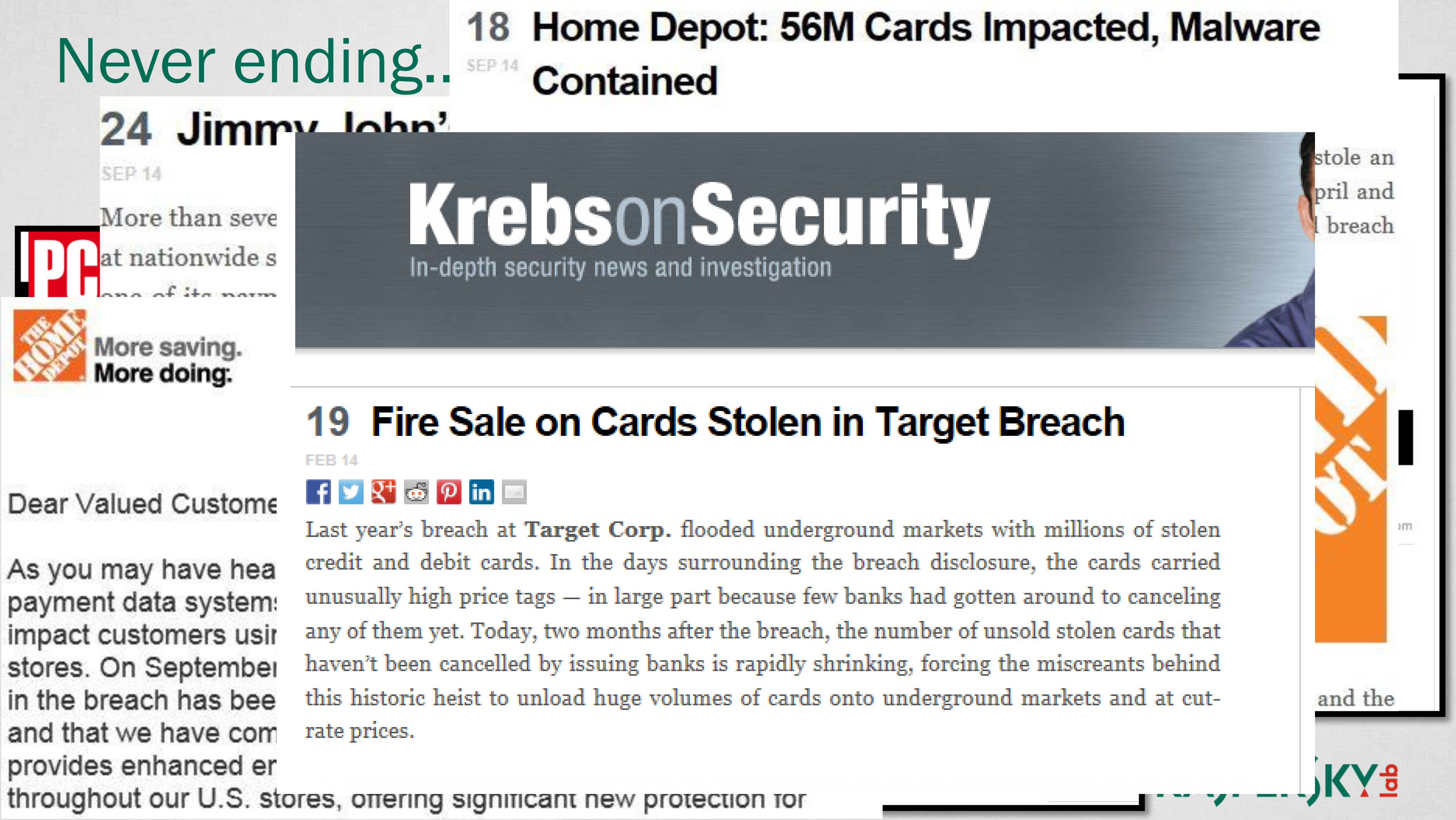
The Explosion of Cybercrime - The 5 Ways IT May Be an Accomplice

Brent Graham
Kaspersky Lab

Never ending..



18 **Home Depot: 56M Cards Impacted, Malware Contained**

SEP 14

24 **Jimmy John'**

SEP 14

More than seve
at nationwide s
one of its paym

KrebsonSecurity

In-depth security news and investigation

More saving.
More doing.

Dear Valued Custome

As you may have hea
payment data system
impact customers usir
stores. On Septembe
in the breach has bee
and that we have com
provides enhanced er
throughout our U.S. stores, offering significant new protection for

19 **Fire Sale on Cards Stolen in Target Breach**

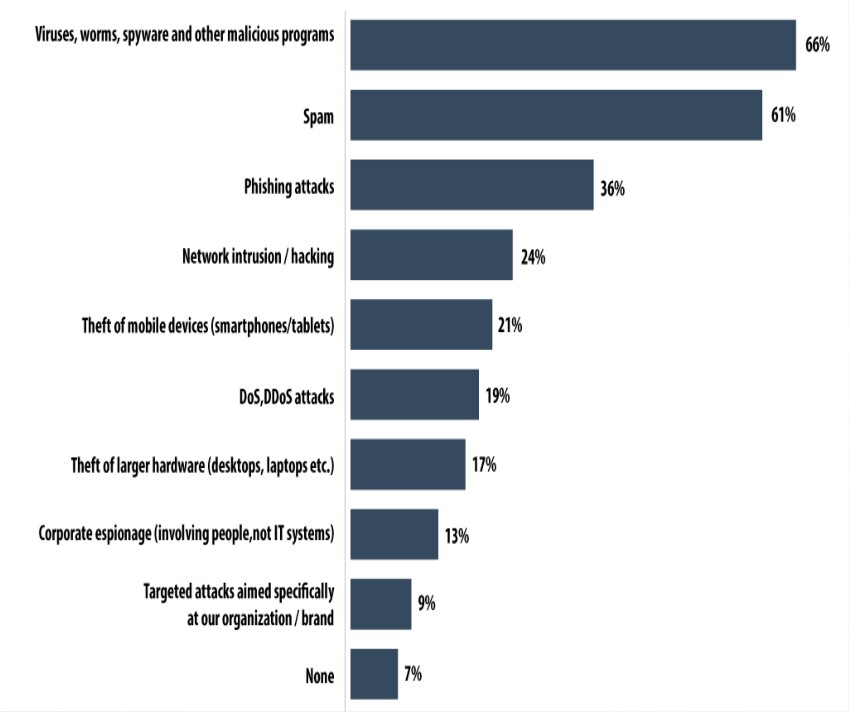
FEB 14

Last year's breach at **Target Corp.** flooded underground markets with millions of stolen credit and debit cards. In the days surrounding the breach disclosure, the cards carried unusually high price tags — in large part because few banks had gotten around to canceling any of them yet. Today, two months after the breach, the number of unsold stolen cards that haven't been cancelled by issuing banks is rapidly shrinking, forcing the miscreants behind this historic heist to unload huge volumes of cards onto underground markets and at cut-rate prices.

stole an
pril and
l breach

and the

2013 Corporate Threats Survey

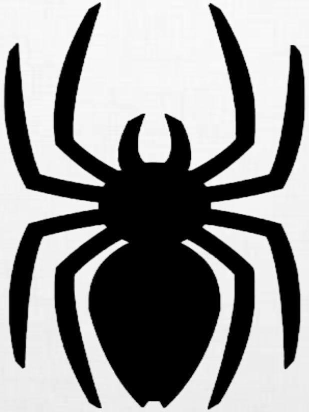


- 91% of business's suffered one cyber attack in the last 12 months
- 9% of business's were victims of a targeted attack
- Malicious programs could soon replace company insiders as the way of gathering information

https://www.securelist.com/en/analysis/204792317/Kaspersky_Security_Bulletin_2013_Corporate_threats

1994

One new virus every hour

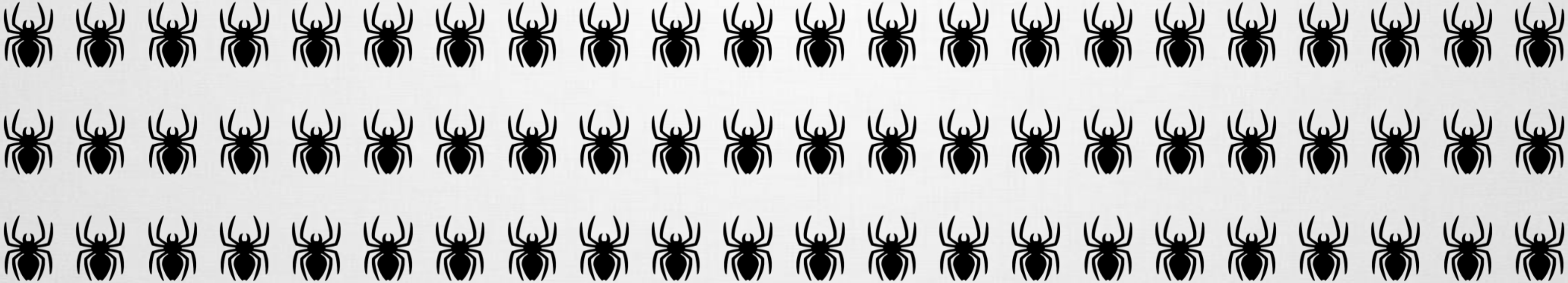


Kaspersky Lab

Evolution of malware waves we have to deal with

2006

One new virus every minute



Kaspersky Lab

Evolution of malware waves we have to deal with

2011

One new virus every second

Or 70,000 samples/day

What about

2014

?

