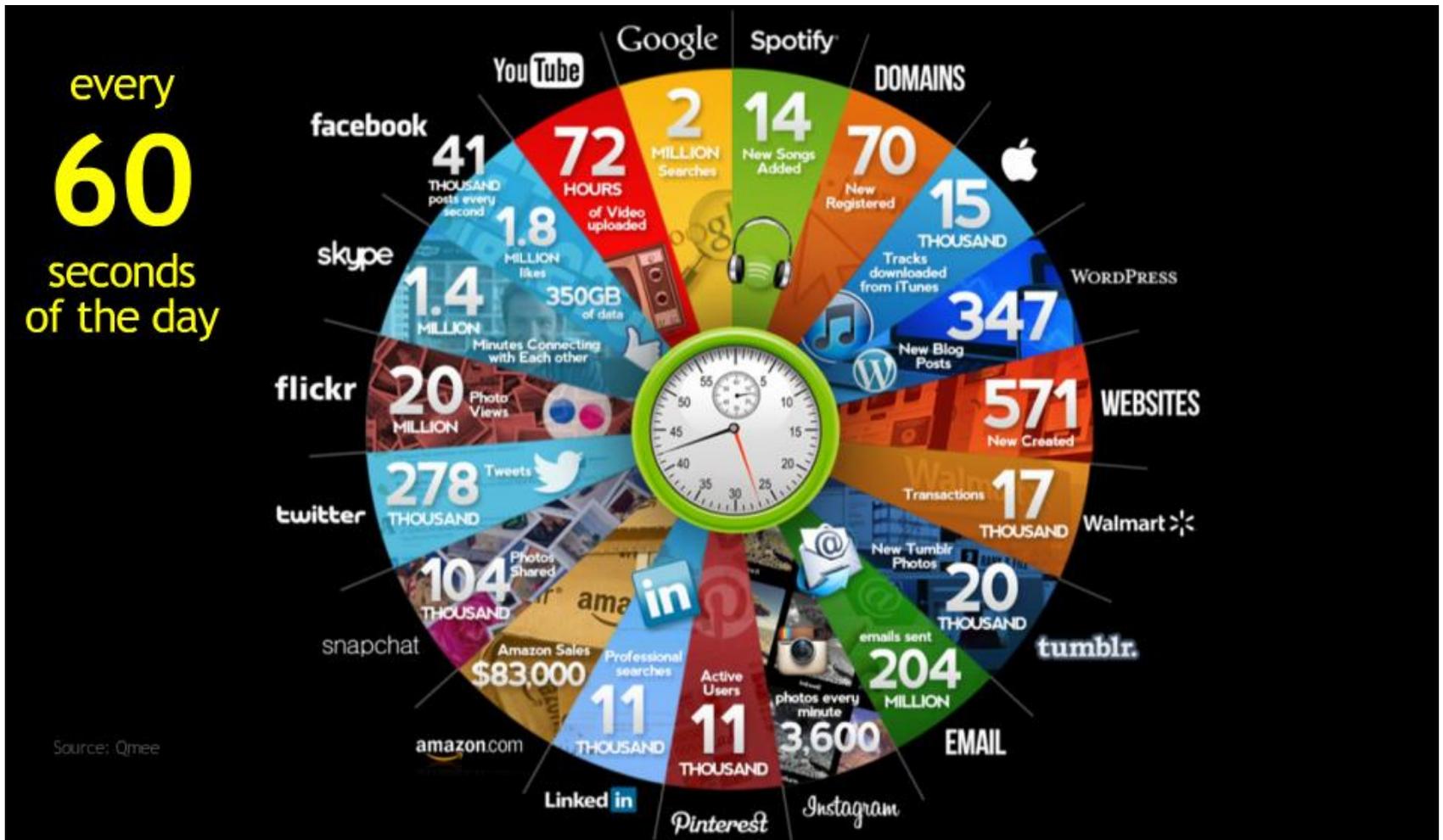


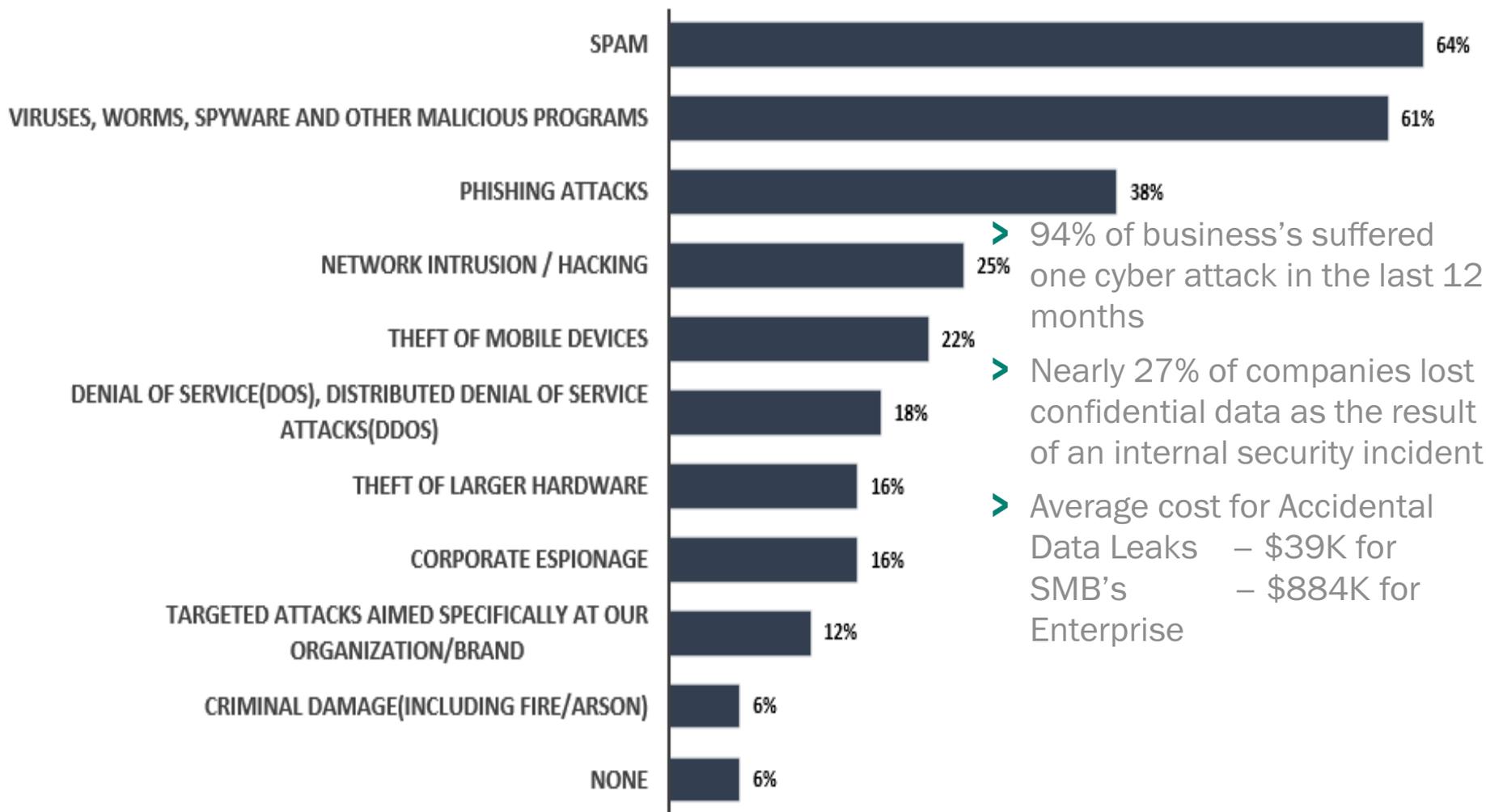
# THE EXPLOSION OF CYBERCRIME- THE 5 WAYS IT MAY BE AN ACCOMPLICE

Mark Villinski  
Kaspersky Lab  
[@markvillinski](mailto:@markvillinski)

