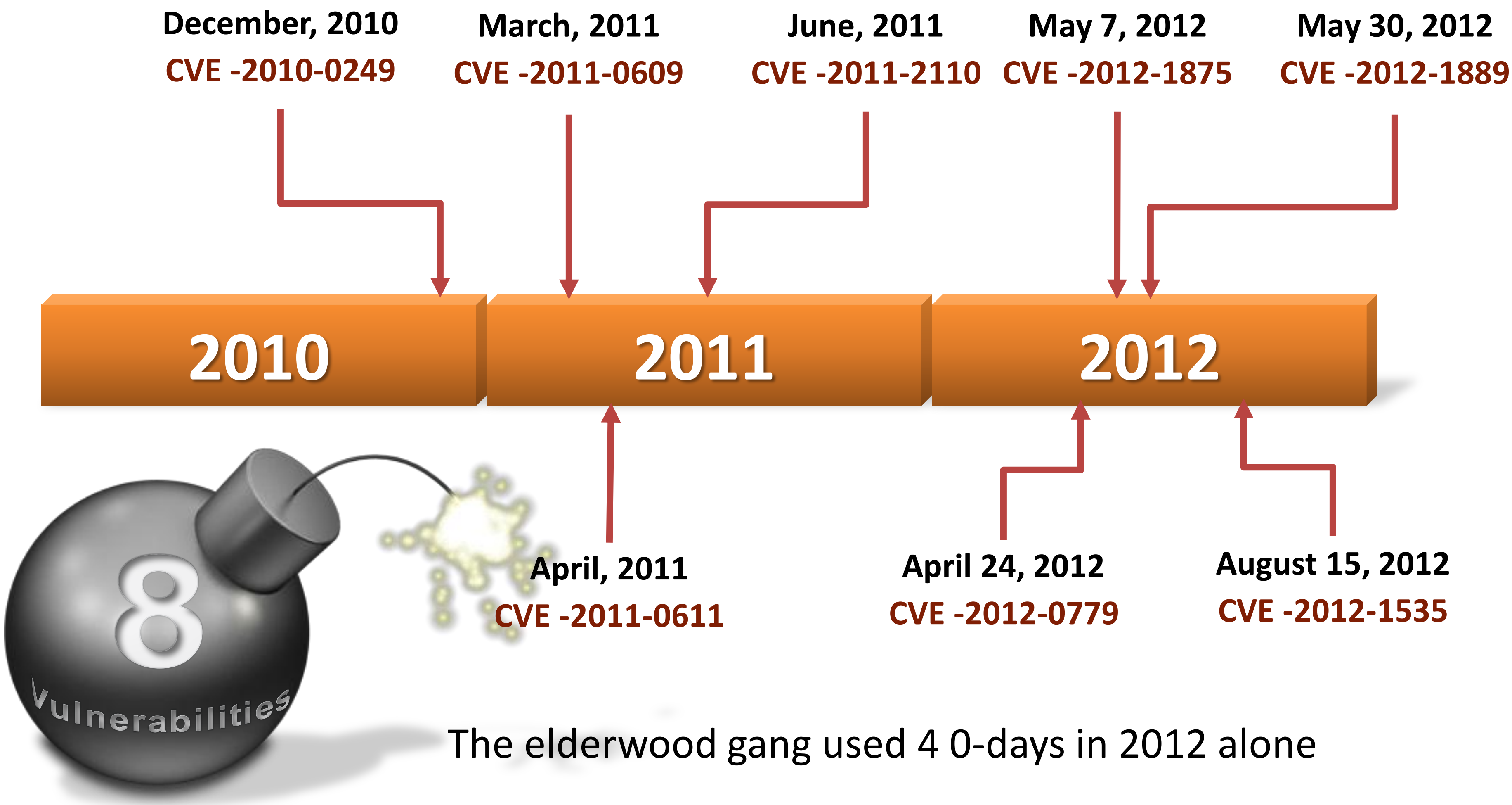
Spear Phishing

Send an email to a person of interest

Watering Hole Attack

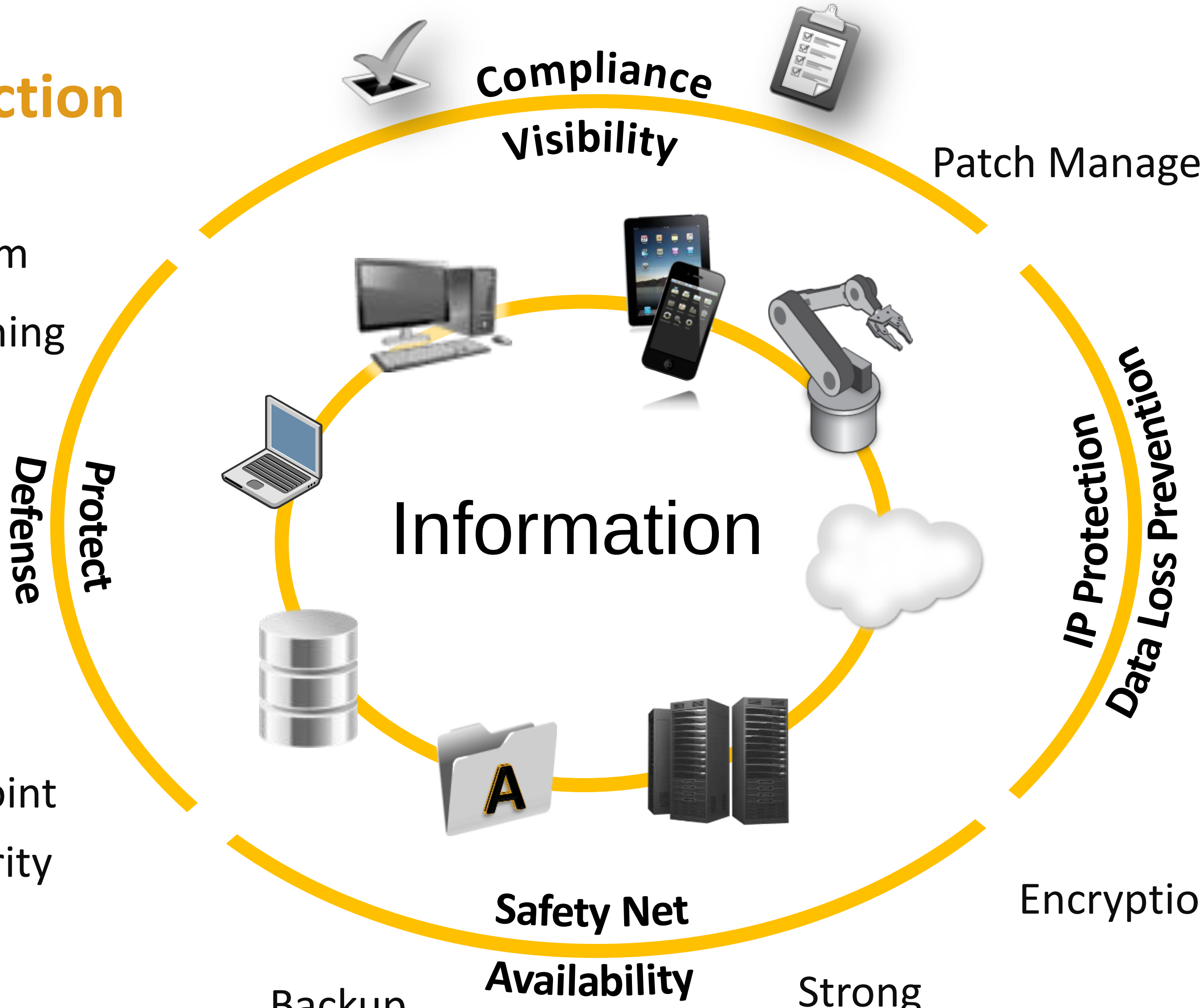
Infect a website of interest to your target user base and lie in wait for them

Some groups do have many 0-days & large resources



The elderwood gang used 4 0-days in 2012 alone

Protection



Compliance

Visibility

Patch Management

System

Hardening

Protect

Defense

Information

IP Protection

Data Loss Prevention

DLP

Endpoint

Security

Safety Net

Availability

Backup

Strong
Authentication

Encryption

Q&A

Merci de votre attention!

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.