Kaspersky Lab

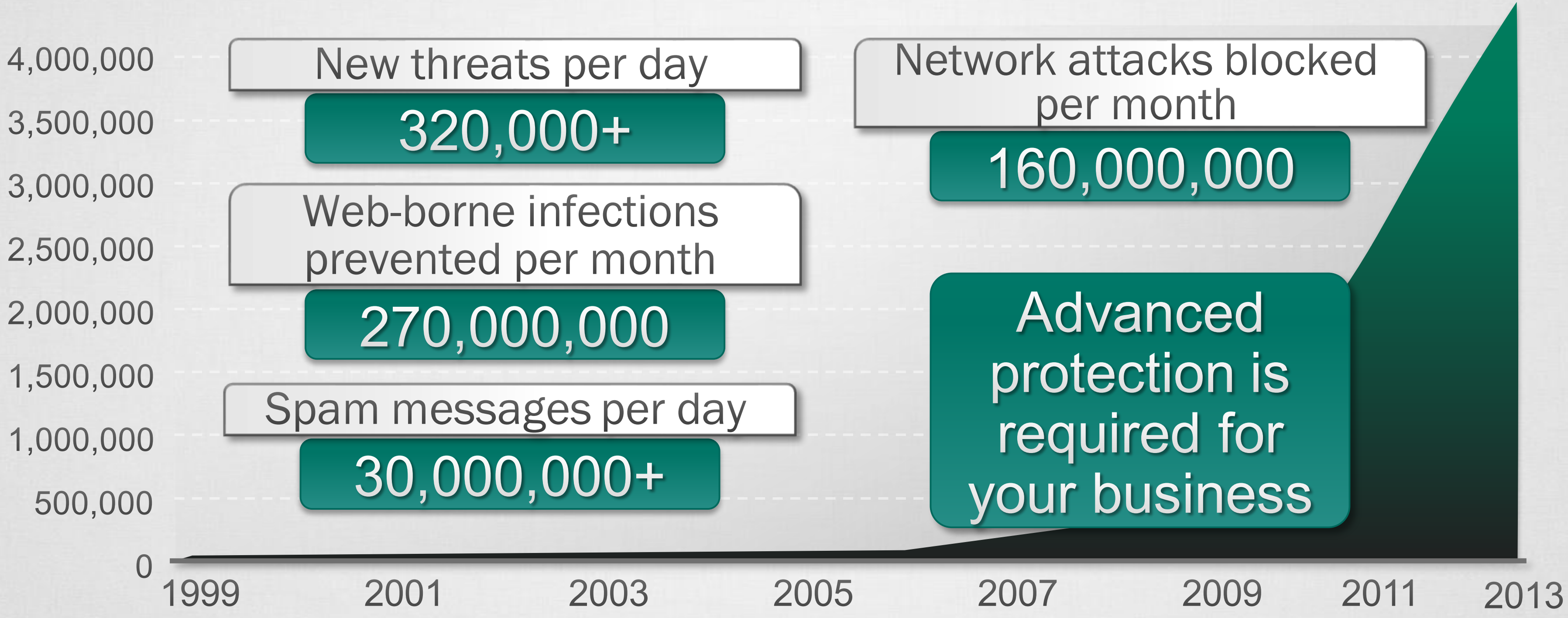
is currently processing

320,000

unique malware samples

EVERY DAY

THREATS: SMARTER, FASTER, MORE



New threats per day

320,000+

Web-borne infections prevented per month

270,000,000

Spam messages per day

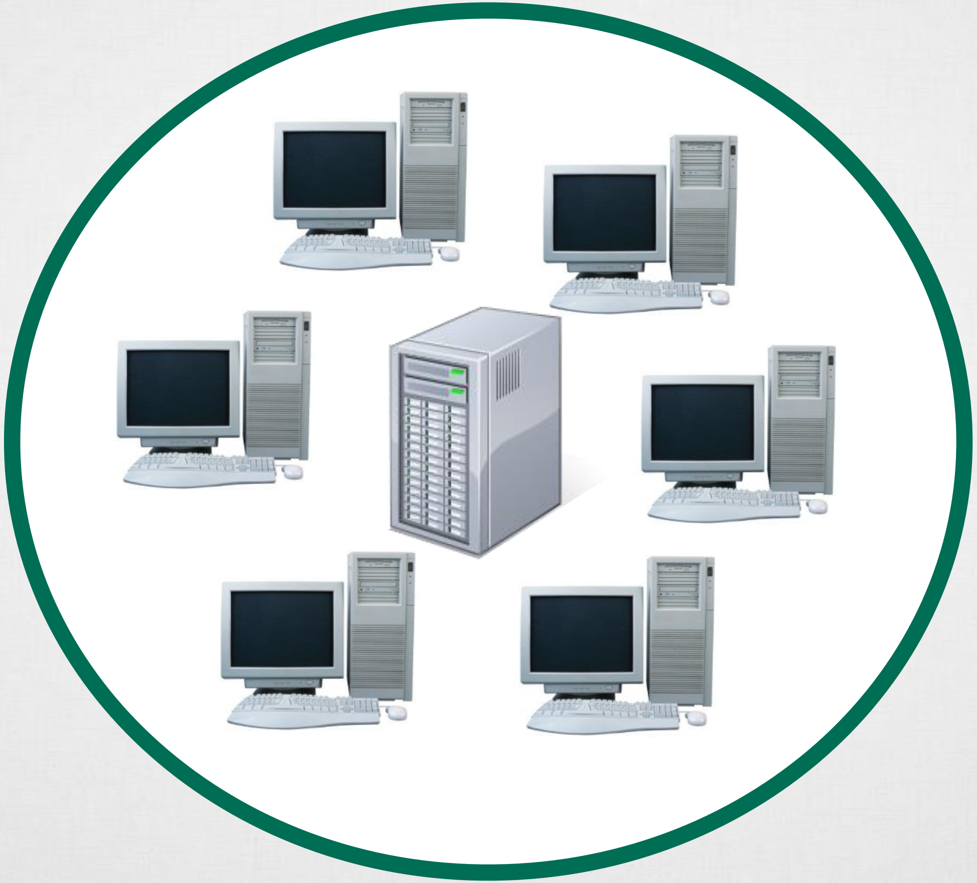
30,000,000+

Network attacks blocked per month

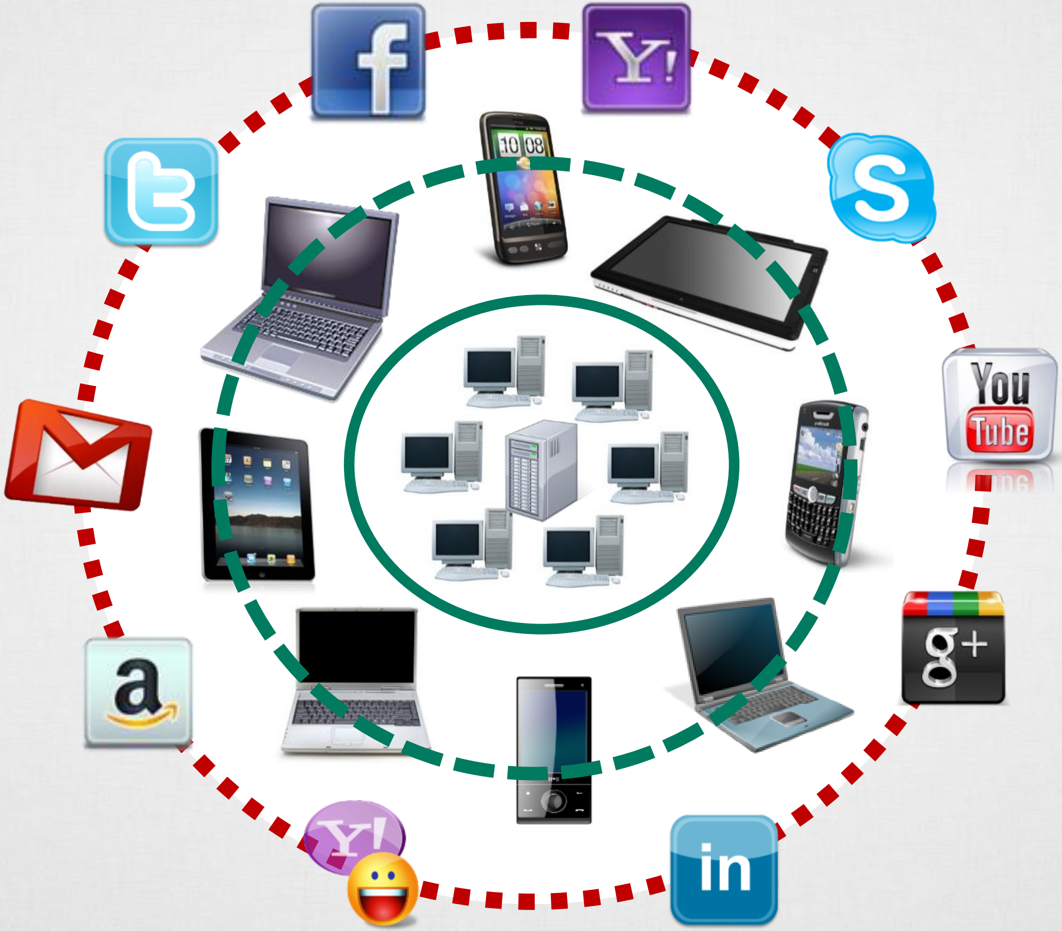
160,000,000

Advanced protection is required for your business

ORIGINAL CORPORATE SECURITY PERIMETER



TODAY'S SECURITY PERIMETER



Online Account Takeover

Corporate accounts a
generated have expe
legal protections tha

the ACH credits that are
not offer the same
tion E.

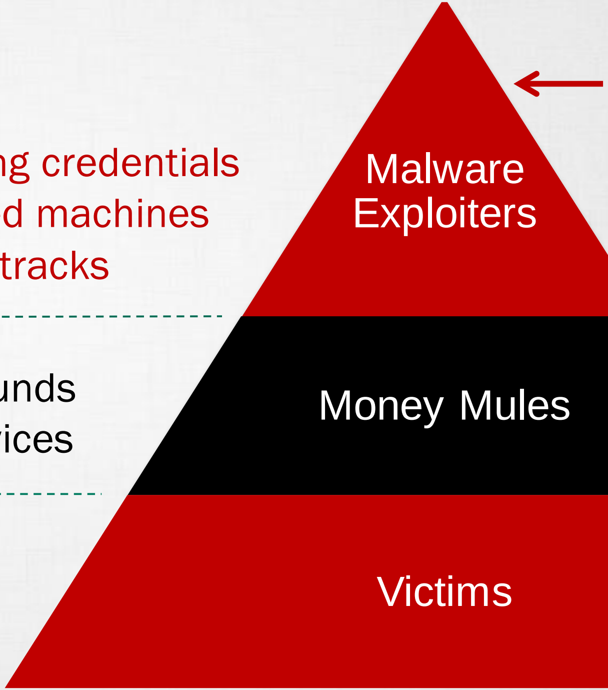
EARN $$$$$$ WITHOUT LEAVING YOUR HOME
Make $1000 a week!
No experience necessary!
Just call 1-800-555-SCAM right away to get started!
Joe accesses Web page for "Bank A" requiring log in
Web Page
oe's information is sent to cyber criminal

THE CYBER-THEFT PYRAMID

- Purchase malware to steal banking credentials
- Launch attacks from compromised machines
- Transfer stolen funds, cover their tracks

- Engage in the transfer of stolen funds
- Retain a percentage for their services

- Individuals
- Businesses
- Financial Institutions

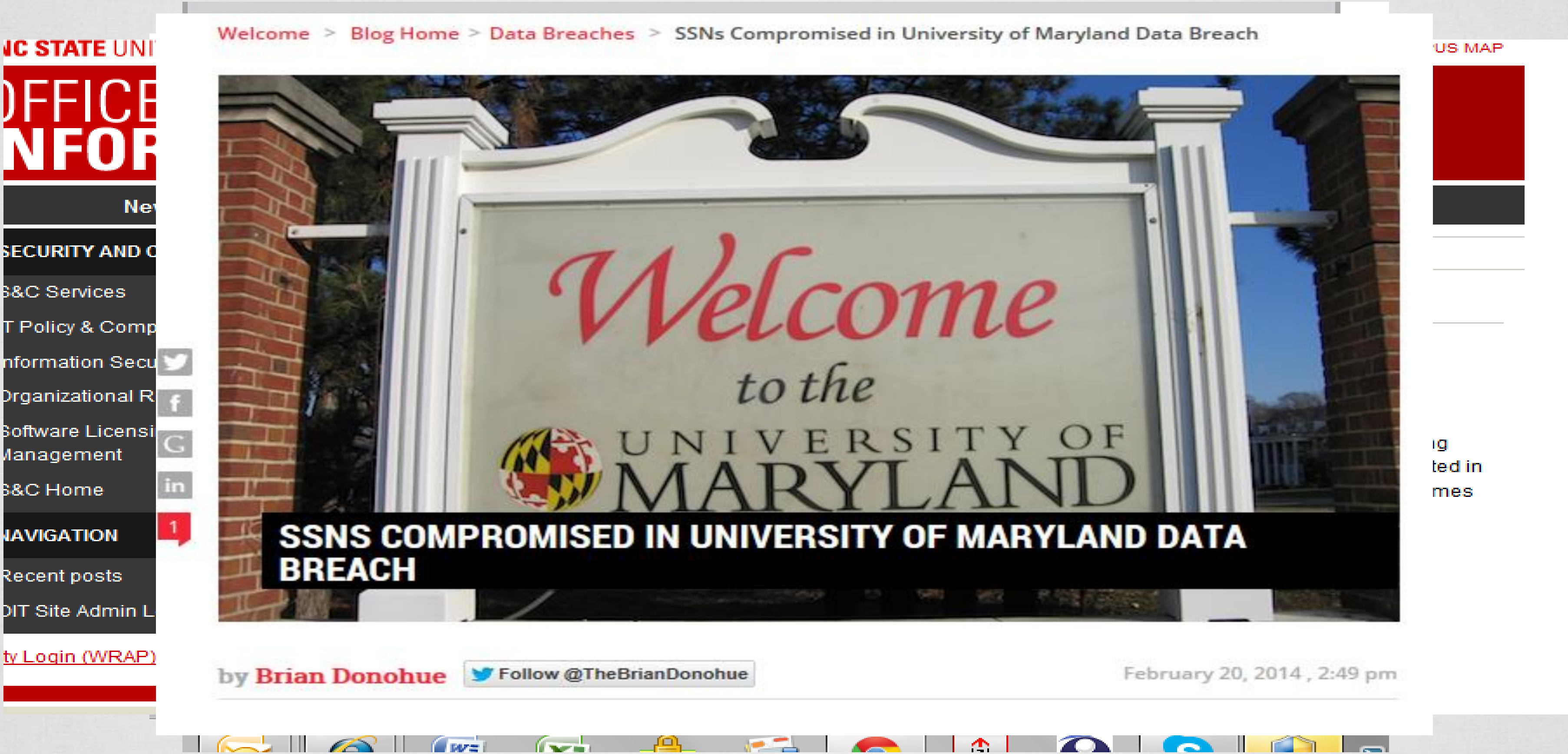


Malware Exploiters

Money Mules

Victims

Malware Coders: Develop malicious software sold on the Black Market



NC STATE UNI

OFFICE
NFOR

Ne

SECURITY AND C

S&C Services

T Policy & Comp

nformation Secu

Organizational R

Software Licensi
Management

S&C Home

NAVIGATION

Recent posts

OIT Site Admin L

ty Login (WRAP)

US MAP

ig
ted in
mes

Welcome > Blog Home > Data Breaches > SSNs Compromised in University of Maryland Data Breach

SSNS COMPROMISED IN UNIVERSITY OF MARYLAND DATA BREACH

by Brian Donohue Follow @TheBrianDonohue

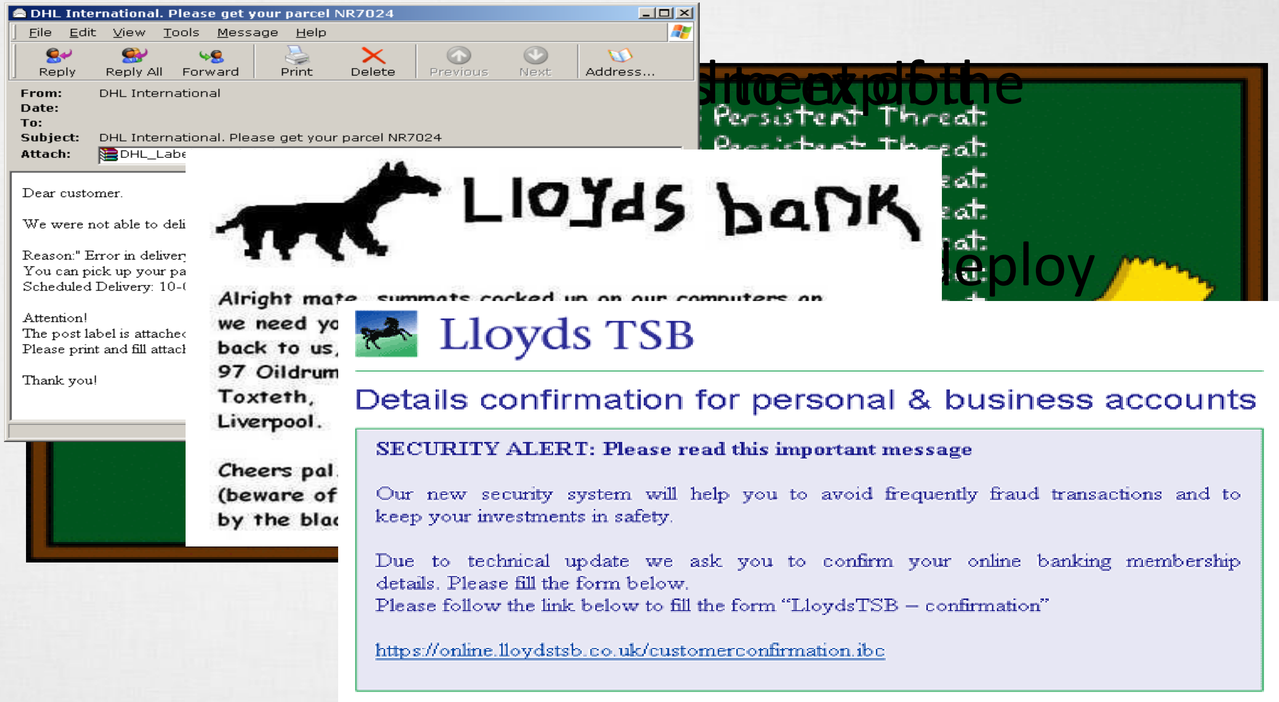
February 20, 2014 , 2:49 pm

Threat Landscape - Malware

A

P

T



DHL International. Please get your parcel NR7024

From: DHL International
Date:
To:
Subject: DHL International. Please get your parcel NR7024
Attach: DHL_Labe

Dear customer.

We were not able to deli

Reason:" Error in deliver
You can pick up your pa
Scheduled Delivery: 10-(

Attention!
The post label is attache
Please print and fill attacl

Thank you!

[illegible] the

deploy

Alright mate, summats cocked up on our computers an
we need yo
back to us,
97 Oildrum
Toxteth,
Liverpool.

Cheers pal.
(beware of
by the blac

Details confirmation for personal & business accounts

SECURITY ALERT: Please read this important message

Our new security system will help you to avoid frequently fraud transactions and to keep your investments in safety.