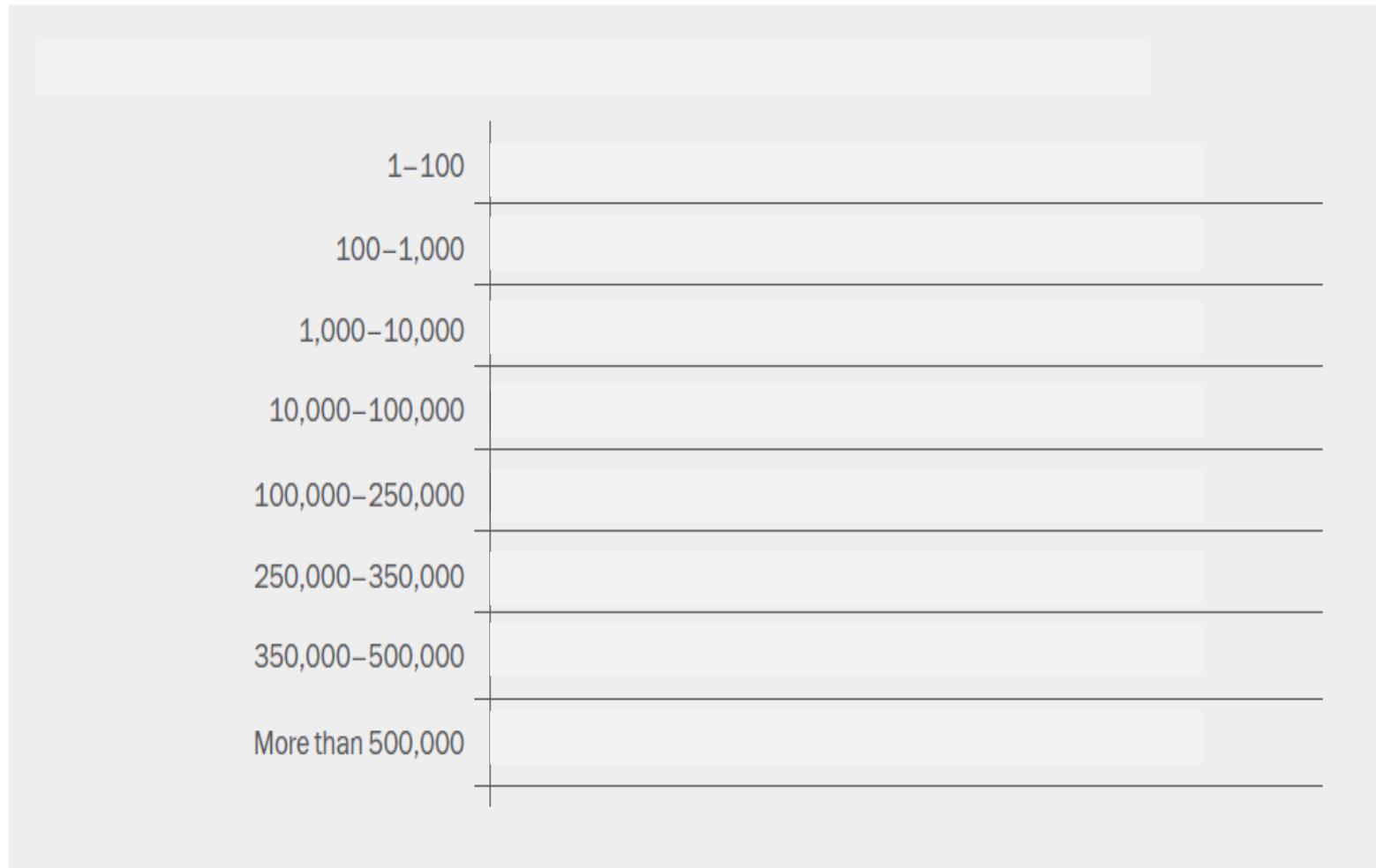
# ALL THIS IS DONE EVERY 60 SECONDS ON THE INTERNET



# 2014 CORPORATE THREATS SURVEY

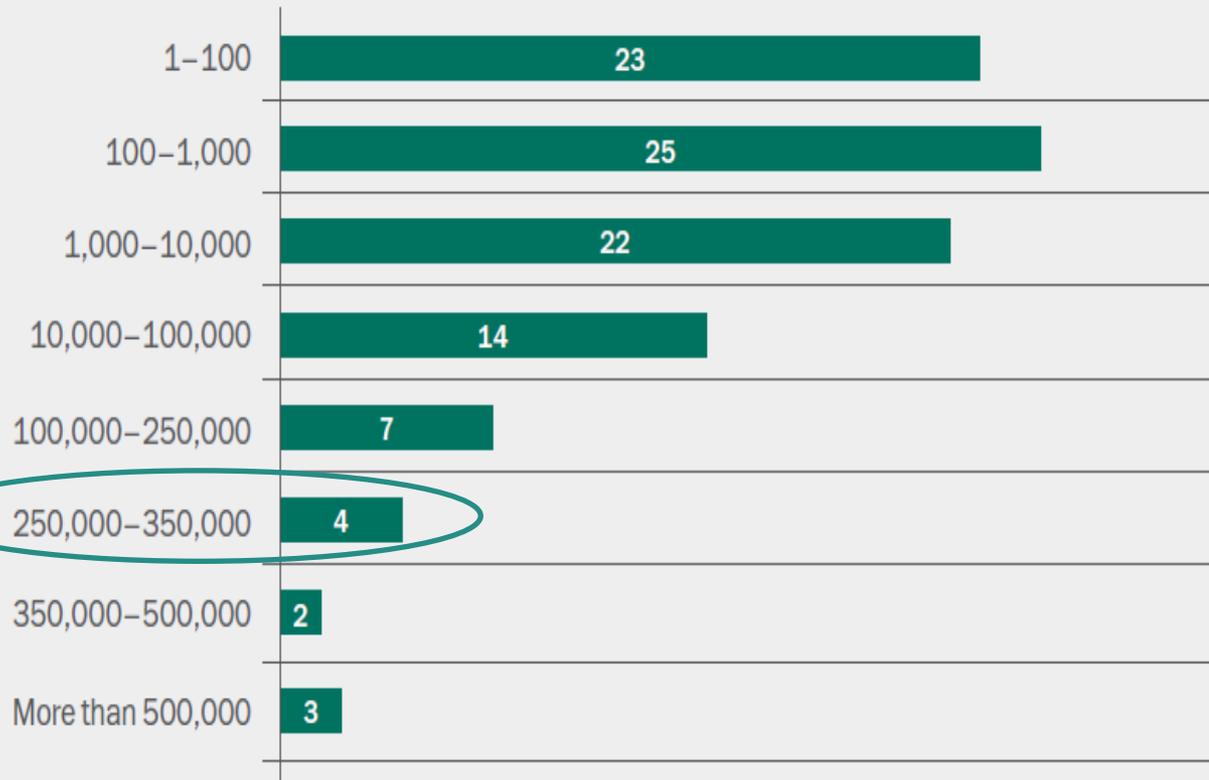


# QUICK POLL



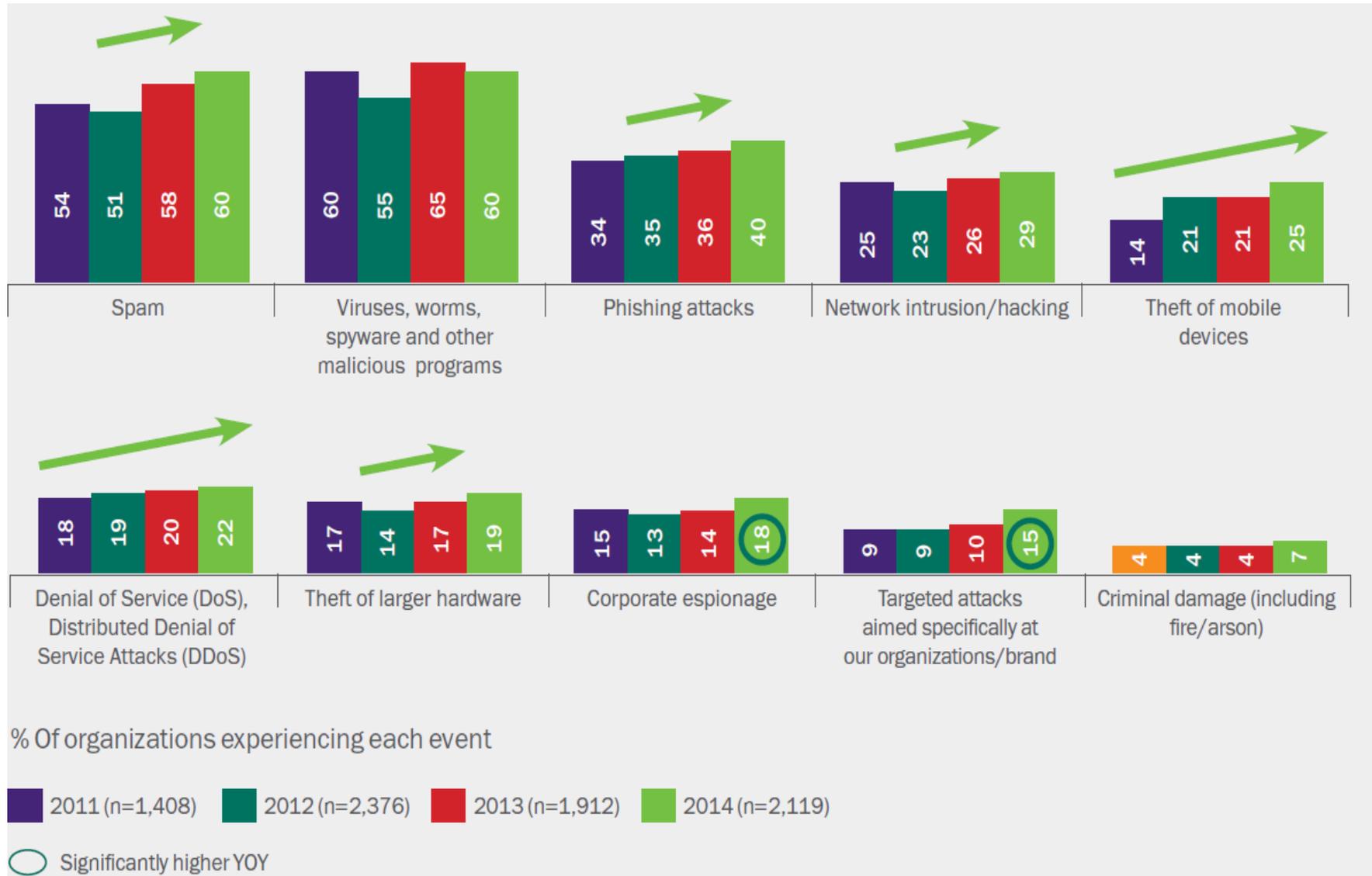
# PERCEPTION VS. REALITY

## Perceived Number Of New Malware Samples Discovered Daily (%)



REALITY TODAY

# EXTERNAL THREATS EXPERIENCED



# THE MOST SERIOUS THREATS



B2B International and Kaspersky Lab, "IT Security Threats and Data Breaches," October, 2014.

Base: Varies All Respondents Of Each Size Who Lost Data

# HOW BAD IS IT OUT THERE?

c|net

Search CNET



Reviews

News

## Today's computers face more attacks than ever

More malicious software has been created in the past 2 years than in the previous 10 years combined.

by [Seth Rosenblatt](#) @sethr / January 9, 2015 3:23 PM PST

38 / 80 / 533 / 148 / / more +

Nestled into a storefront at the top of San Francisco's tree-lined Valencia Street is one of the city's top defenses in the war against malicious-software infections: a computer repair shop owned by Del Jaljaa.

People bring their infected computers to [Jaljaa's San Francisco Computer Repair store](#) 5 to 10 times a day, desperate for help restoring their



# 2014 REVIEW

- Kaspersky products detected and neutralized a total of **6,167,233,068** threats
- Kaspersky solutions blocked 1,363,549 attacks on Android-based devices.
- Kaspersky solutions repelled 1,432,660,467 attacks launched from online resources
- To carry out their attacks, cybercriminals used 9,766,119 unique hosts.
- 38% of user computers were subjected to at least one web attack over the year.
- A total of 1,910,520 attempts to launch banking malware on user computers were neutralized
- Kaspersky web antivirus detected **123,054,503** unique malicious objects: scripts, exploits, executable files, etc.
- Kaspersky antivirus solutions detected a total of **1,849,949** unique malicious and potentially unwanted objects.

# ORIGINAL CORPORATE SECURITY PERIMETER



# TODAY'S SECURITY PERIMETER



“Most organizational management and security teams understand what phishing is. The problem is they do not know how, or do not have the time and resources, to teach people what phishing is and how to detect or defend against it.”

LANCE SPITZNER, SANS INSTITUTE

# PHISHING ATTACKS

From:  American Airlines <verification@thebestdentalchair.com>  
To:  Mark Villinski  
Cc:  
Subject: Your order is ready

Message AA-0069557964.zip (57 KB)

This is your e-ticket receipt.

TICKET TYPE / TICKET NUMBER / AA-0031056340

SEAT / 40F/ZONE 2

DATE / TIME 29 JANUARY, 2014, 12:15 AM

ARRIVING / Raleigh

ST / OK

REF / EF.6260 BAG / 5PC

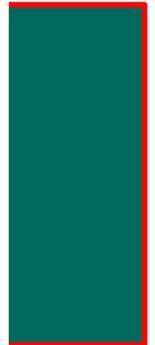
TOTAL PRICE / 559.83 USD

FORM OF PAYMENT / CC

Your ticket is attached.

You can print your e-ticket.

Yours sincerely,  
AA E-Ticket services.



# KASPERSKY LAB ANALYSIS REPORT

## THE EVOLUTION OF PHISHING ATTACKS:

2011-2013

KASPERSKY  
LAB

- ▶ In 2012-2013, 37.3 million users around the world were subjected to phishing attacks, up 87% from 2011-2012
- ▶ The number of distinct sources of attacks in 2012 and 2013 increased 3.3 times (+330%)

Most targeted: Social, Search, Banks

Others

49.07%

Yahoo!