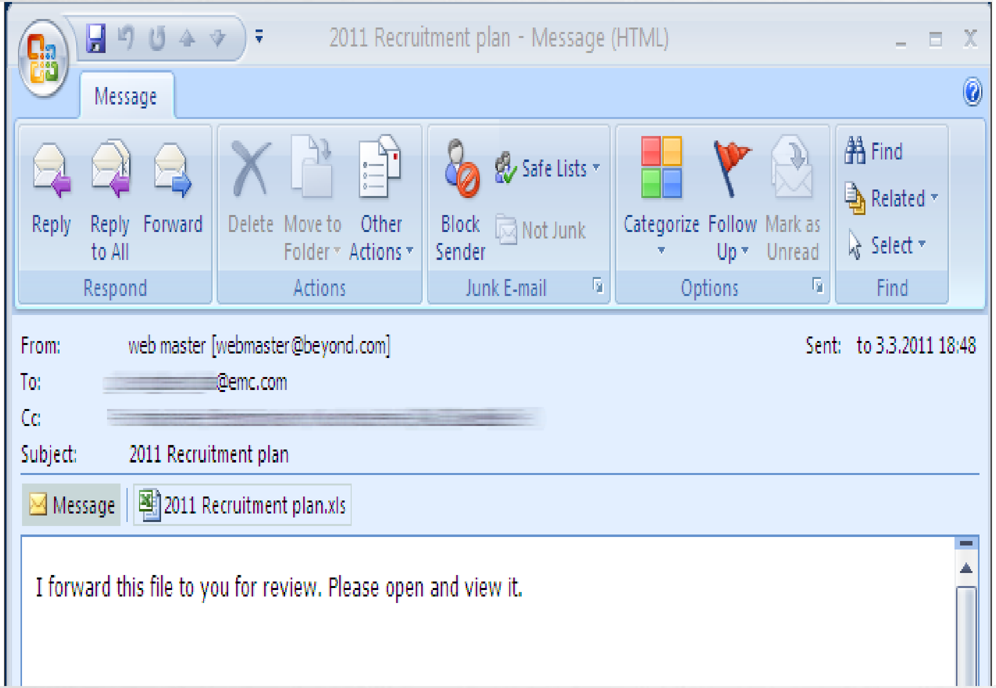
Due to technical update we ask you to confirm your online banking membership details. Please fill the form below.
Please follow the link below to fill the form "LloydsTSB – confirmation"

https://online.lloydstsb.co.uk/customerconfirmation.ibc

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



From: web master [webmaster@beyond.com]

Sent: to 3.3.2011 18:48

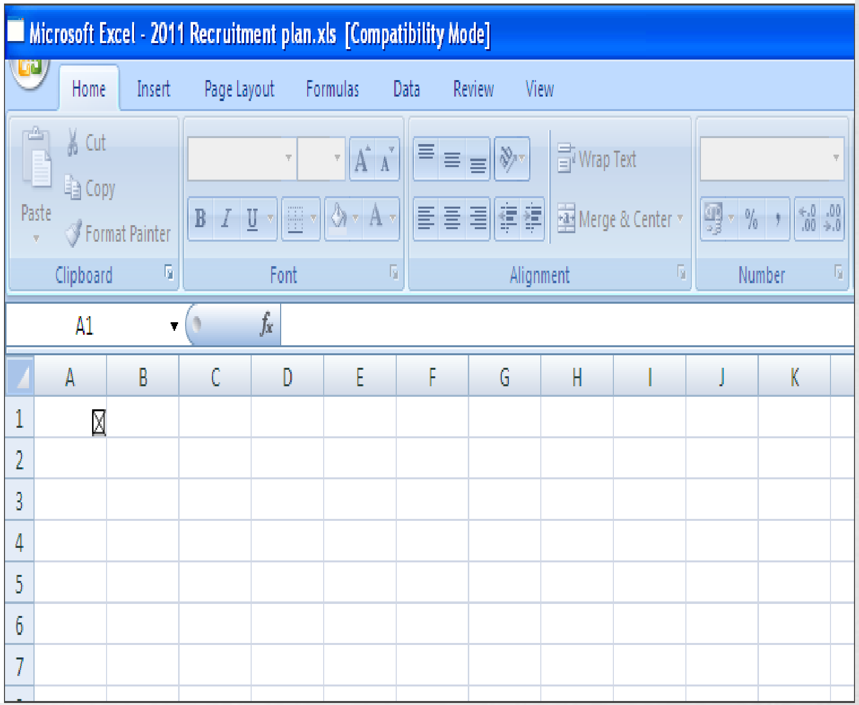
To: [redacted]@emc.com

Cc: [redacted]

Subject: 2011 Recruitment plan

Message | 2011 Recruitment plan.xls

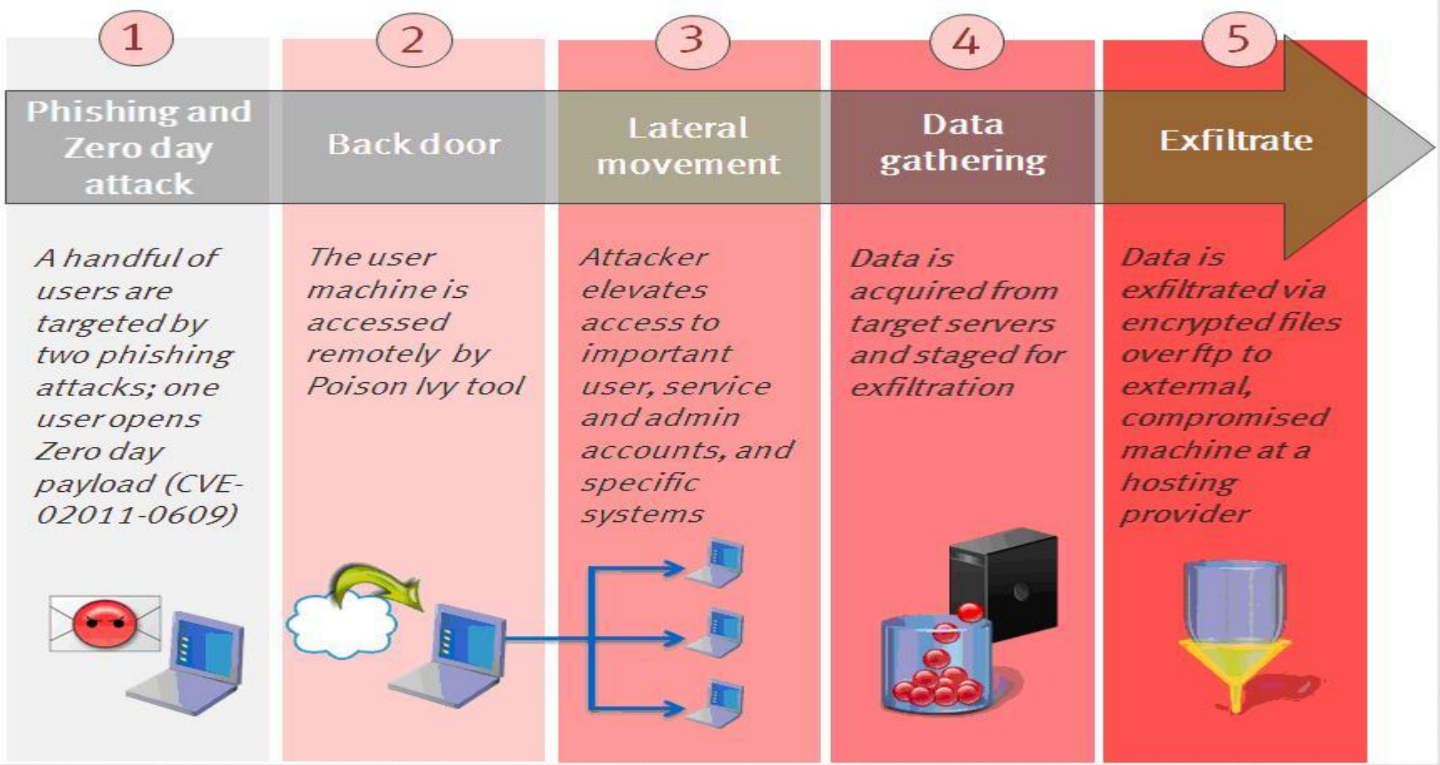
I forward this file to you for review. Please open and view it.



http://www.f-secure.com/weblog/archives/00002226.html

The Blueprint

How does this happen?



1 Phishing and Zero day attack

A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)

2 Back door

The user machine is accessed remotely by Poison Ivy tool

3 Lateral movement

Attacker elevates access to important user, service and admin accounts, and specific systems

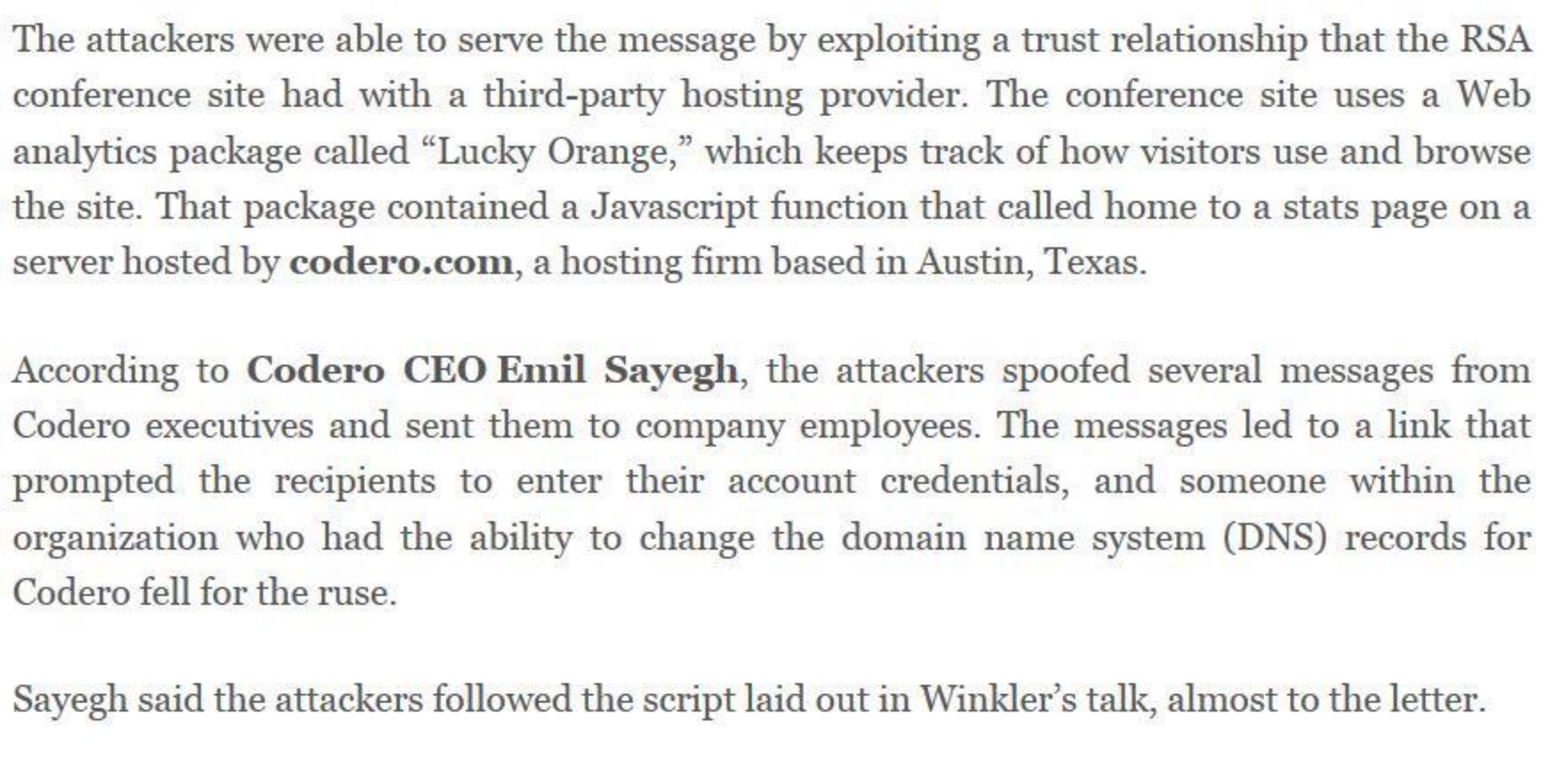
4 Data gathering

Data is acquired from target servers and staged for exfiltration

5 Exfiltrate

Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

Targeted Attacks:



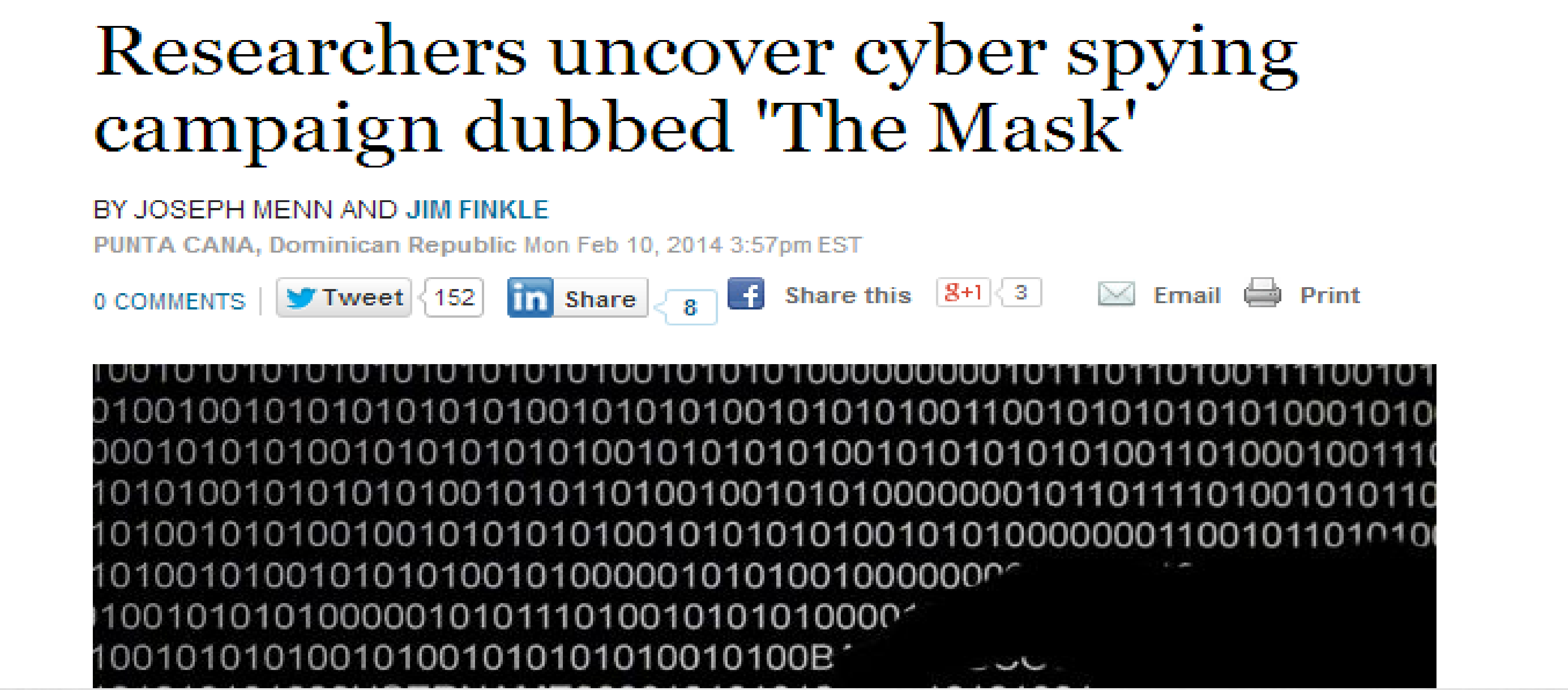
The attackers were able to serve the message by exploiting a trust relationship that the RSA conference site had with a third-party hosting provider. The conference site uses a Web analytics package called “Lucky Orange,” which keeps track of how visitors use and browse the site. That package contained a Javascript function that called home to a stats page on a server hosted by **codero.com**, a hosting firm based in Austin, Texas.

According to **Codero CEO Emil Sayegh**, the attackers spoofed several messages from Codero executives and sent them to company employees. The messages led to a link that prompted the recipients to enter their account credentials, and someone within the organization who had the ability to change the domain name system (DNS) records for Codero fell for the ruse.

Sayegh said the attackers followed the script laid out in Winkler’s talk, almost to the letter.

http://krebsonsecurity.com/2014/05/complexity-as-the-enemy-of-security/#more-25821

State Sponsored Cyber Terrorism



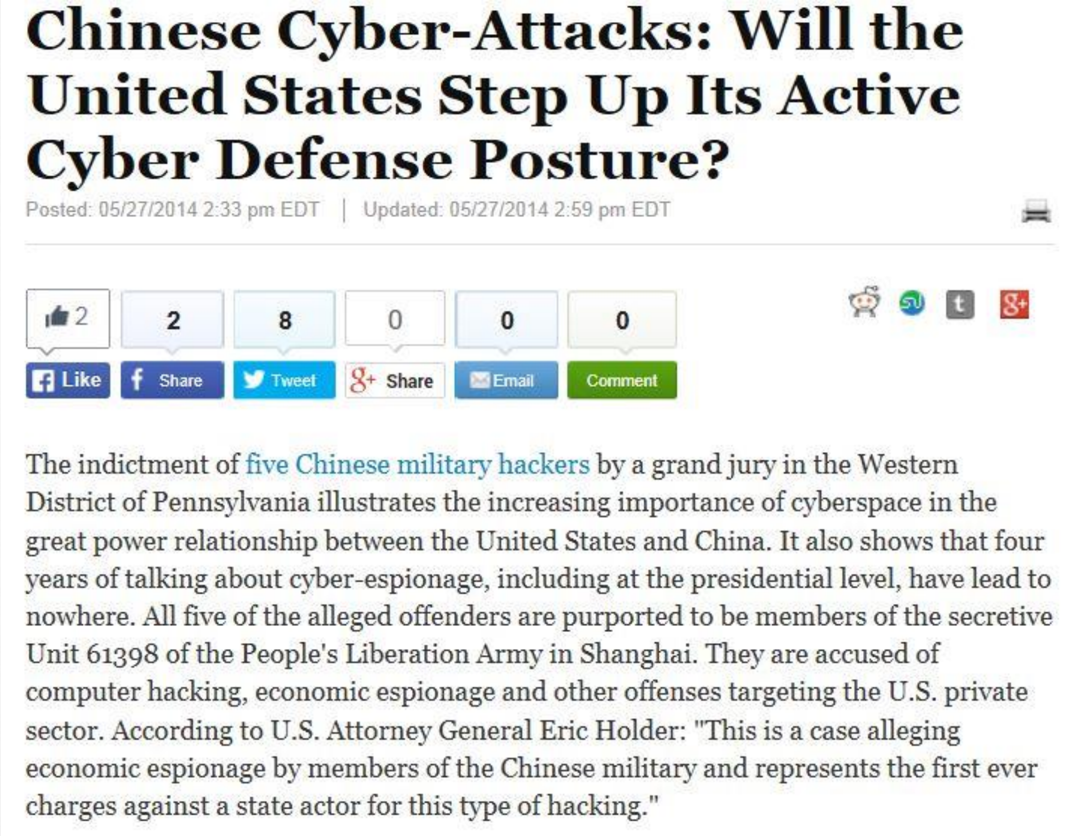
Researchers uncover cyber spying campaign dubbed 'The Mask'

BY JOSEPH MENN AND JIM FINKLE

PUNTA CANA, Dominican Republic Mon Feb 10, 2014 3:57pm EST

http://www.reuters.com/article/2014/02/10/us-cybersecurity-espionage-mask-idUSBREA191KU20140210

State Sponsored Cyber Terrorism



Chinese Cyber-Attacks: Will the United States Step Up Its Active Cyber Defense Posture?

Posted: 05/27/2014 2:33 pm EDT | Updated: 05/27/2014 2:59 pm EDT

The indictment of five Chinese military hackers by a grand jury in the Western District of Pennsylvania illustrates the increasing importance of cyberspace in the great power relationship between the United States and China. It also shows that four years of talking about cyber-espionage, including at the presidential level, have lead to nowhere. All five of the alleged offenders are purported to be members of the secretive Unit 61398 of the People's Liberation Army in Shanghai. They are accused of computer hacking, economic espionage and other offenses targeting the U.S. private sector. According to U.S. Attorney General Eric Holder: "This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking."

http://www.huffingtonpost.com/franzstefan-gady/chinese-cyberattacks-will_b_5384845.html

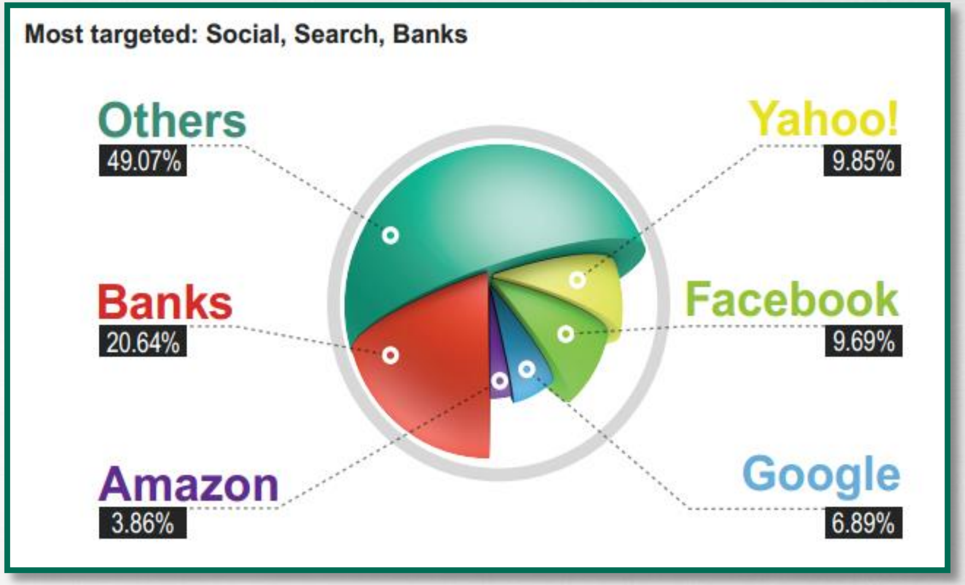
KASPERSKY LAB ANALYSIS REPORT

THE EVOLUTION

OF PHISHING ATTACKS:

2011-2013

KASPERSKY lab



Most targeted: Social, Search, Banks

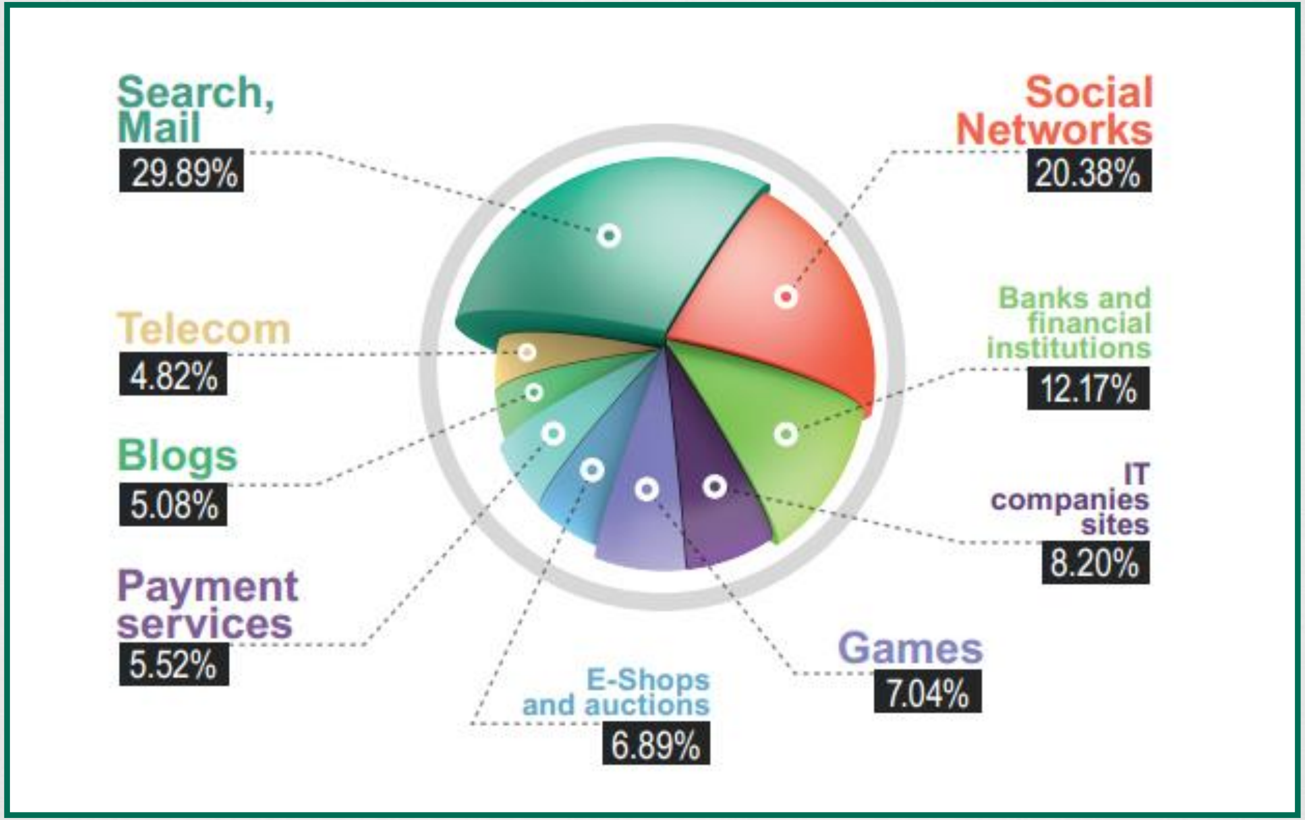
- In 2012-2013, 37.3 million users around the world were subjected to phishing attacks, up 87% from 2011-2012

- The number of distinct sources of attacks in 2012 and 2013 increased 3.3 times (+330%)

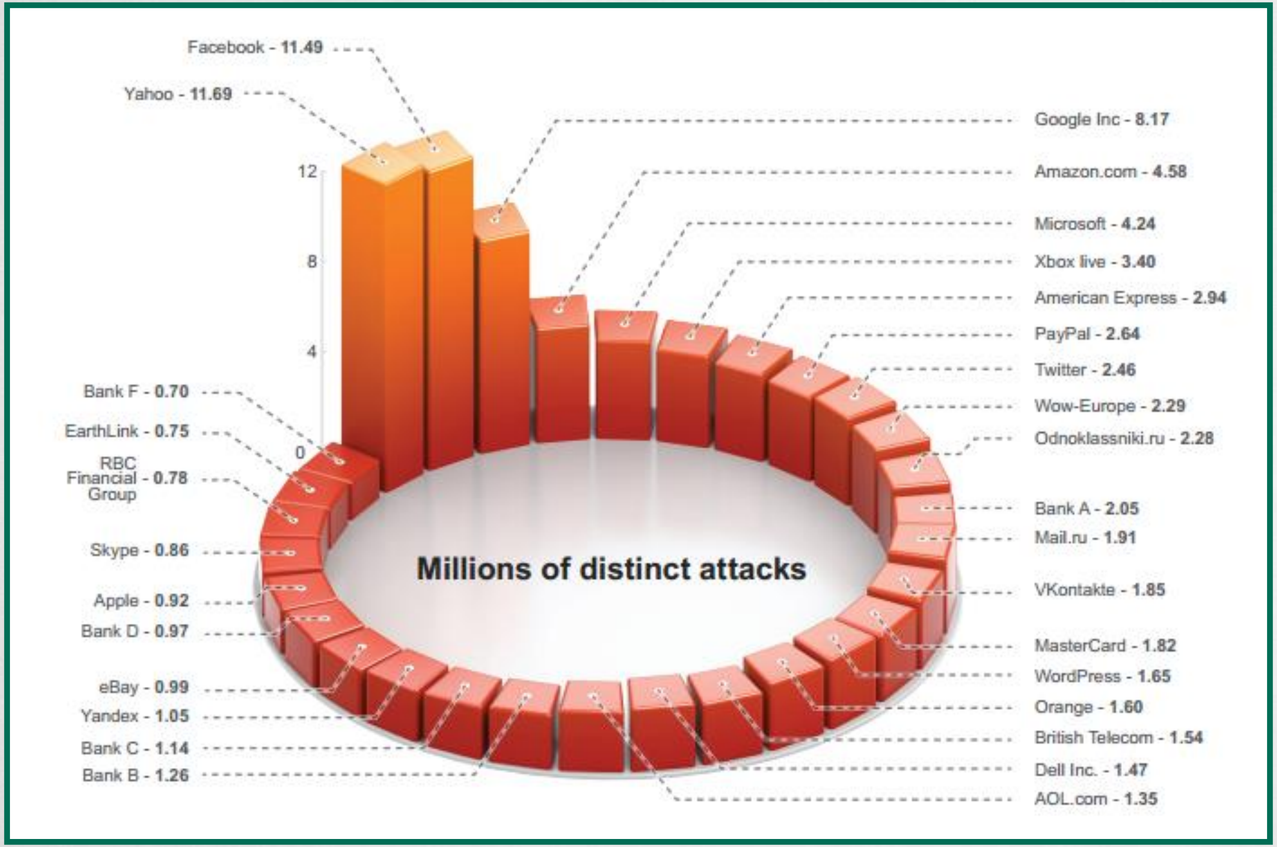
- 102,100 Internet users around the world were subjected to phishing attacks daily!