9.85%

Banks

20.64%

Facebook

9.69%

Amazon

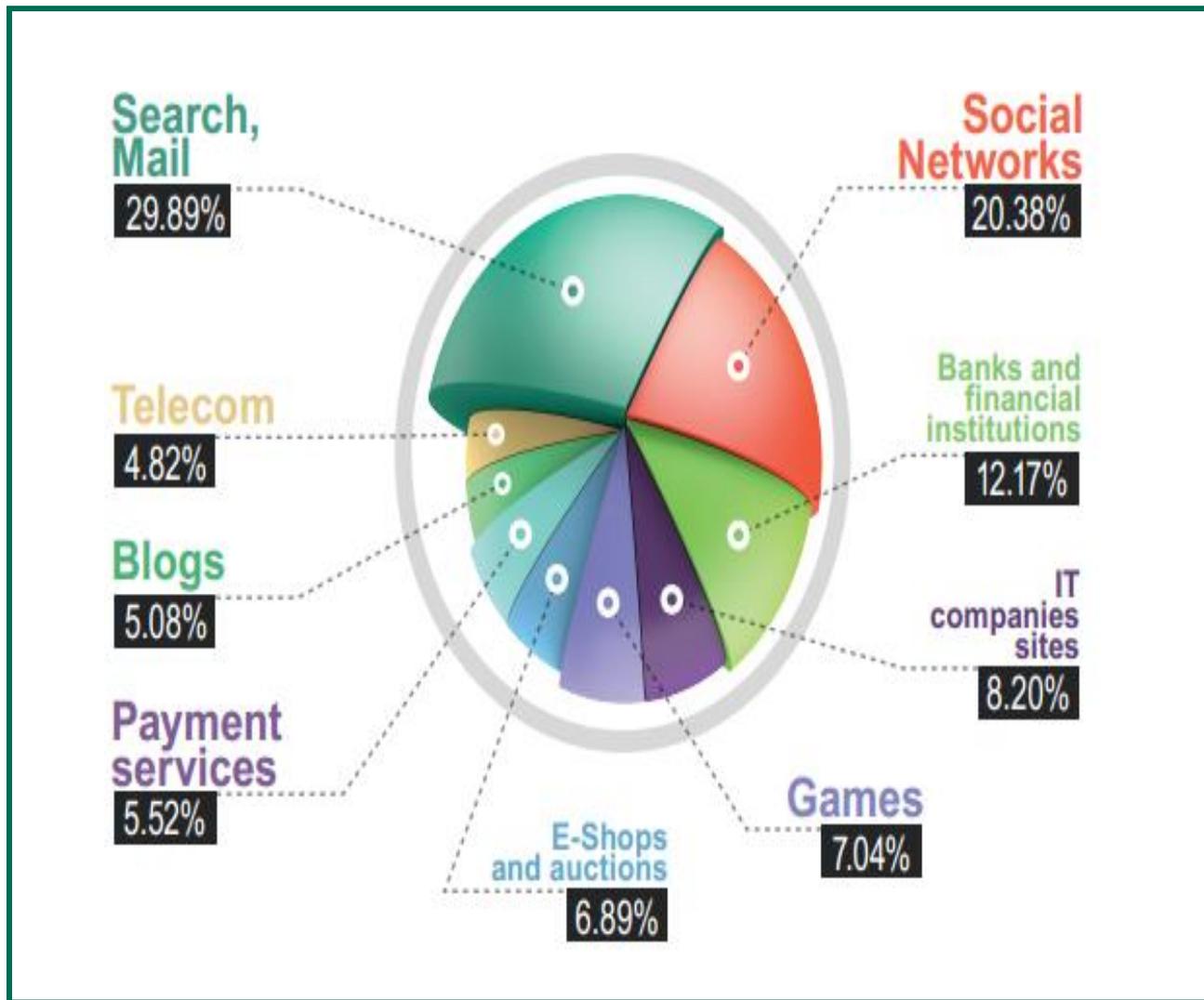
3.86%

Google

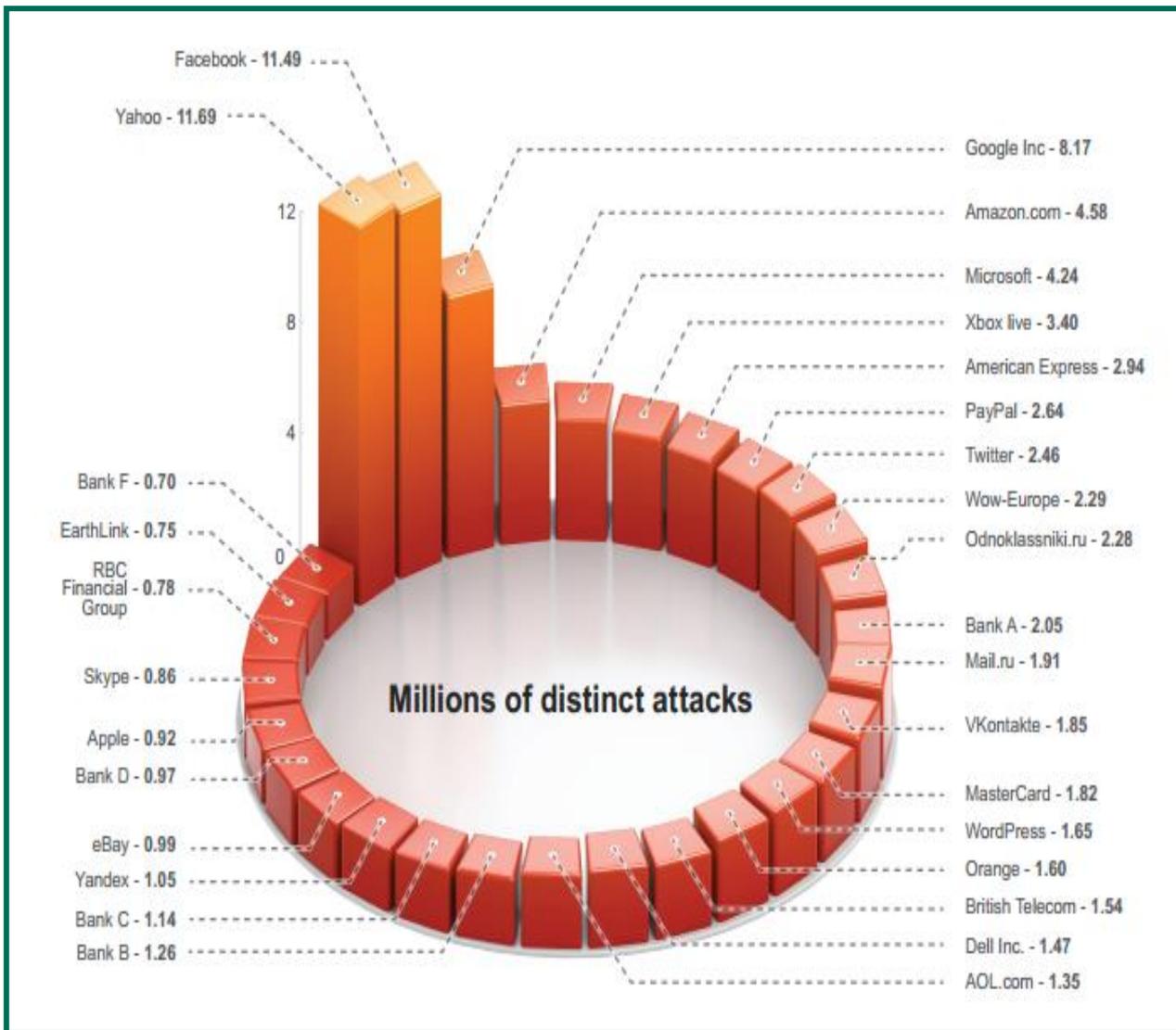
6.89%

- ▶ 102,100 Internet users around the world were subjected to phishing attacks daily!

# PHISHING SITES BY CATEGORY



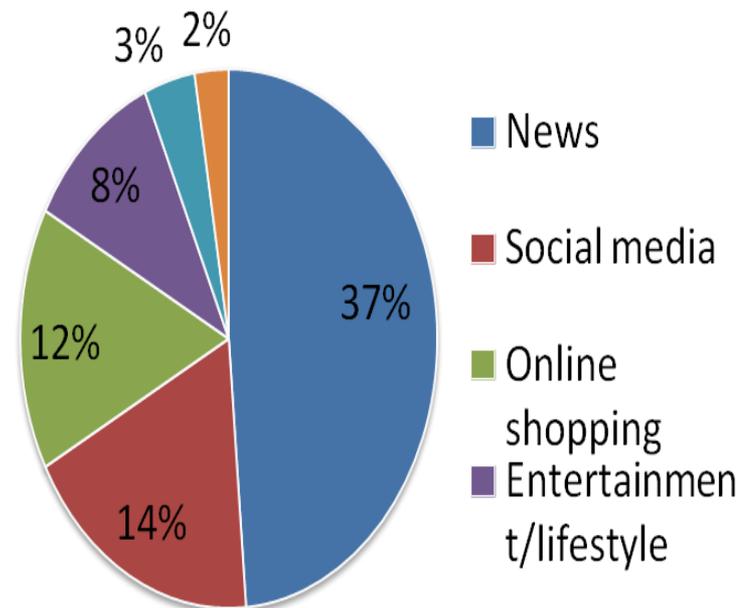
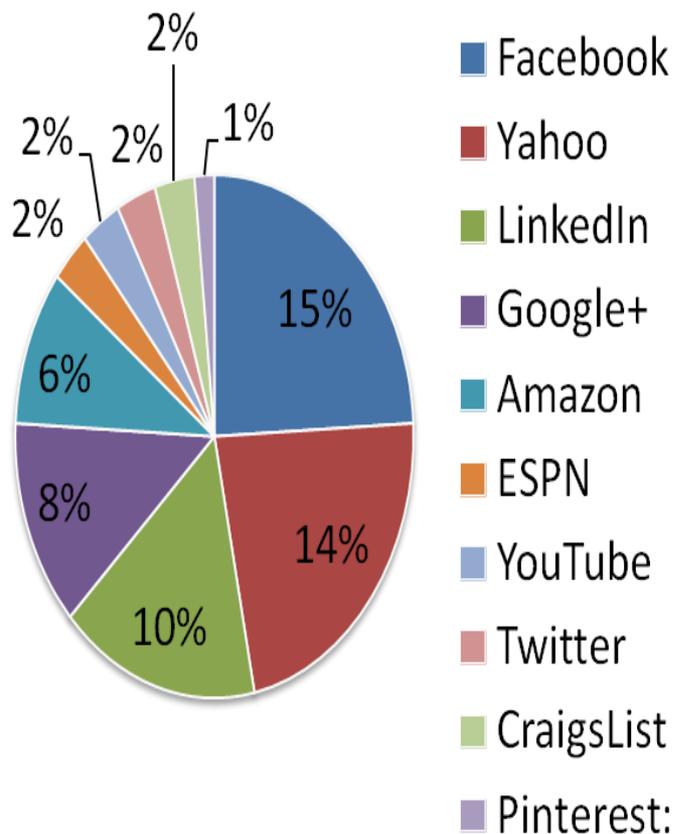
# TOP 30 PHISHING TARGETED SITES 2012-2013



 USA	
1	Yahoo!
2	Facebook
3	Google Inc
4	Amazon.com: Online Shopping
5	Wow-Europe
6	Microsoft Corporation
7	AOL.com
8	American Express
9	Bank A
10	Twitter

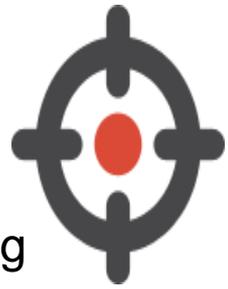
# CORPORATE EMPLOYEE ACTIVITIES

- ▶ 69% of U.S. employees spend at least 30 minutes on personal activities during business hours
- ▶ 34% of those employees spend their time online, most commonly on:



SOURCE: Salary.com's 2013 Wasting Time at Work Survey: <http://www.salary.com/2013-wasting-time-at-work-survey/>

# SPEAR-PHISHING & TARGETED ATTACKS



- ▶ Spear-phishing emails is one of the most common methods for infecting valuable targets in corporations, often used in targeted attacks
- ▶ Highly customized, it now combines social engineering and common system vulnerabilities to breach defenses
- ▶ In the past 12 months, 91% of the companies surveyed had at least one external IT security incident and 85% reported internal incidents.
- ▶ A large enterprise breach in North America was calculated at an average of \$818,000 per incident
- ▶ For small to medium size businesses, the average cost was \$82,000 per incident

SOURCE: GLOBAL IT SECURITY RISKS SURVEY 2013

# RSA: TARGETED ATTACK CASE STUDY

- ▶ On March 17th 2011, RSA announced that it was hacked
- ▶ During the 2011 Kaspersky Security Analyst Summit, Uri Rivner from RSA talked about how it happened:
  - ▶ Two employees received an e-mail which contained a spreadsheet attachment labeled “2011 Recruitment Plan”.
  - ▶ The e-mail has been marked as SPAM and put into the spam folder
  - ▶ One of the employees opened it...and released a zero-day Adobe Flash vulnerability.