SOURCE: THE EVOLUTION OF PHISHING ATTCKS 2011-2013, KASPERSKY LAB ANALYSIS REPORT

PHISHING SITES BY CATEGORY



TOP 30 PHISHING TARGETED SITES 2012-2013

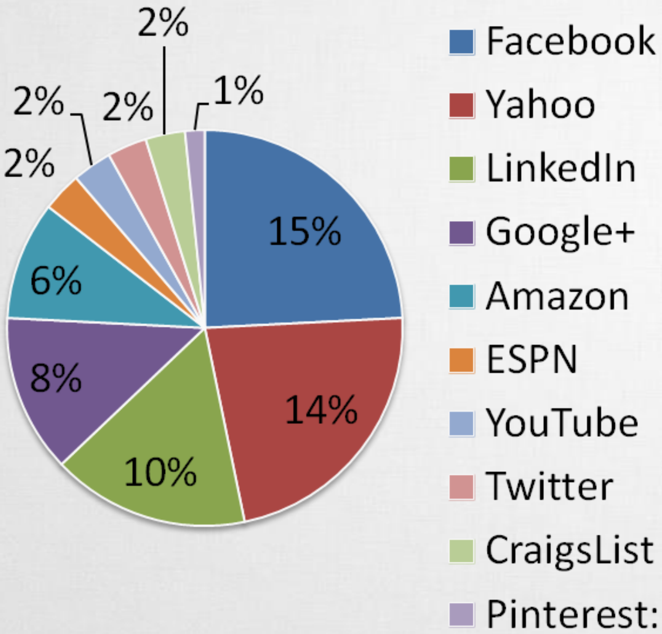


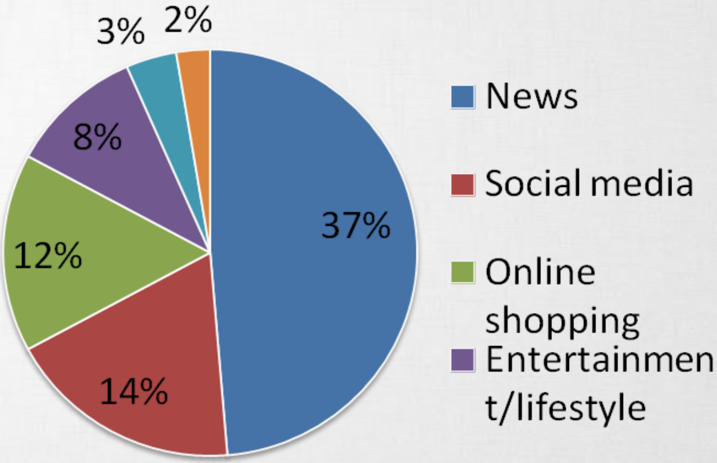
	USA
1	Yahoo!
2	Facebook
3	Google Inc
4	Amazon.com: Online Shopping
5	Wow-Europe
6	Microsoft Corporation
7	AOL.com
8	American Express
9	Bank A
10	Twitter

KASPERSKY lab

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/

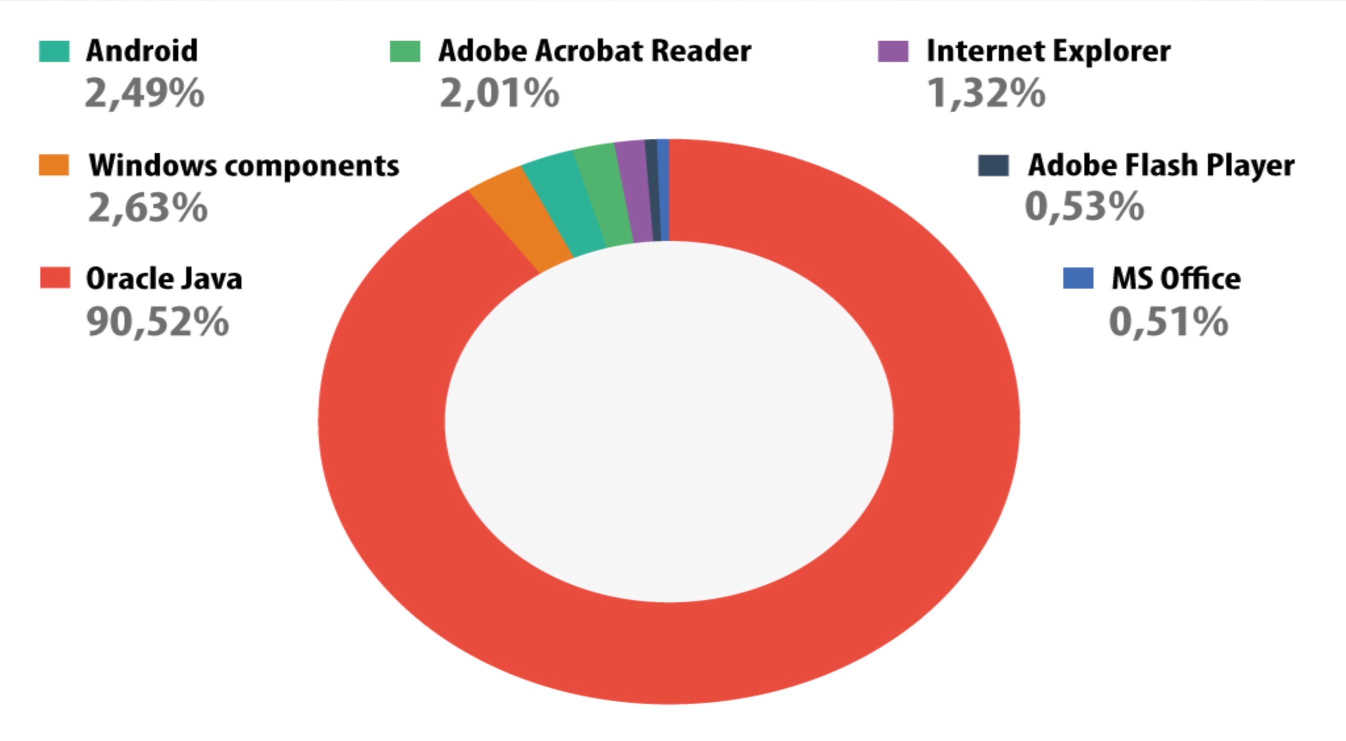
VULNERABILITIES – WHO IS AT RISK?

- 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

Source: Kaspersky Lab 2013 Vulnerabilities Report

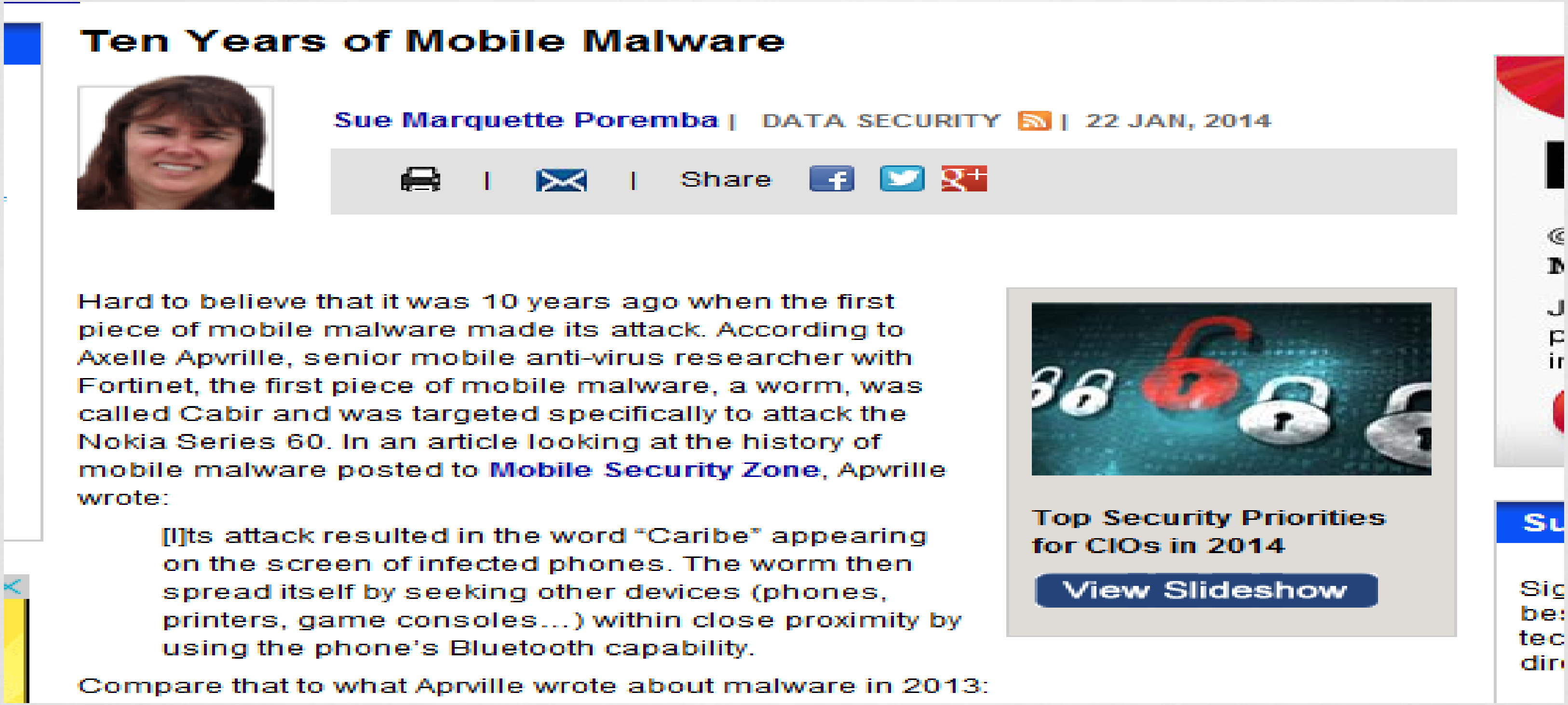
Vulnerable Apps Exploited by "The Bad Guys"



https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

KASPERSKY lab

Mobile Malware 10 Years Old Already



Ten Years of Mobile Malware

Sue Marquette Poremba | DATA SECURITY | 22 JAN, 2014

Hard to believe that it was 10 years ago when the first piece of mobile malware made its attack. According to Axelle Apvrille, 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**, Apvrille wrote:

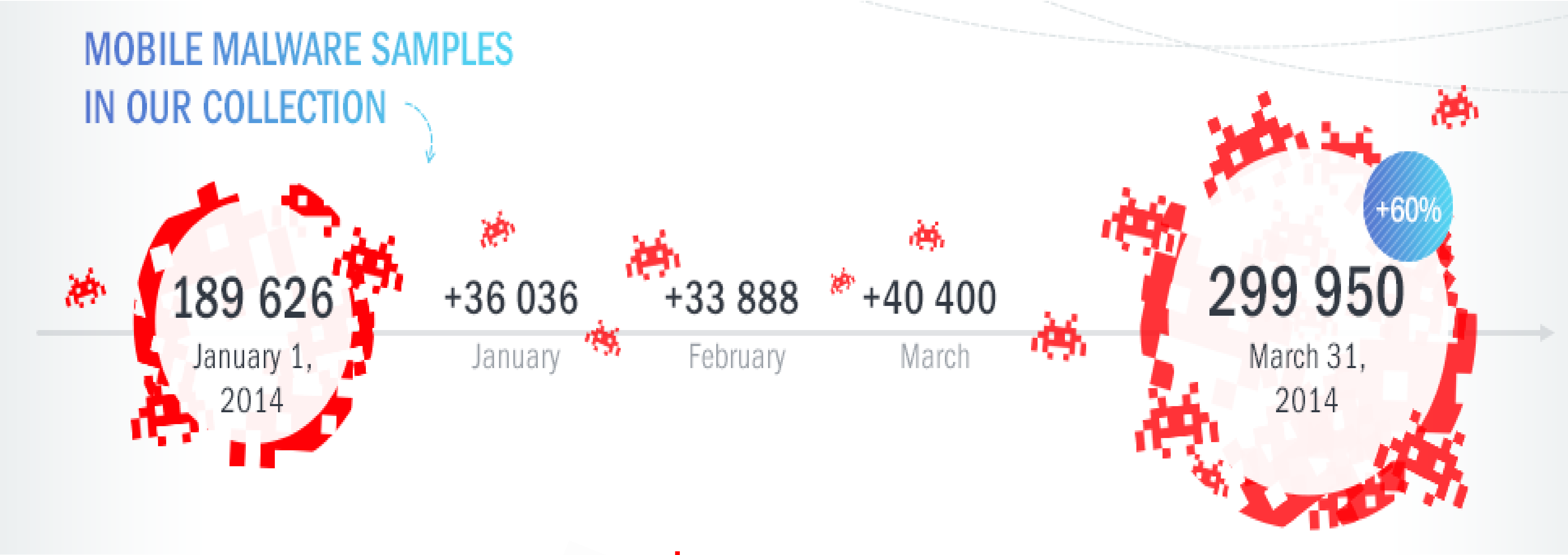
> [I]ts attack resulted in the word "Caribe" appearing on the screen of infected phones. The worm then spread itself by seeking other devices (phones, printers, game consoles…) within close proximity by using the phone's Bluetooth capability.

Compare that to what Aprville wrote about malware in 2013:

Top Security Priorities for CIOs in 2014

http://www.itbusinessedge.com/blogs/data-security/ten-years-of-mobile-malware.html

2014 MOBILE MALWARE STATISTICS



MOBILE MALWARE SAMPLES
IN OUR COLLECTION

189 626
January 1, 2014

+36 036
January

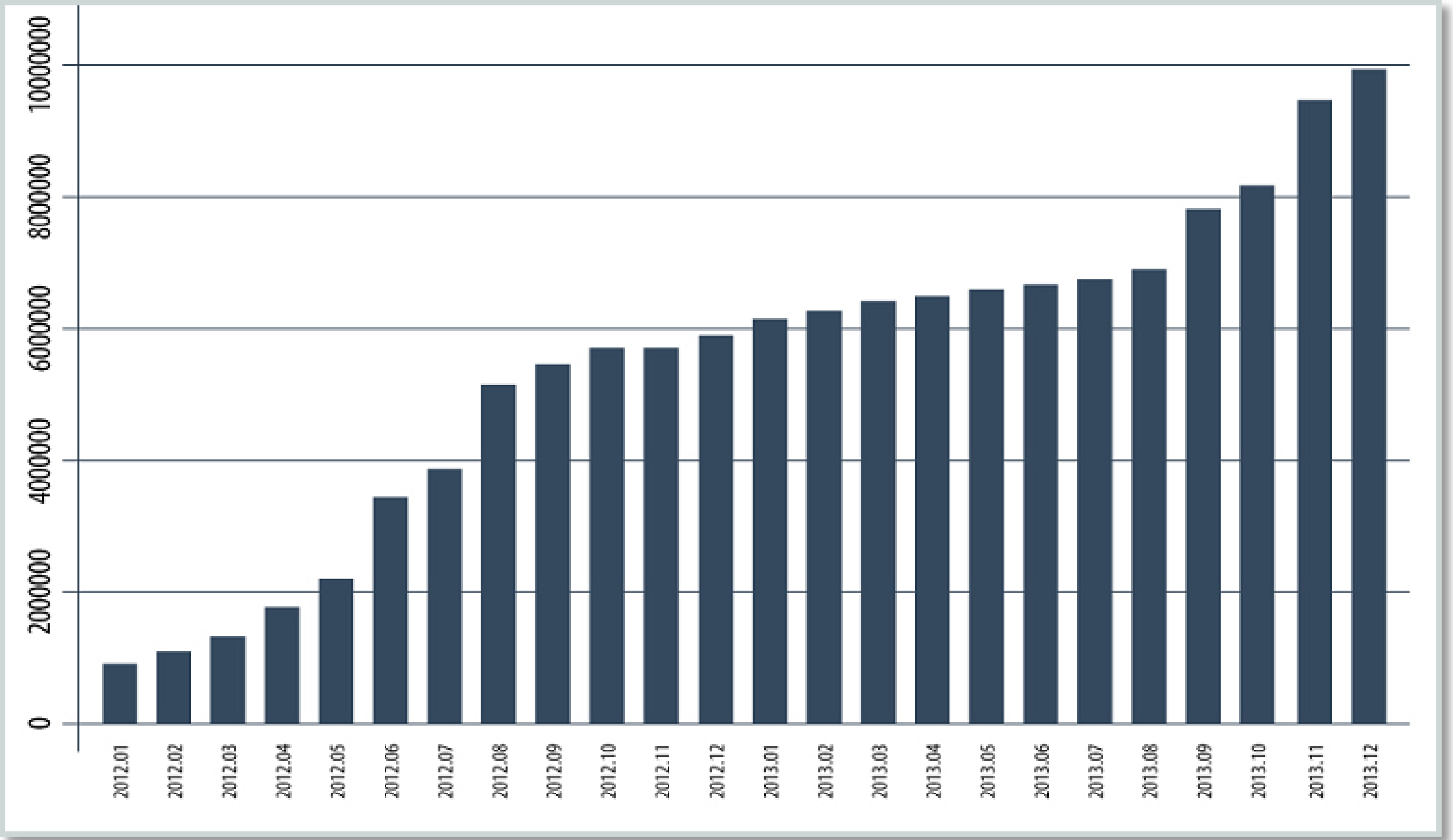
+33 888
February

+40 400
March

299 950
March 31, 2014

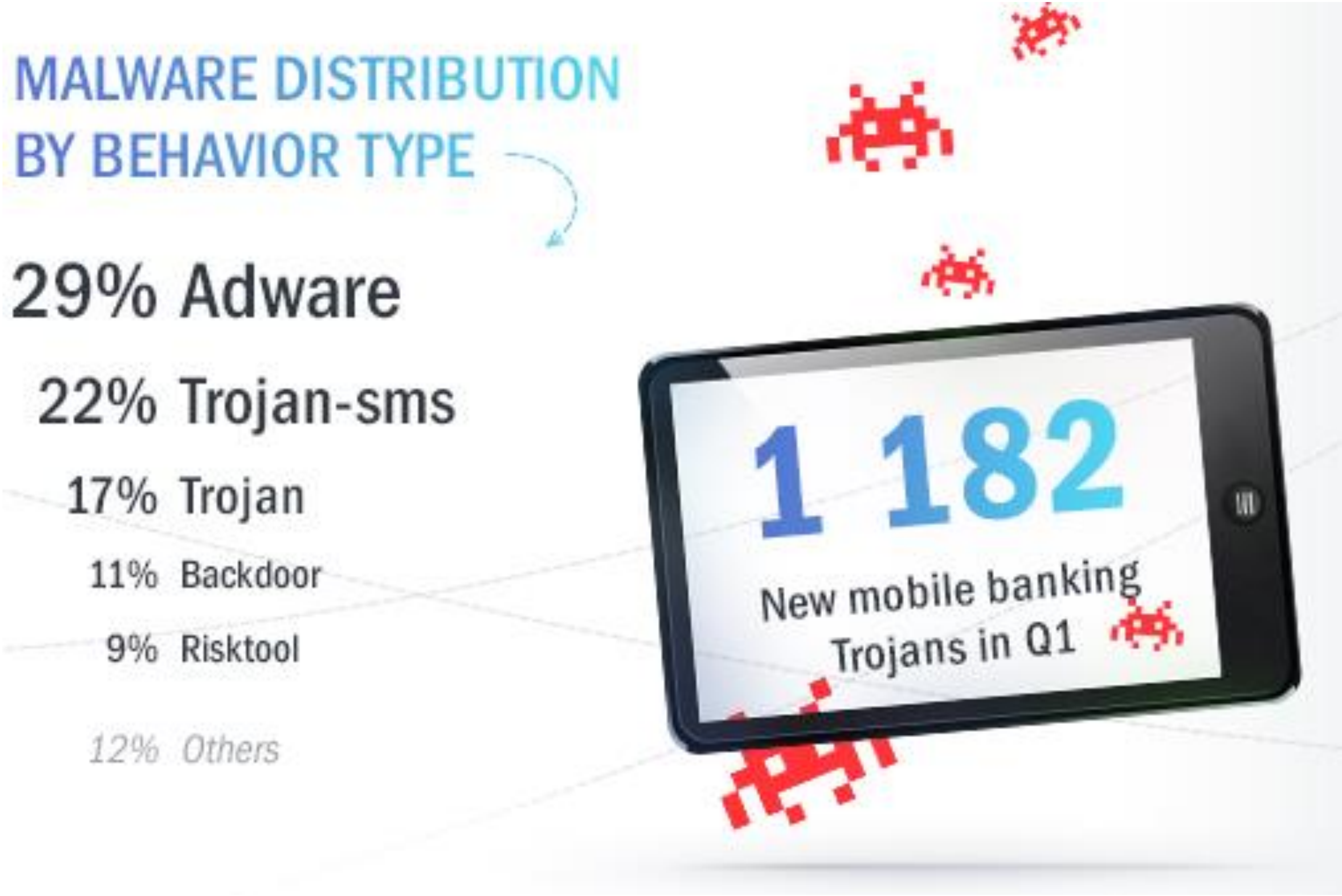
+60%

2013: MOBILE MALWARE INSTALLATION PACKAGES



- In 2013, 3,905,502 installation packages were used by cybercriminals to distribute mobile malware.
- From 2012-2013 we detected approximately 10,000,000 unique malicious installation packages