# RSA E-MAIL & ATTACHMENT

The image shows two overlapping windows. The left window is an email client displaying a message titled "2011 Recruitment plan - Message (HTML)". The message header includes:

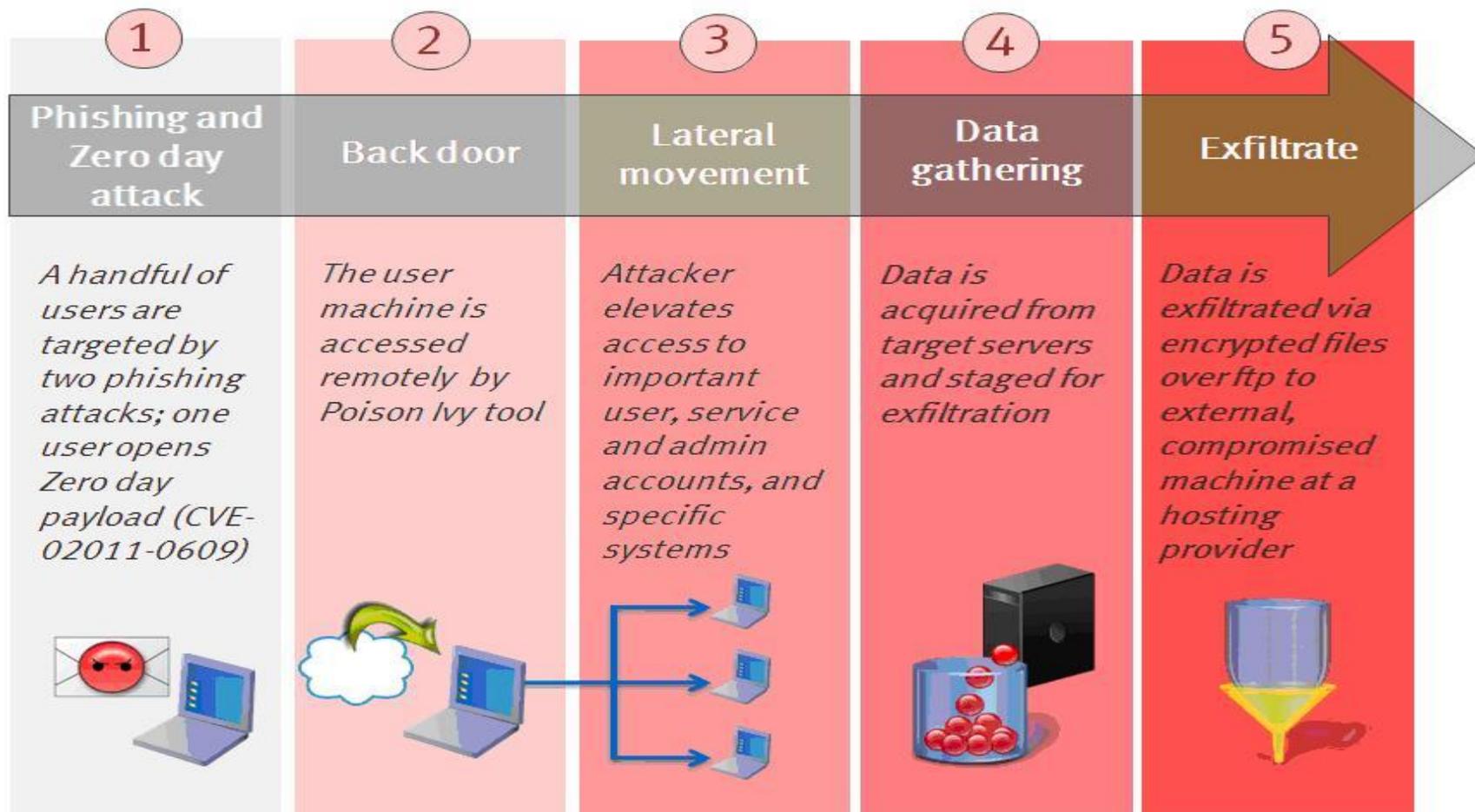
From: web master [webmaster@beyond.com] Sent: to 3.3.2011 18:48  
To: [redacted]@emc.com  
Cc: [redacted]  
Subject: 2011 Recruitment plan

The email body contains the text: "I forward this file to you for review. Please open and view it." Below the text is a message icon and an attachment icon for "2011 Recruitment plan.xls".

The right window is Microsoft Excel, titled "Microsoft Excel - 2011 Recruitment plan.xls [Compatibility Mode]". The ribbon shows the "Home" tab with various options like Cut, Copy, Paste, Format Painter, Font, Alignment, and Number. The active cell is A1, and the formula bar shows a formula. The spreadsheet grid is visible, with a checkmark in cell B1.

# THE BLUEPRINT

## How does this happen?



# PHISHING AT ABC UNIVERSITY



## IC3 PUBLIC SERVICE ANNOUNCEMENT

FEDERAL BUREAU OF INVESTIGATION

**13 January 2015**

Alert Number  
**I-011315b-PSA**

### UNIVERSITY EMPLOYEE PAYROLL SCAM

University employees are receiving fraudulent e-mails indicating a change in their human resource status. The e-mail contains a link directing the employee to login to their human resources website to identify this change. The website provided appears very similar to the legitimate site in an effort to steal the employee's credentials. Once the employee enters his/her login information, the scammer takes that information and signs into the employee's official human resources account to change the employee's direct deposit information. This redirects the employee's paycheck to the bank account of another individual involved in the scam.

#### Consequences of this Scam:

- The employee's paycheck can be stolen.
- The money may not be returned in full to the employee.
- The scammers can take the employee's log-in credentials and attempt to log into other accounts that belong to the employee.

#### Tips on how to Protect Yourself from this Scam:

- Look for poor use of the English language in e-mails such as incorrect grammar, capitalization, and tenses. Many of the scammers who send these messages are not native English speakers.
- Roll your cursor over the links received via e-mail and look for inconsistencies. If it is not the website the e-mail claims to be directing you to then the link is to a fraudulent site.

# HOW DID THIS HAPPEN?

- Trickery. A spear-phishing attack.
  - People were tricked by a believable e-mail message into giving their passwords to the bad guys
- Spear-phishers and their tactics
  - Message crafted for ABC University
  - Sent to a small number of selected people
  - Strike on weekends & holidays, when you are less protected
- Goals
  - To collect information that will let them steal money:
  - Passwords, social security numbers, bank account or credit card numbers



Dear ABC University Employee,

Our new intrusion monitoring system that checkmates the increased incidents of phishing attacks and database compromise detected that your "ABC University" account was accessed from a blacklisted IP located in Arizona. Here are the details:

IP: 23.19.88.141

Registered to: Nobis Technology Group, LLC. Phoenix, Arizona

Time of compromise: 8:17 AM, Eastern Standard Time (EST) -0500 UTC

Date of compromise: Saturday, November 30, 2013

Did you access your account from this location? If this wasn't you, your computer might have been infected by malicious software. To protect your account from any further compromise, kindly follow these two steps immediately:

1. Follow this ITS secure link below to reconfirm your login details and allow the new IP monitoring alert system automatically block the suspicious IP (23.19.88.141) from further future compromise

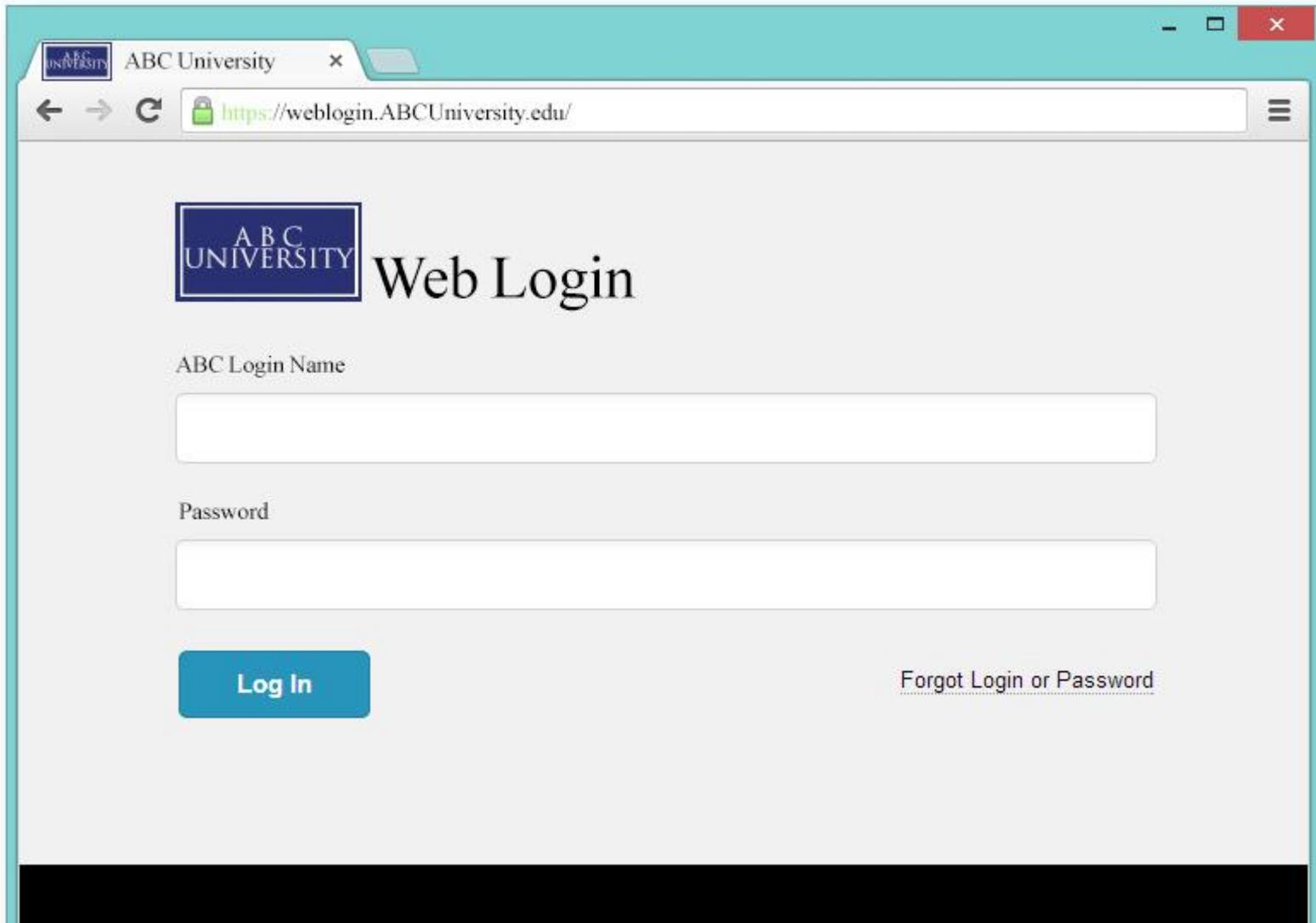
<http://ABCUniversity.edu/blockIP&malware>

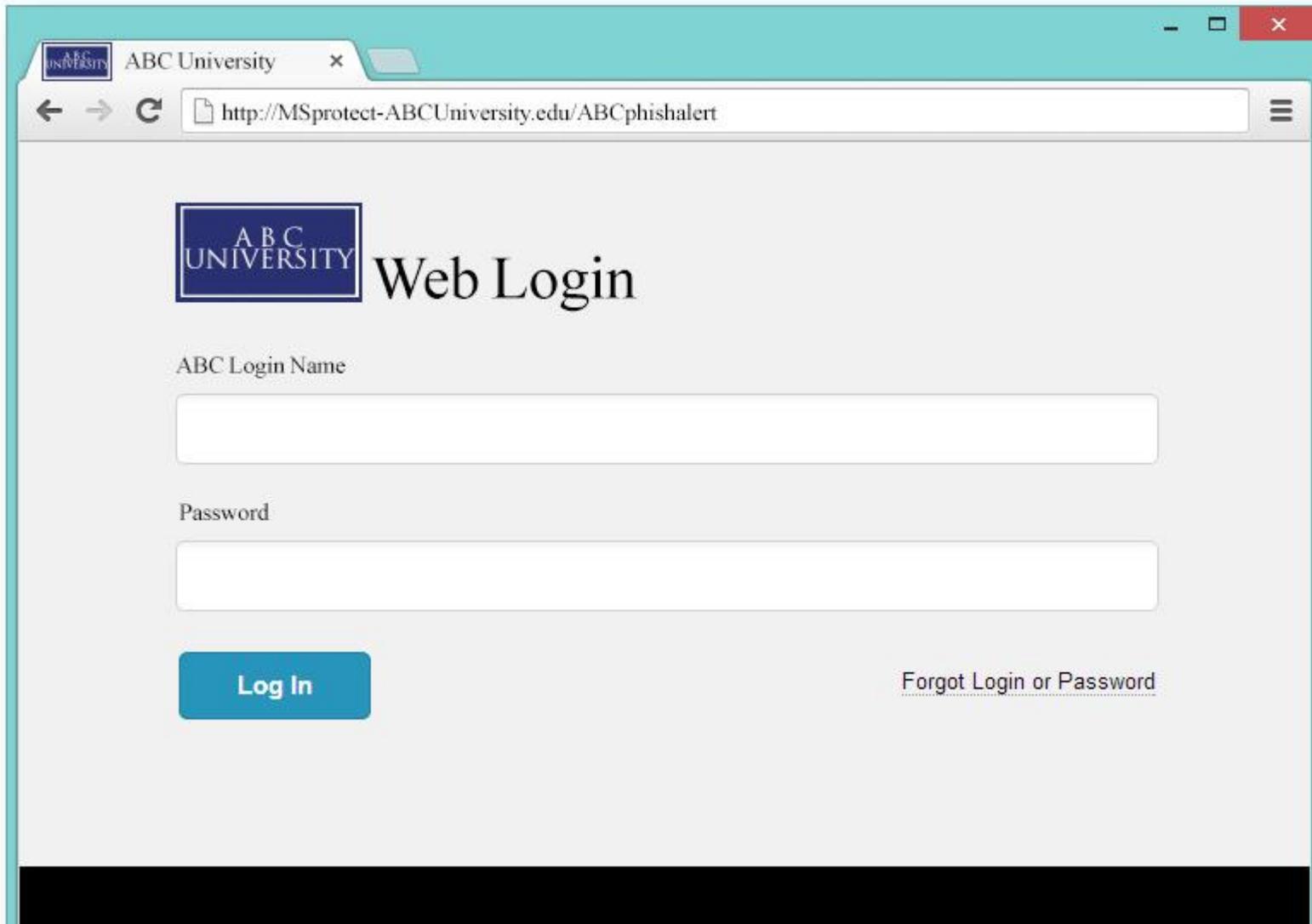
2. Update your anti-malware software and scan your PC immediately

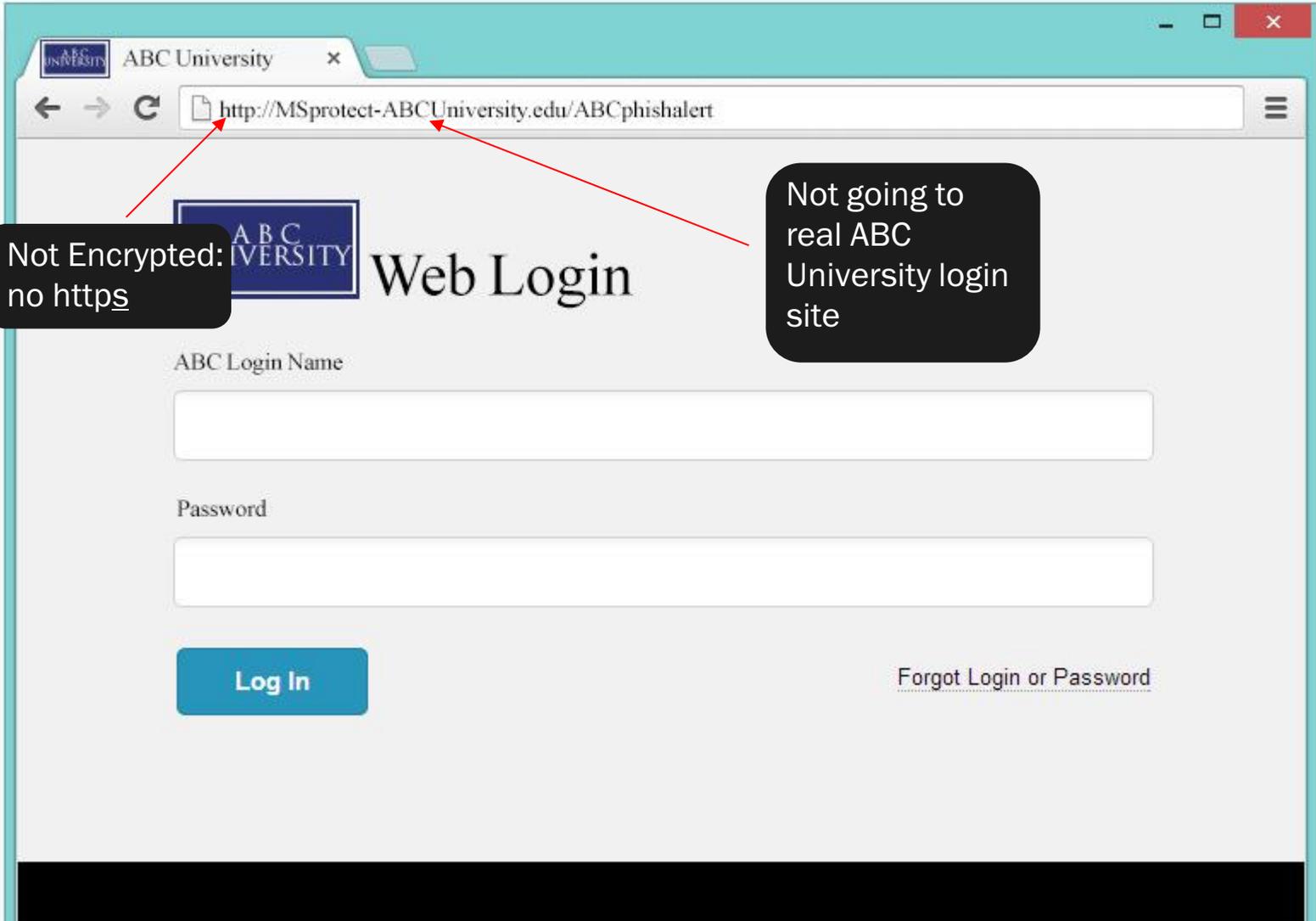
With these two steps taken, your account will be secured.

Serving you better,

ITS and Database Security, ABC University









Dear ABC University Employee,

In recent days, ABC University Information Security Office identified an email scam "phishing" attack where most of our employees details were thoroughly compromised. The email scam has been reported to the authorities with appropriate penalties in place for the culprits. Every employee affected so far have been compensated one way or the other.

Hence, the ABC University Human Resources, IST and Information Security unanimously agreed that our employees portal be upgraded to the latest platform with improved security checks in place.

Therefore, every employee is mandated to immediately follow this procedure below to ensure his/her details are protected from any future compromise by cyber criminals. Follow the link below to upgrade your employee platform

<http://protect.ABCUniversity.edu/>

Protect your information now!!

Sincerely,  
IST & Database Security, ABC University

# IMPACT TO PEOPLE AND ABC UNIVERSITY

- The University was able to recover a good portion of the money
- Anyone can fall for a clever phishing scam
- The University did replace paychecks
  - This would be very challenging on a large scale



# LESSONS LEARNED

- Understand how to know if you are at the real University web login, or a clever fake
- Learn how to analyze email messages to detect ones that are malicious
- Find out how to protect yourself and your devices from cyber threats
- Know common scams



# CARBANAK: THE GREAT ONLINE BANK ROBBERY

# WHAT IS CARBANAK

- Global bank robbery that stole \$1B from 30 banks
- Cyber-criminals using advanced APT techniques
- Used malware to infect bank networks
- Manual reconnaissance of networks
- Transferred millions of dollars via ATMs, SWIFT
- One victim lost \$7.3M from ATM fraud; Another suffered \$10M loss by exploiting the online banking platform

Read more at:

<https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-a>

# How the Carbanak cybergang stole \$1bn

## A targeted attack on a bank

### 1. Infection



100s of machines infected in search of the admin PC



### 2. Harvesting Intelligence

Intercepting the clerks' screens



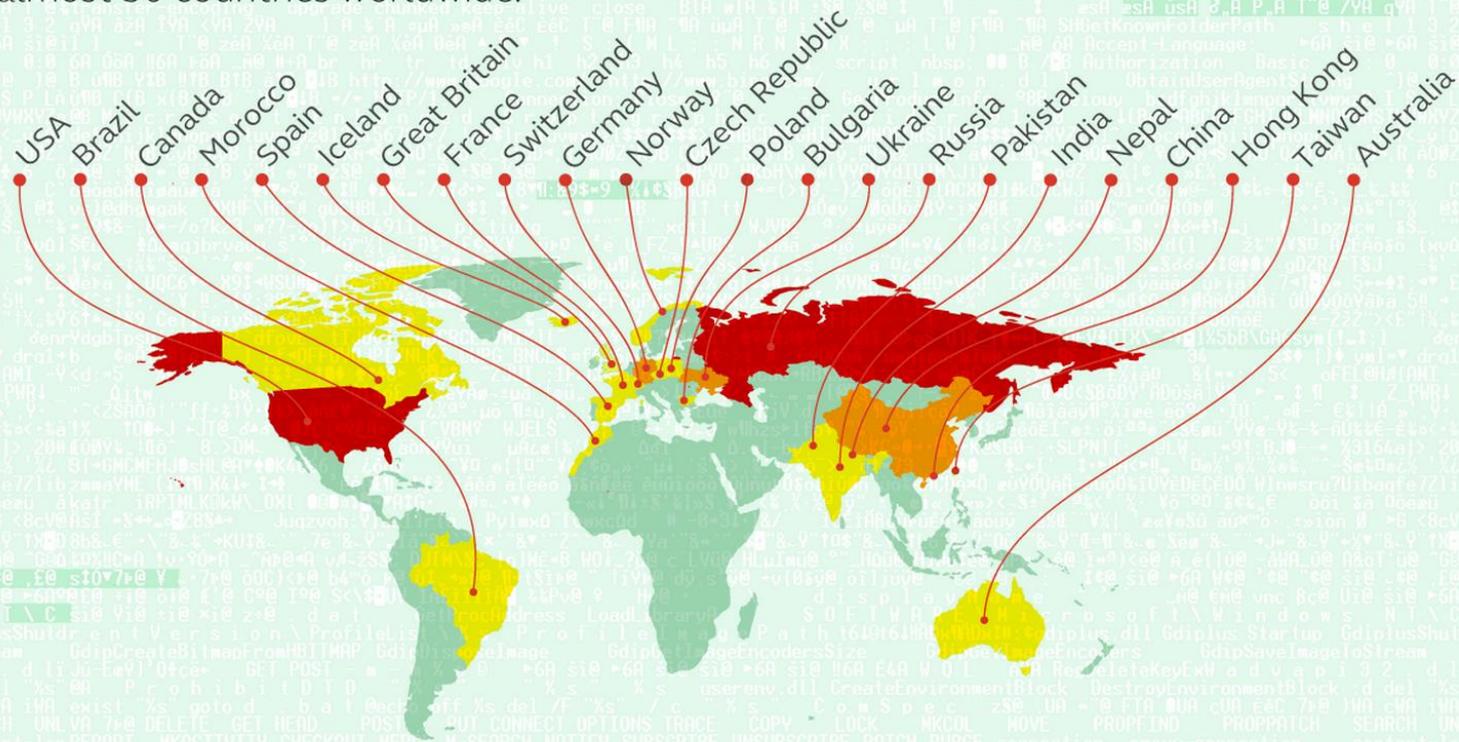
### 3. Mimicking the staff

How the money was stolen



# Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.



Number of target IPs by country

1 - 9      9 - 35      35 - 200

# CONCLUSION

- Fusion between APT and cybercrime
- Cybercriminals are getting smarter – going directly to the source of the money
- Nation-state level techniques are available to cybercriminals
- Attacks are becoming more sophisticated

# DATA IS ON THE MOVE



Device Proliferation

Data Storage Capability

Loss of Confidential Data

Untrusted Networks

# MOBILE MALWARE: 10 YEARS OLD ALREADY

## Ten Years of Mobile Malware



Sue Marquette Poremba | DATA SECURITY  | 22 JAN, 2014



Share



Hard to believe that it was 10 years ago when the first piece of mobile malware made its attack. According to Axelle Aprville, senior mobile anti-virus researcher with Fortinet, the first piece of mobile malware, a worm, was called Cabir and was targeted specifically to attack the Nokia Series 60. In an article looking at the history of mobile malware posted to [Mobile Security Zone](#), Aprville wrote:

[I]ts attack resulted in the word "Caribe" appearing on the screen of infected phones. The worm then spread itself by seeking other devices (phones, printers, game consoles...) within close proximity by using the phone's Bluetooth capability.

Compare that to what Aprville wrote about malware in 2013:



Top Security Priorities for CIOs in 2014

[View Slideshow](#)

# 2014 MOBILE MALWARE STATISTICS

## MOBILE MALWARE SAMPLES

Kaspersky Lab solutions blocked 1.4 million attacks on Android-based devices, four times as many as last year.

295,500 new mobile malicious programs were detected, 2.8 times as many as in 2013.

12,100 mobile banking Trojans were detected, nine times as many as last year.

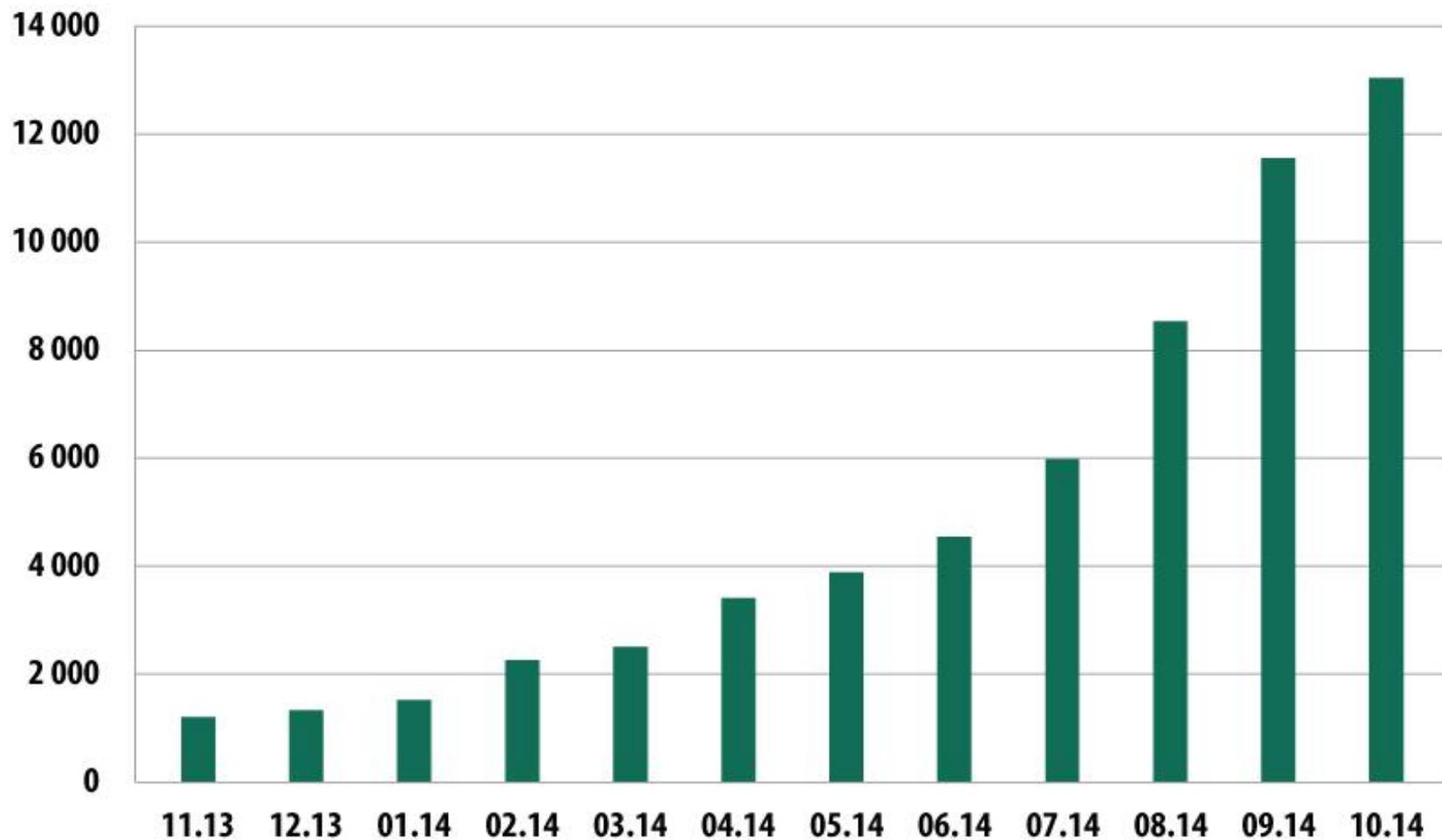
53 percent of attacks involved mobile Trojans targeting users' money (SMS-Trojans, banking Trojans)

19 percent of Android users (one in five) encountered a mobile threat at least once over the year.

Mobile malware attacks were registered in more than 200 countries worldwide.