2014 MALWARE CLASSIFICATION & CAPABILITIES



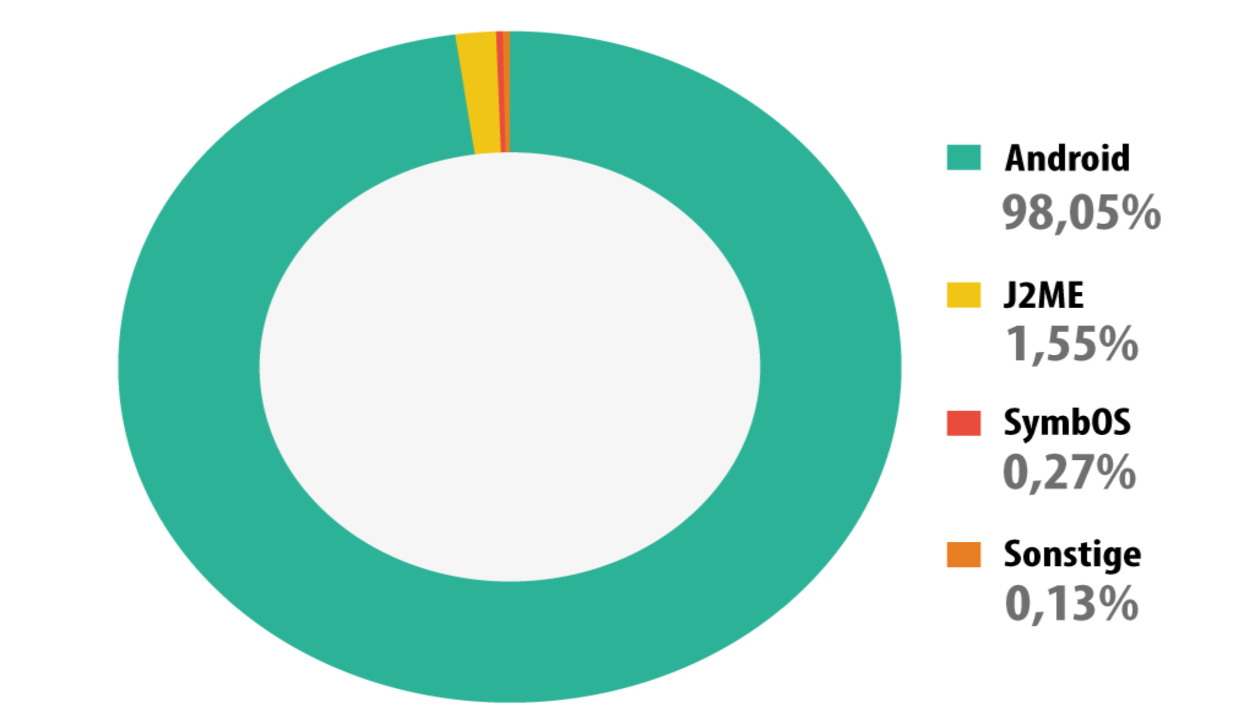
MALWARE DISTRIBUTION BY BEHAVIOR TYPE

29%	Adware
22%	Trojan-sms
17%	Trojan
11%	Backdoor
9%	Risktool
12%	Others

1 182

New mobile banking Trojans in Q1

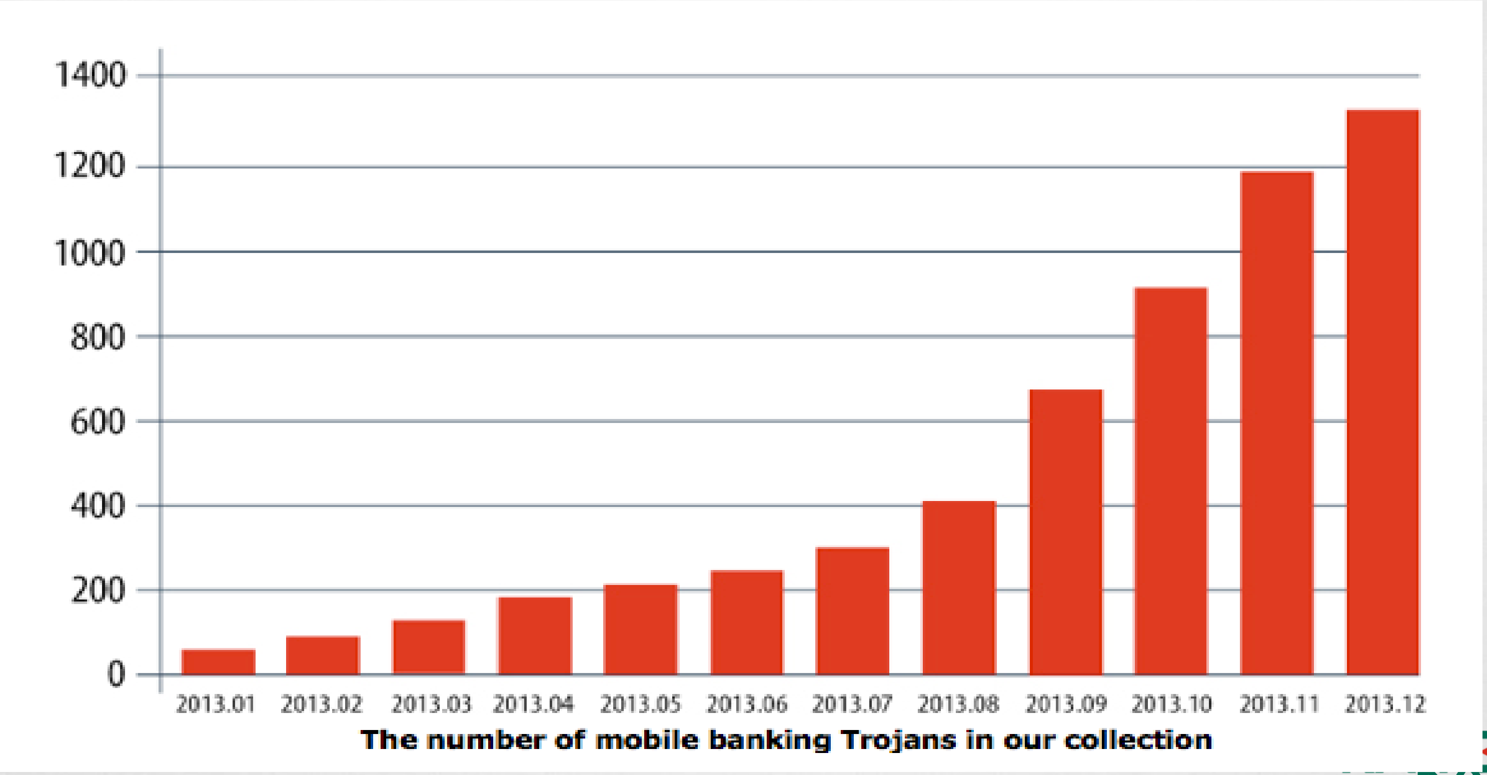
Mobile Malware by Mobile OS



https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

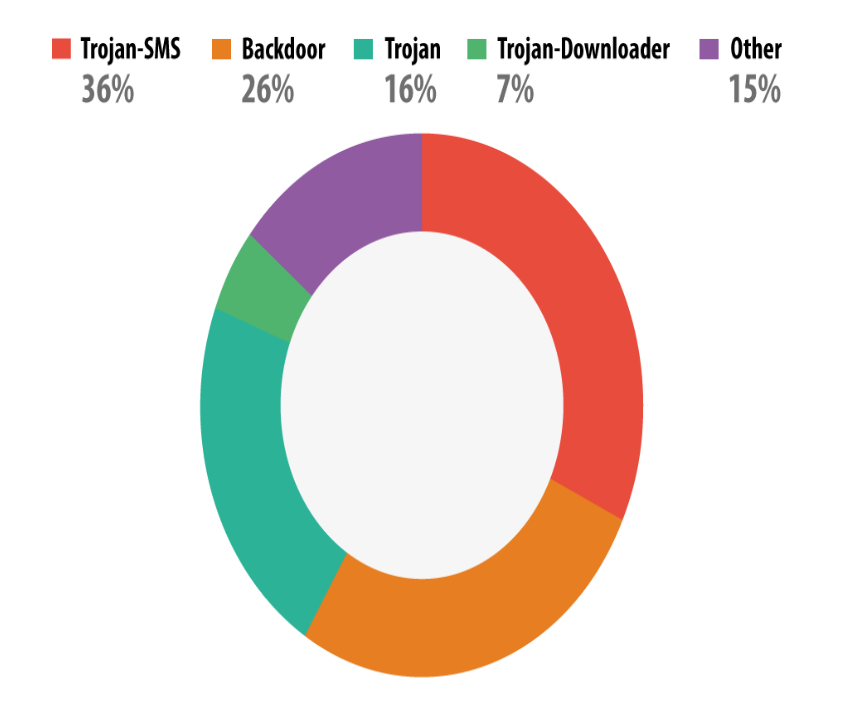
Mobile Banking Trojans

Staggering growth from 67 to 1321 during 2013



The number of mobile banking Trojans in our collection

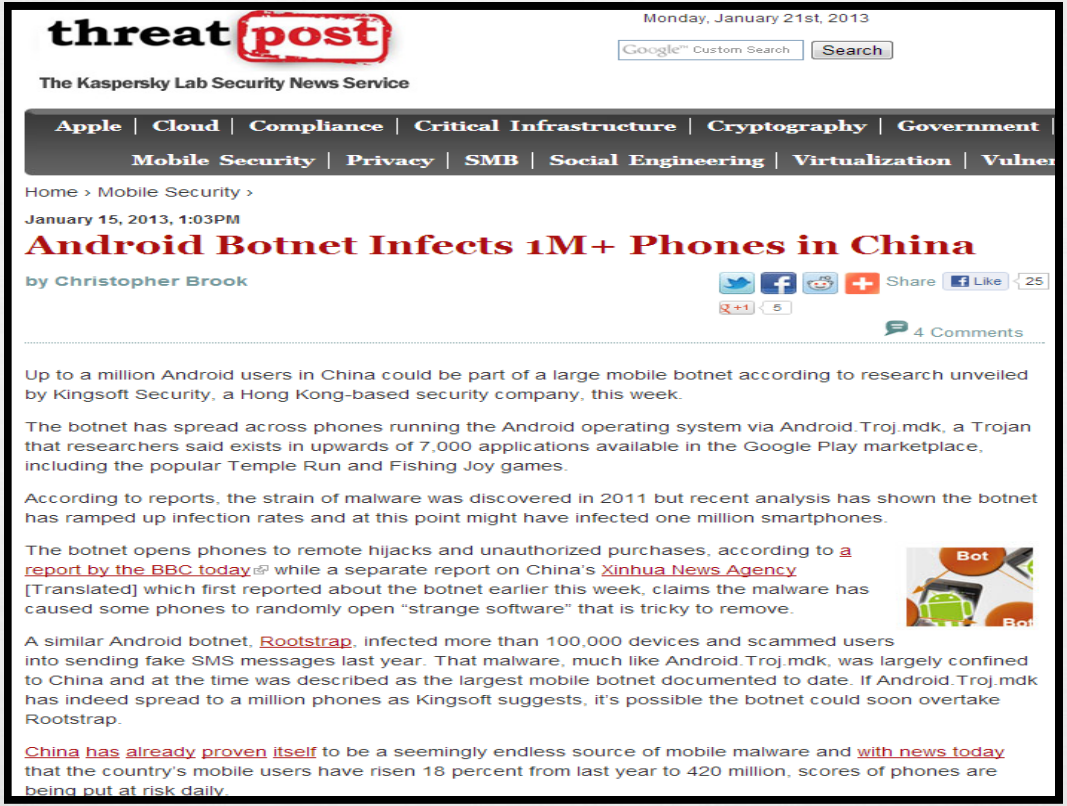
2013 Mobile Malware Breakdown



- All mechanisms used to target PC’s moving to mobile
- Main target to steal money; secondary target to steal personal data
- Majority of Mobile Malware are botnets with rich feature set
- Online Banking the clear target

https://www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013

Large Android Botnet



threatpost

The Kaspersky Lab Security News Service

Monday, January 21st, 2013

Google™ Custom Search
Search
Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government |
Mobile Security | Privacy | SMB | Social Engineering | Virtualization | Vulner
Home › Mobile Security ›

January 15, 2013, 1:03PM

Android Botnet Infects 1M+ Phones in China

by Christopher Brook

Share
Like 25
+1 5
4 Comments

Up to a million Android users in China could be part of a large mobile botnet according to research unveiled by Kingsoft Security, a Hong Kong-based security company, this week.

The botnet has spread across phones running the Android operating system via Android.Troj.mdk, a Trojan that researchers said exists in upwards of 7,000 applications available in the Google Play marketplace, including the popular Temple Run and Fishing Joy games.

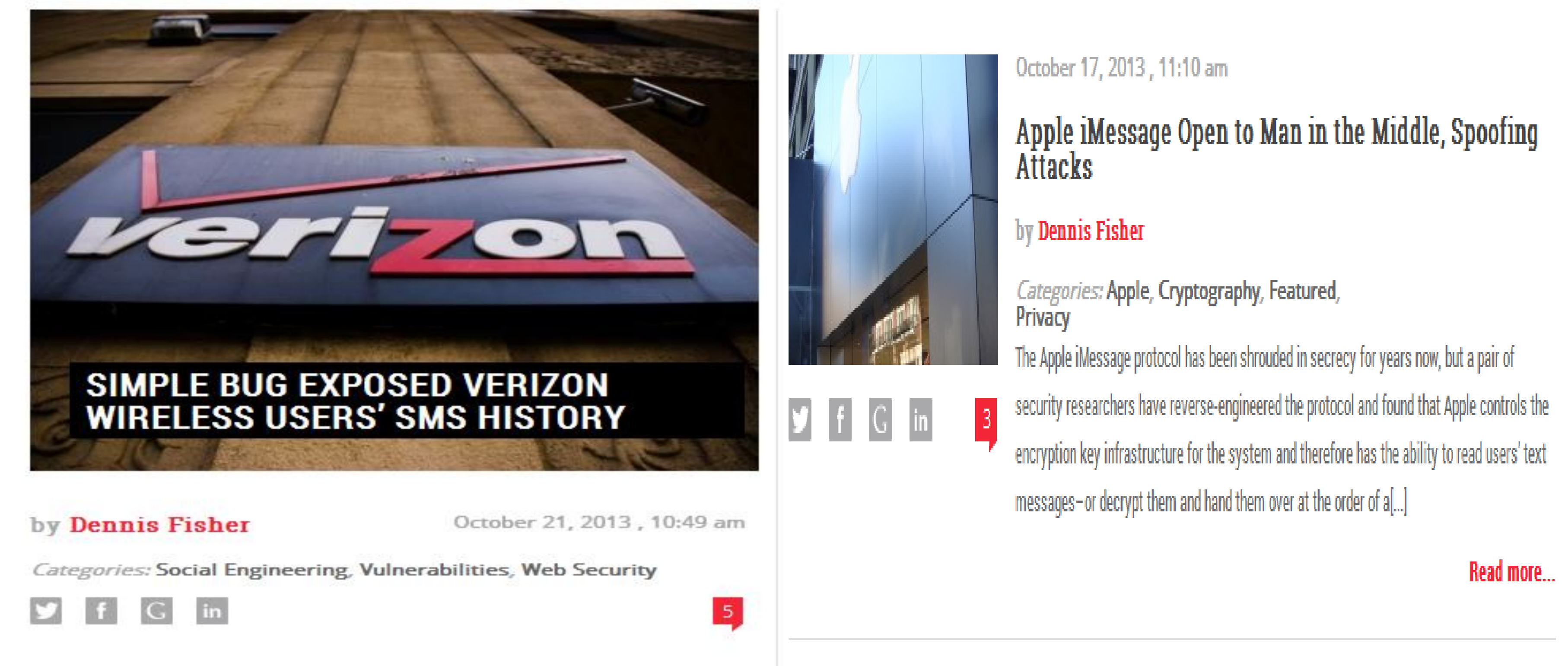
According to reports, the strain of malware was discovered in 2011 but recent analysis has shown the botnet has ramped up infection rates and at this point might have infected one million smartphones.

The botnet opens phones to remote hijacks and unauthorized purchases, according to a report by the BBC today while a separate report on China's Xinhua News Agency [Translated] which first reported about the botnet earlier this week, claims the malware has caused some phones to randomly open "strange software" that is tricky to remove.

A similar Android botnet, Rootstrap, infected more than 100,000 devices and scammed users into sending fake SMS messages last year. That malware, much like Android.Troj.mdk, was largely confined to China and at the time was described as the largest mobile botnet documented to date. If Android.Troj.mdk has indeed spread to a million phones as Kingsoft suggests, it's possible the botnet could soon overtake Rootstrap.

China has already proven itself to be a seemingly endless source of mobile malware and with news today that the country's mobile users have risen 18 percent from last year to 420 million, scores of phones are being put at risk daily.

In the last few months



SIMPLE BUG EXPOSED VERIZON WIRELESS USERS' SMS HISTORY

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

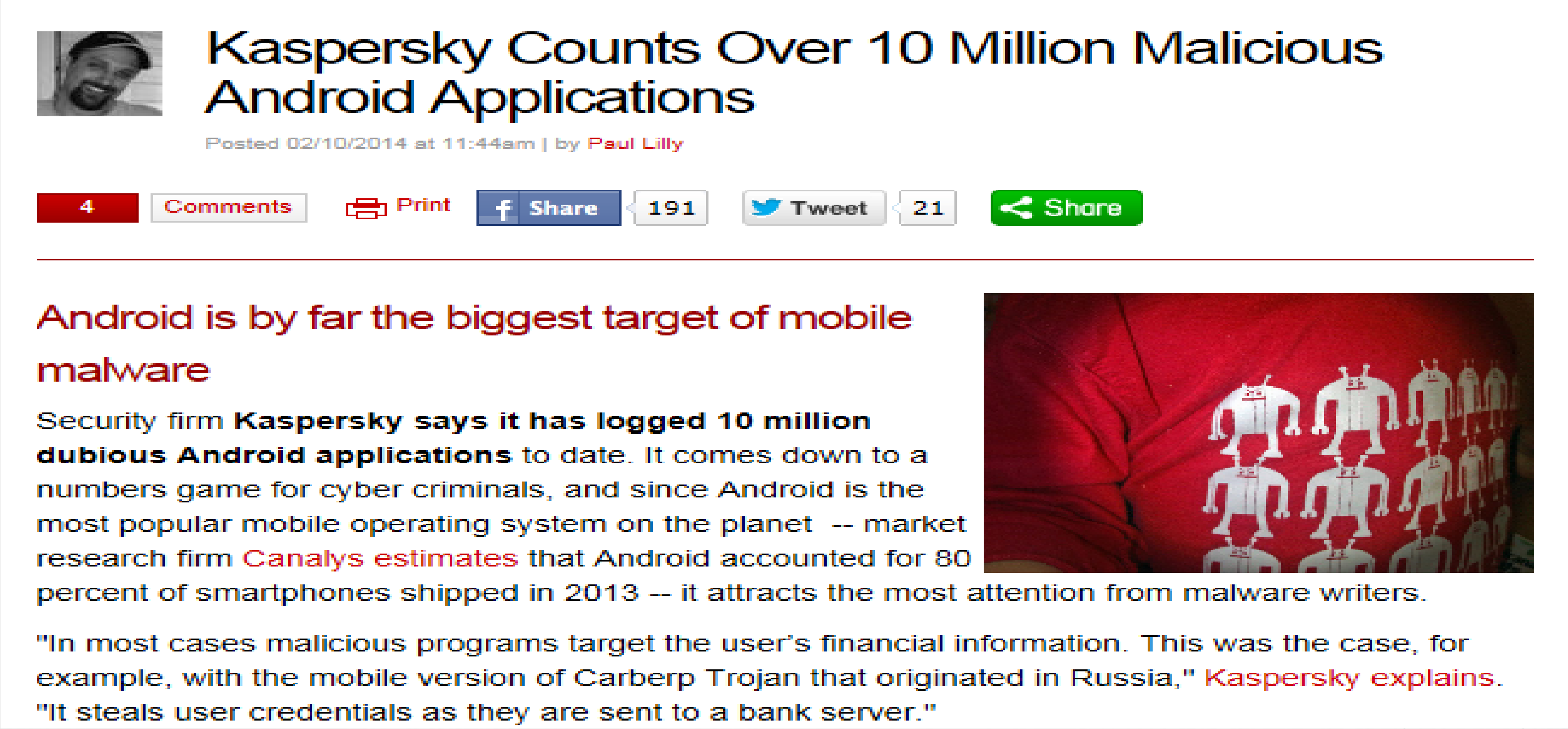
Categories: Apple, Cryptography, Featured, Privacy

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

3

Read more...

Not a Typo!!



Kaspersky Counts Over 10 Million Malicious Android Applications

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

Android is by far the biggest target of mobile malware

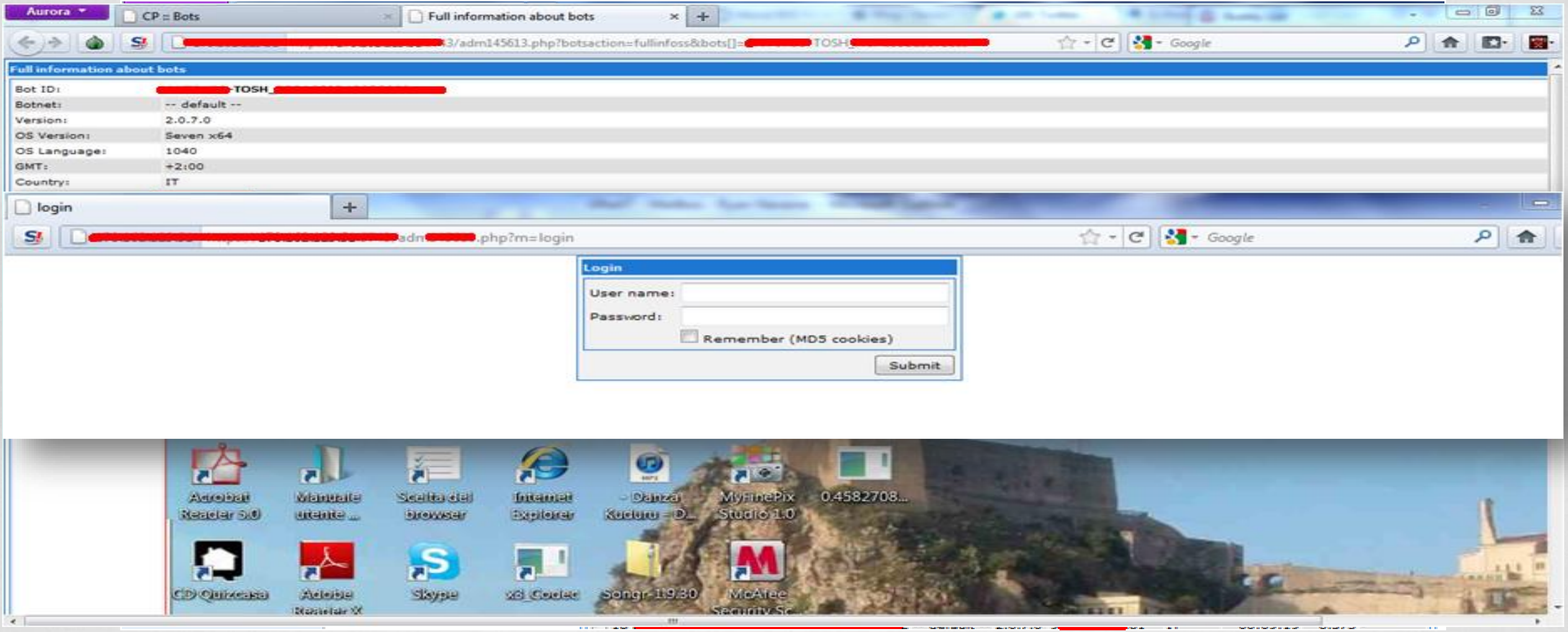
Security firm **Kaspersky says it has logged 10 million dubious Android applications** to date. It comes down to a numbers game for cyber criminals, and since Android is the most popular mobile operating system on the planet -- market research firm Canalys estimates that Android accounted for 80 percent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

http://www.maximumpc.com/kaspersky_counts_over_10_million_malicious_android_applications2014

I LOVE THIS THING!