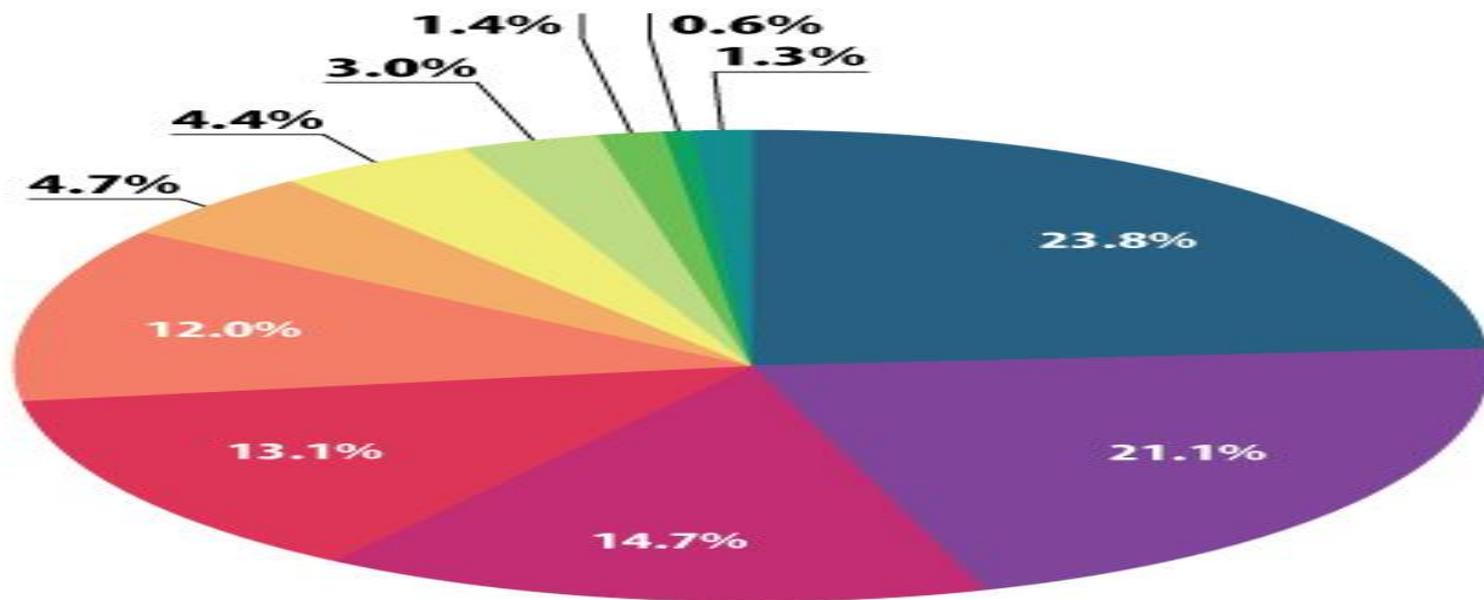


# MOBILE BANKING TROJANS 2014



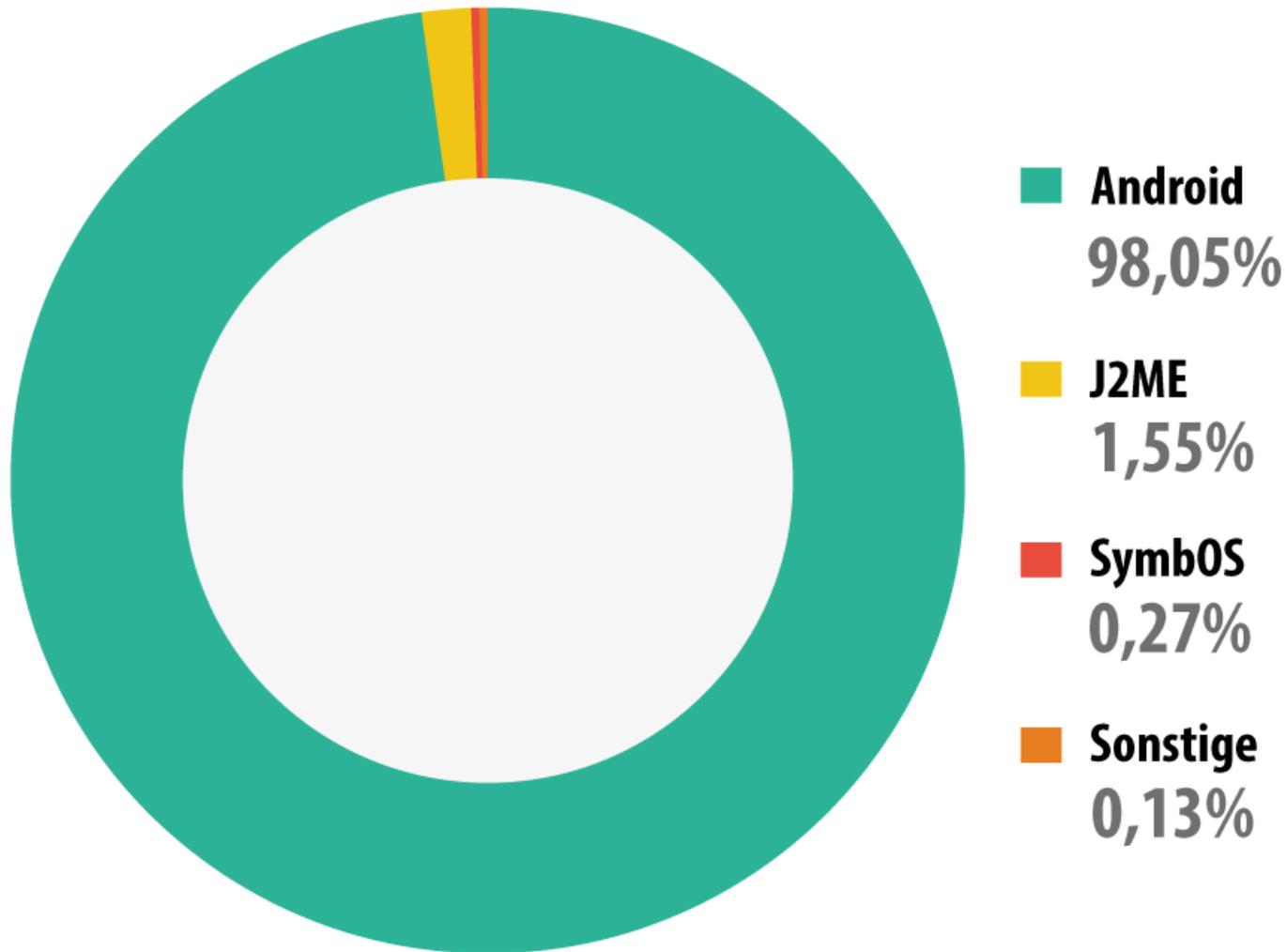
© Kaspersky Lab

# 2014 MOBILE MALWARE BREAKDOWN



© Kaspersky Lab

# MOBILE MALWARE BY MOBILE OS



I SA

# Hacker Says He Can Break Into Commercial Planes Via WiFi And In-Flight Entertainment Systems

Submitted by I33tdawg on Tue, 2014-08-05 01:34



- 24
- Like
- Share
- 4
- 8+1
- 32
- Tweet
- 9
- Share
- 
- Submit

Techno  
Hac

By Sa

Fol

Credit: Business Insider

Cyber security researcher Ruben Santamarta says he has figured out how to hack the satellite communications equipment on passenger jets through their WiFi and inflight entertainment systems - a claim that, if confirmed, could prompt a review of aircraft security.

Santamarta, a consultant with cyber security firm IOActive, is scheduled to lay out the technical details of his research at this week's Black Hat hacking conference in Las Vegas, an annual convention where



# IT IS NOT JUST THE MOBILE DEVICE YOU HAVE TO WORRY ABOUT



by **Dennis Fisher**

October 21, 2013 , 10:49 am

*Categories:* Social Engineering, Vulnerabilities, Web Security



5



October 17, 2013 , 11:10 am

## Apple iMessage Open to Man in the Middle, Spoofing Attacks

by **Dennis Fisher**

*Categories:* Apple, Cryptography, Featured, Privacy

The Apple iMessage protocol has been shrouded in secrecy for years now, but a pair of



3

security researchers have reverse-engineered the protocol and found that Apple controls the encryption key infrastructure for the system and therefore has the ability to read users' text messages—or decrypt them and hand them over at the order of a[...]

[Read more...](#)

# MALICIOUS AC/DC CHARGERS



What exactly is a malicious AC/DC charger? It will still charge your battery, but at the same time it will silently steal information from your smartphone when recharging via a USB port. In some cases fake charges can also install malware capable of tracking your location even when you leave the area, of stealing your notes, your contacts, your pictures, your messages and call records, your saved passwords and even your browser's cookies.

# NOT A TYPO!!



## Kaspersky Counts Over 10 Million Malicious Android Applications

Posted 02/10/2014 at 11:44am | by Paul Lilly

4

Comments

Print

Share

191

Tweet

21

Share

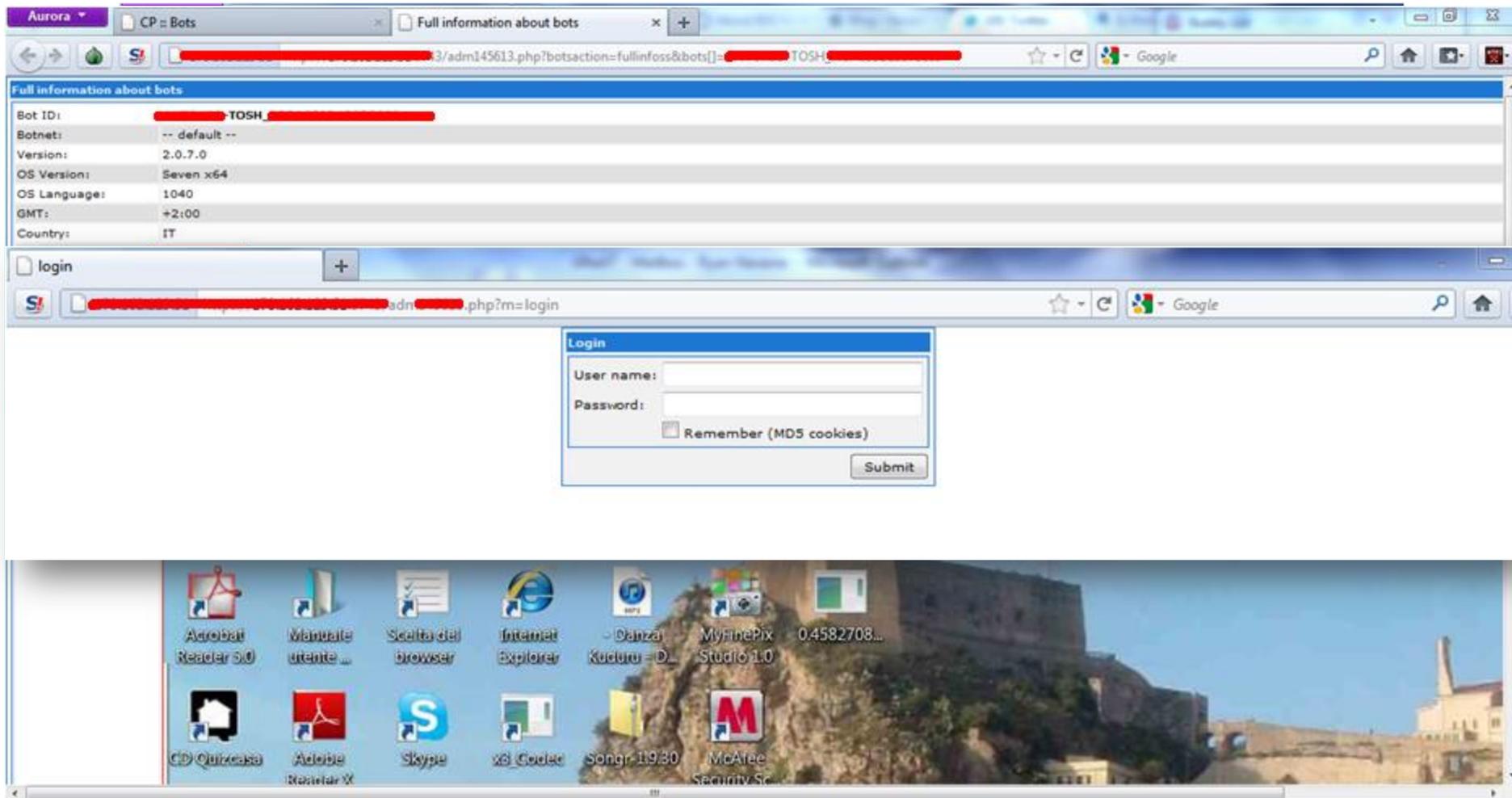
### Android is by far the biggest target of mobile malware

Security firm **Kaspersky** says it has logged **10 million dubious Android applications** to date. It comes down to a numbers game for cyber criminals, and since Android is the most popular mobile operating system on the planet -- market research firm **Canalys estimates** that Android accounted for 80 percent of smartphones shipped in 2013 -- it attracts the most attention from malware writers.

"In most cases malicious programs target the user's financial information. This was the case, for example, with the mobile version of Carberp Trojan that originated in Russia," **Kaspersky explains**. "It steals user credentials as they are sent to a bank server."



# THE DROPZONE – THIS IS REAL



# VULNERABILITIES – WHO IS AT RISK?

- ▶ In the first half of 2013, over 30,900,000 vulnerable programs and files were detected on user computers running Kaspersky Security Network (KSN)
- ▶ An average of 8 vulnerabilities were detected on each user's computer
- ▶ 45% of vulnerabilities detected by users were Oracle & Java
- ▶ Oracle Java, Adobe Reader, Office and Adobe Flash are the most exploited programs by cybercriminals in attacks



**In short, many more users are vulnerable than conventional thinking suggests**

# KREBS'S 3 BASIC RULES FOR ONLINE SAFETY

***“If you didn’t go looking for it, don’t install it!”***

***“If you installed it, update it.”***

***“If you no longer need it, remove it.”***

<http://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/>

# 5 WAYS IT MAY BE AN ACCOMPLICE



# 1) MIGRATION MYOPIA

Believing that company data never finds its way to home systems



## 2) SOCIAL MEDIA MANIA

### Adopting Social Media Without Protection



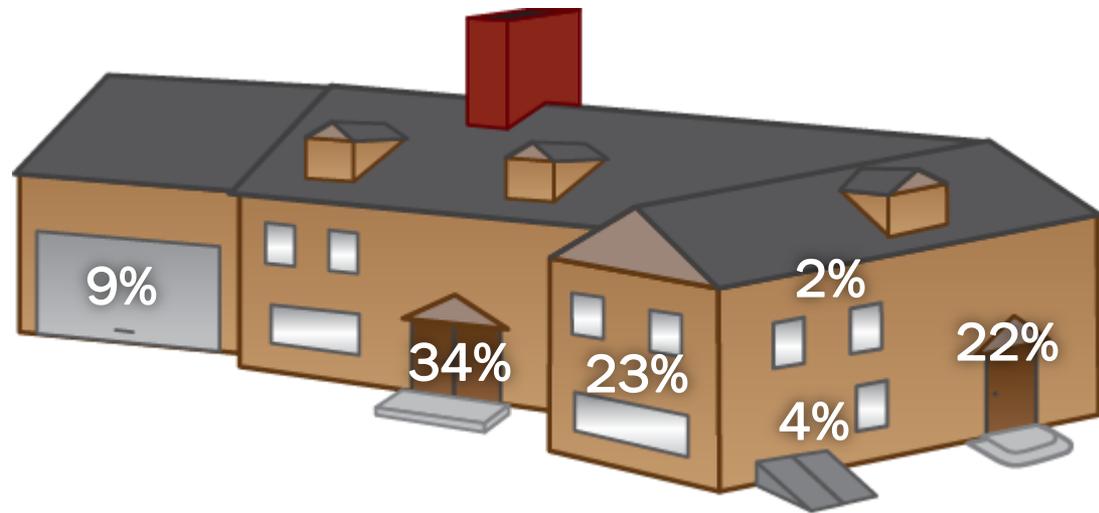
# 3) ATTENTION MISDIRECTION

## Focusing on Prevention vs. Detection and Response

95% of respondents listed the 12 items below

95% thought that Prevention was key

IT Security spending follows the same mindset



### Prevention

Doors  
Locks  
Windows  
Fence

### Detection

Alarm  
Motion detector  
Monitoring  
Crime watch

### Response

Dog  
Police  
Gun  
Insurance

## 4) AWARENESS DEFICIT

# Failing To Foster A Culture Of Awareness



KASPERSKY lab

KASPERSKY lab

## 5) RELIANCE ON COMPLIANCE

Compliance... just one step north of negligence.

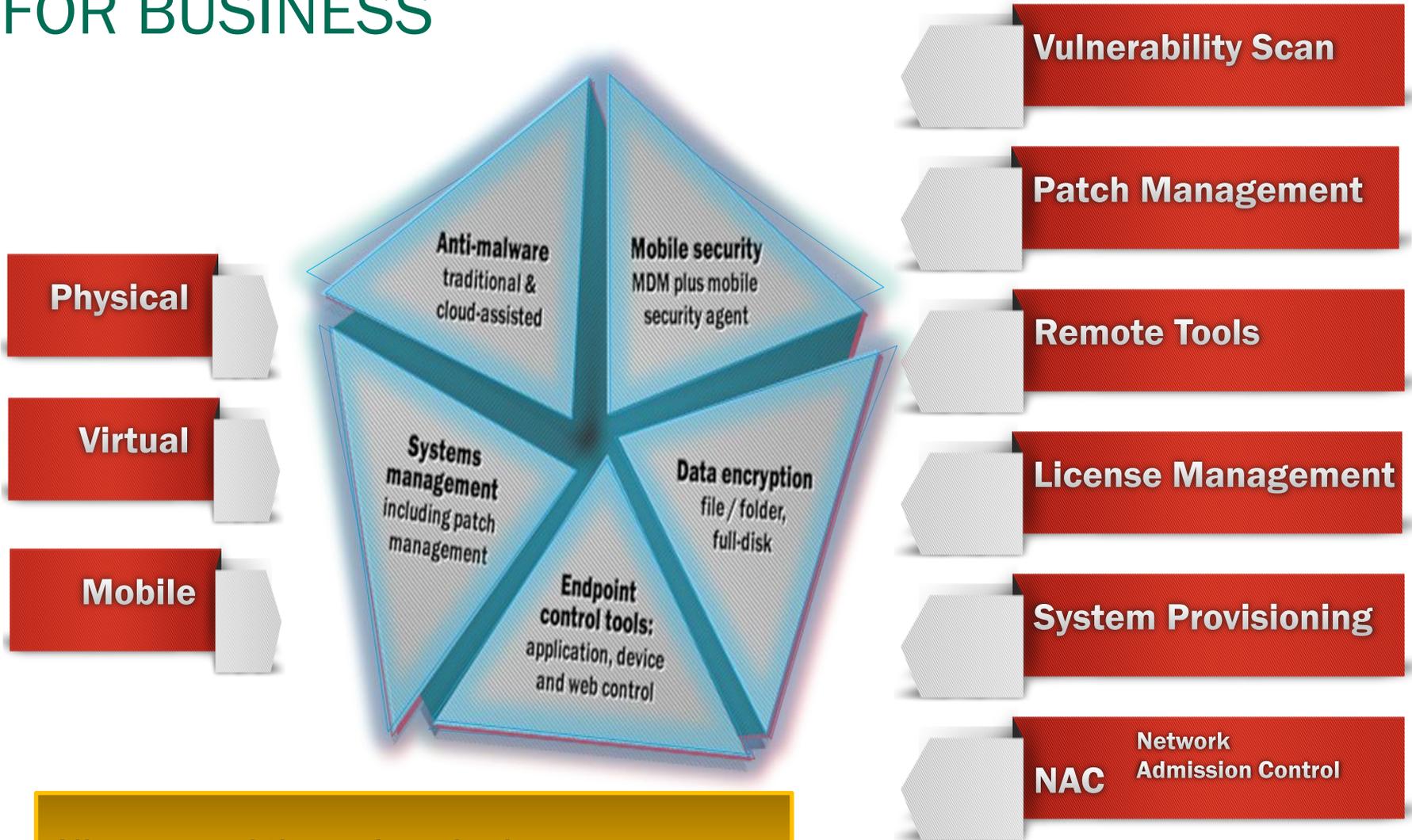
*Josh Corman*

**MEETS  
COMPLIANCY  
STANDARDS**



Compliant Lifeboat Capacity:	1,060
Actual Lifeboat Capacity:	1,178
Passengers:	3,547

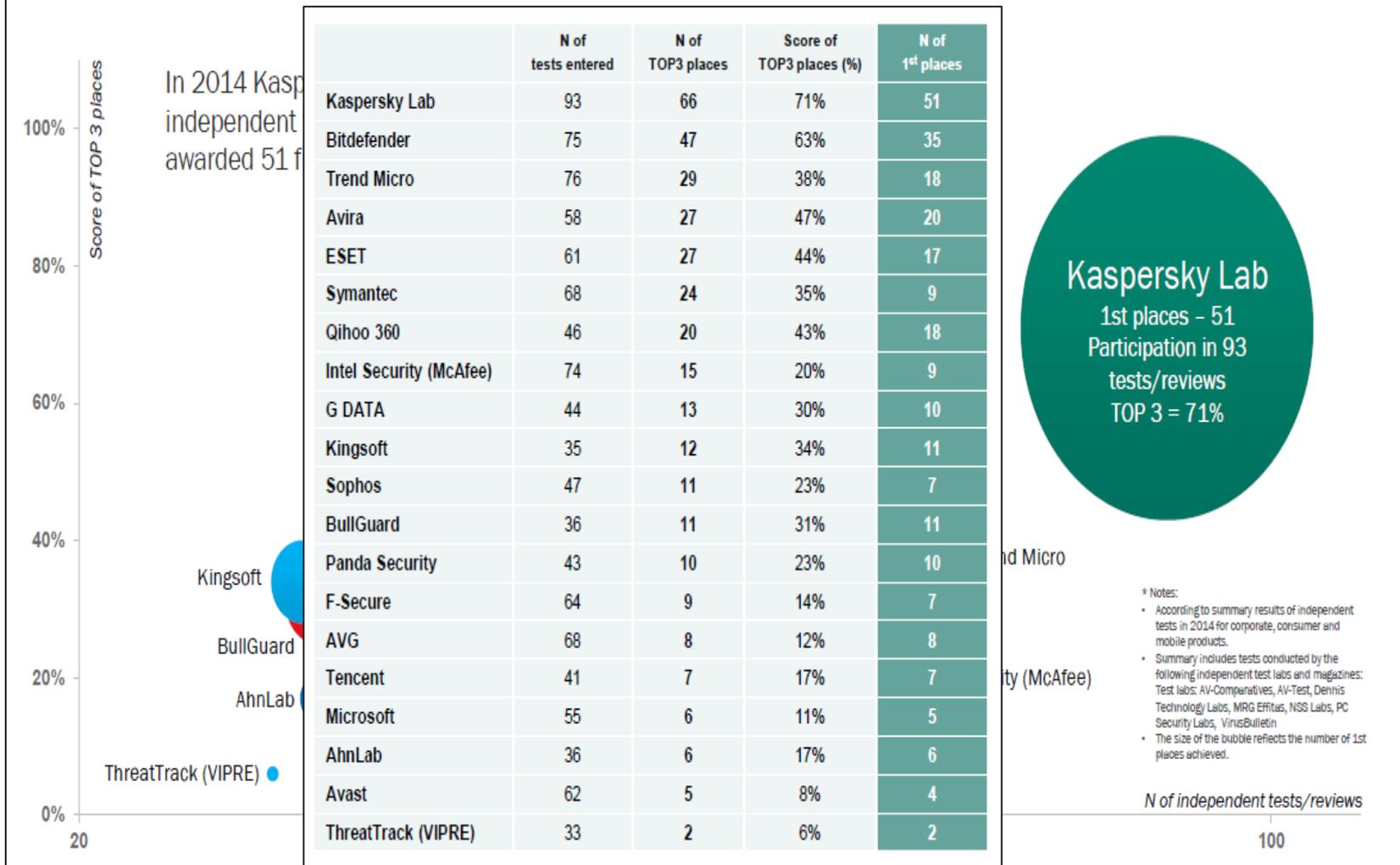
# KASPERSKY ENDPOINT SECURITY FOR BUSINESS



All managed through a single management console: Kaspersky Security Center

# OUR LEADERSHIP IS PROVEN BY INDEPENDENT TESTS

## KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION\*



# QUESTIONS & ANSWERS

**Contact Kaspersky:**

**866-563-3099**

**[corporatesales@kaspersky.com](mailto:corporatesales@kaspersky.com)**

**[www.kaspersky.com](http://www.kaspersky.com)**

**Mark Villinski**

**[Mark.villinski@kaspersky.com](mailto:Mark.villinski@kaspersky.com)**