The DropZone – This is Real



[redacted]3/adm145613.php?botsaction=fullinfoss&bots[]=[redacted]TOSH[redacted]

Full information about bots

Bot ID:	[redacted]-TOSH_[redacted]
Botnet:	-- default --
Version:	2.0.7.0
OS Version:	Seven x64
OS Language:	1040
GMT:	+2:00
Country:	IT

[redacted]adm[redacted].php?m=login

Login

User name:

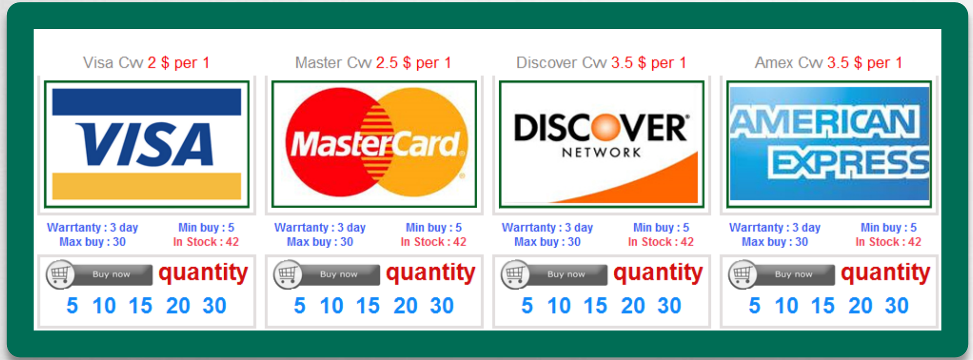
Password:

☐ Remember (MD5 cookies)

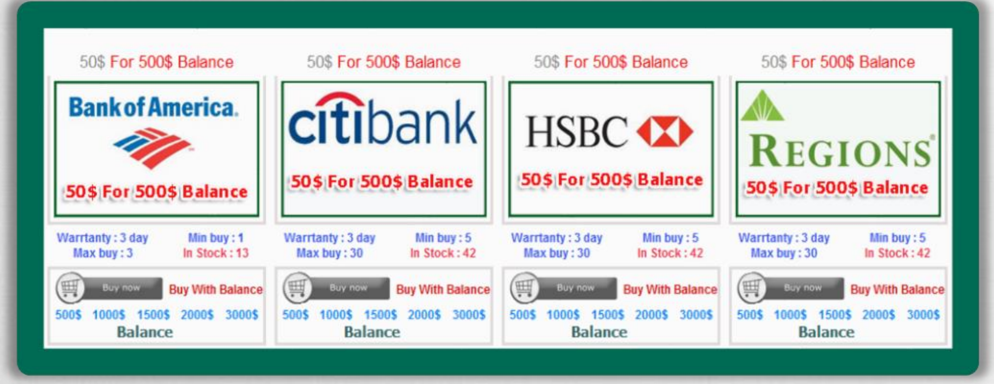
Submit

THE UNDERGROUND MARKET

RESELLING STOLEN CREDIT CARDS

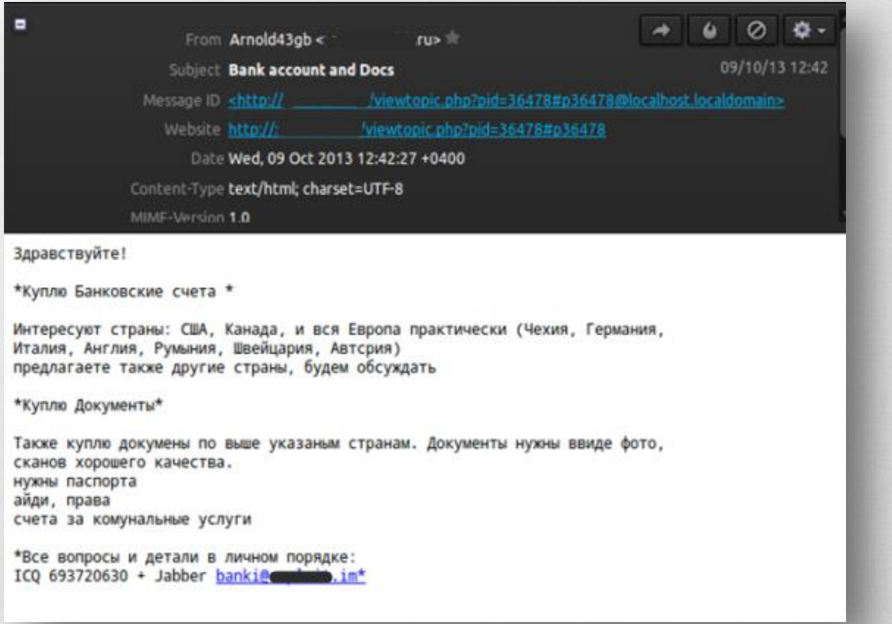


Visa Cvv 2 $ per 1	Master Cvv 2.5 $ per 1	Discover Cvv 3.5 $ per 1	Amex Cvv 3.5 $ per 1
Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42	Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42	Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42	Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42
Buy now quantity 5 10 15 20 30	Buy now quantity 5 10 15 20 30	Buy now quantity 5 10 15 20 30	Buy now quantity 5 10 15 20 30



50$ For 500$ Balance	50$ For 500$ Balance	50$ For 500$ Balance	50$ For 500$ Balance
Bank of America 50$ For 500$ Balance	citibank 50$ For 500$ Balance	HSBC 50$ For 500$ Balance	REGIONS 50$ For 500$ Balance
Warrtanty : 3 day Min buy : 1 Max buy : 3 In Stock : 13	Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42	Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42	Warrtanty : 3 day Min buy : 5 Max buy : 30 In Stock : 42
Buy now Buy With Balance 500$ 1000$ 1500$ 2000$ 3000$ Balance	Buy now Buy With Balance 500$ 1000$ 1500$ 2000$ 3000$ Balance	Buy now Buy With Balance 500$ 1000$ 1500$ 2000$ 3000$ Balance	Buy now Buy With Balance 500$ 1000$ 1500$ 2000$ 3000$ Balance

RESELLING DATABASES OF STOLEN & AGGREGATED FINANCIAL CREDENTIALS

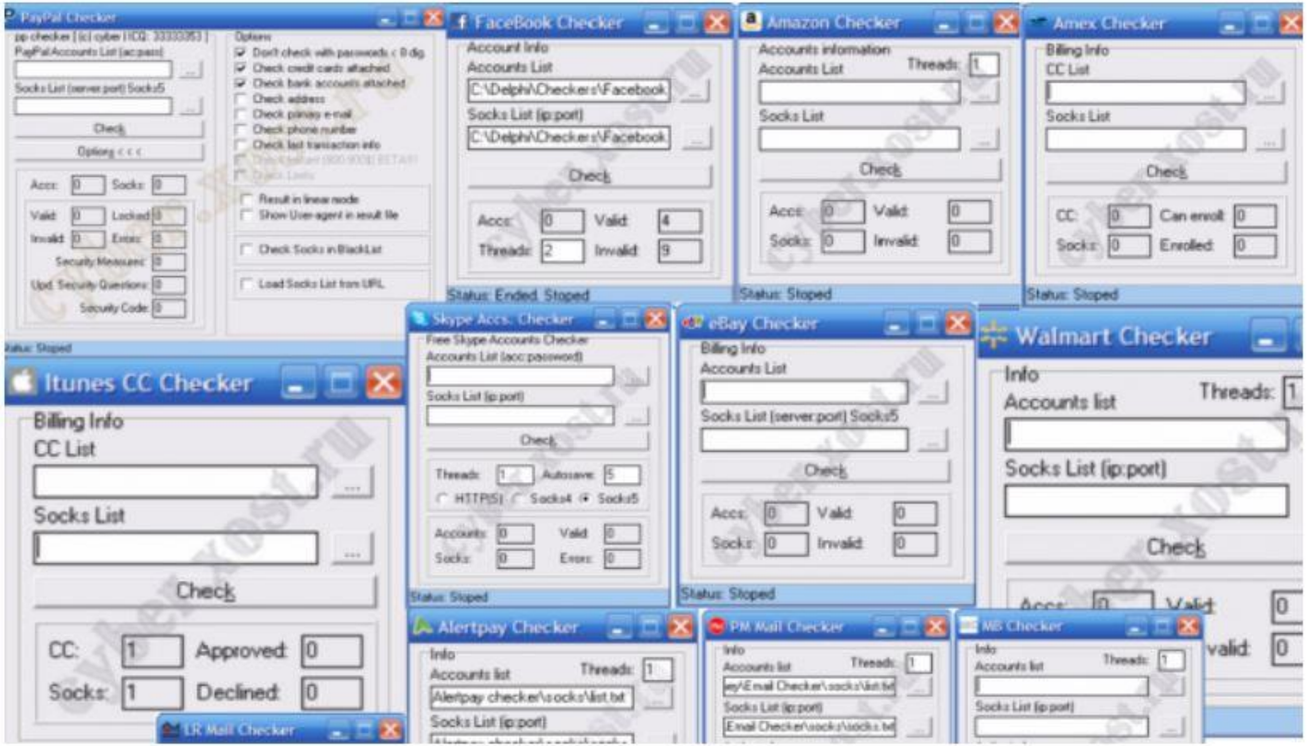


From Arnold43gb < ru>
Subject **Bank account and Docs** 09/10/13 12:42
Message ID <http:// /viewtopic.php?pid=36478#p36478@localhost.localdomain>
Website http:// /viewtopic.php?pid=36478#p36478
Date Wed, 09 Oct 2013 12:42:27 +0400
Content-Type text/html; charset=UTF-8
MIMF-Version 1.0

```
Здравствуйте!

*Куплю Банковские счета *

Интересуют страны: США, Канада, и вся Европа практически (Чехия, Германия,
Италия, Англия, Румыния, Швейцария, Автсрия)
предлагаете также другие страны, будем обсуждать

*Куплю Документы*

Также куплю докумены по выше указаным странам. Документы нужны ввиде фото,
сканов хорошего качества.
нужны паспорта
айди, права
счета за комунальные услуги

*Все вопросы и детали в личном порядке:
ICQ 693720630 + Jabber banki@[redacted].im*
```

KASPERSKY lab

The Value of a Hacked PC



PayPal Checker
pp checker [(c) cyber ICQ: 33333353]
PayPal Accounts List (ac:pass)
Socks List (server:port) Socks5
Options
☑ Don't check with passwords < 8 dig
☑ Check credit cards attached
☑ Check bank accounts attached
□ Check address
□ Check primary e-mail
□ Check phone number
□ Check last transaction info
□ Result in linear mode
□ Show User-agent in result file
□ Check Socks in BlackList
□ Load Socks List from URL
Accs: 0 Socks: 0
Valid: 0 Locked: 0
Invalid: 0 Errors: 0
Security Measures: 0
Upd. Security Questions: 0
Security Code: 0
Status: Stoped

FaceBook Checker
Account Info
Accounts List: C:\Delphi\Checkers\Facebook
Socks List (ip:port): C:\Delphi\Checkers\Facebook
Accs: 0 Valid: 4
Threads: 2 Invalid: 9
Status: Ended. Stoped

Amazon Checker
Accounts information
Threads: 1
Accs: 0 Valid: 0
Socks: 0 Invalid: 0
Status: Stoped

Amex Checker
Billing Info
CC: 0 Can enroll: 0
Socks: 0 Enrolled: 0
Status: Stoped

Itunes CC Checker
Billing Info
CC: 1 Approved: 0
Socks: 1 Declined: 0

Skype Accs. Checker
Free Skype Accounts Checker
Accounts List (acc:password)
Socks List (ip:port)
Threads: 1 Autosave: 5
○ HTTP(S) ○ Socks4 ● Socks5
Accounts: 0 Valid: 0
Socks: 0 Errors: 0
Status: Stoped

eBay Checker
Billing Info
Accounts List
Socks List (server:port) Socks5
Accs: 0 Valid: 0
Socks: 0 Invalid: 0
Status: Stoped

Walmart Checker
Info
Threads: 1
Accs: 0 Valid: 0
Invalid: 0

Alertpay Checker
Info
Threads: 1
Accounts list: Alertpay checker\socks\list.txt
Socks List (ip:port)

PM Mail Checker
Info
Threads: 1
Accounts list: ey\Email Checker\socks\list.txt
Socks List (ip:port): Email Checker\socks\socks.txt

MB Checker
Info
Threads: 1
Accounts list
Socks List (ip:port)

LR Mail Checker

Account checking tools sold on the cybercriminal underground by one vendor.

http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Be Ready for What's Next

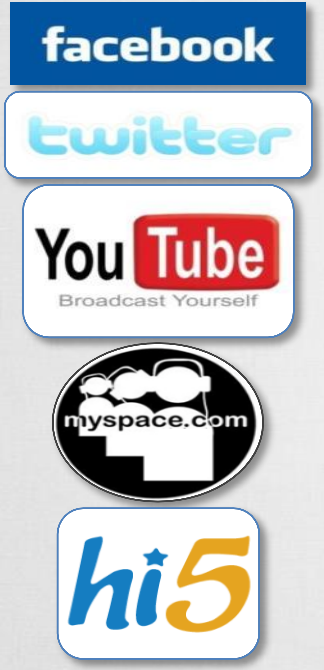
5 Ways IT may Be an Accomplice

1) Migration Myopia

Believing that company data never finds its way to home systems

2) Social Media Mania

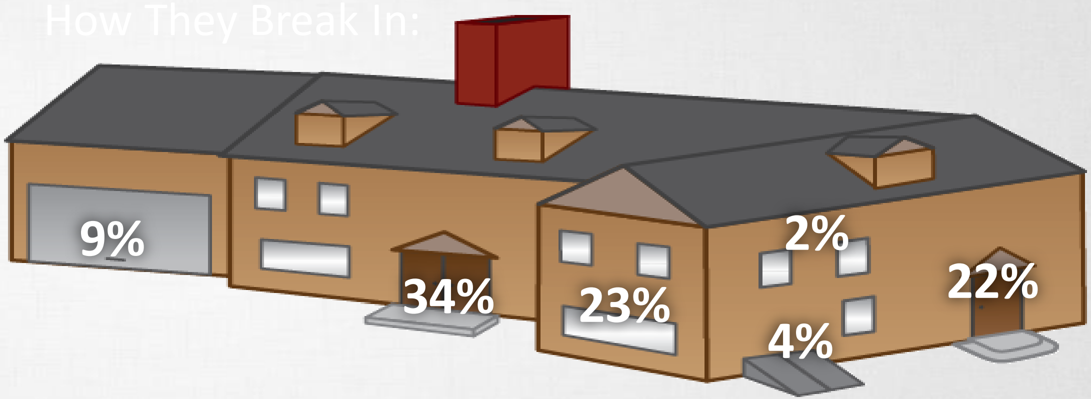
Adopting Social Media Without Protection



3) Attention Misdirection

Focusing on Protection 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 Gun
Police Insurance

Source: "Data @ Risk" by David H. Stelzl

4) Awareness Deficit

Failing To Foster A Culture Of Awareness

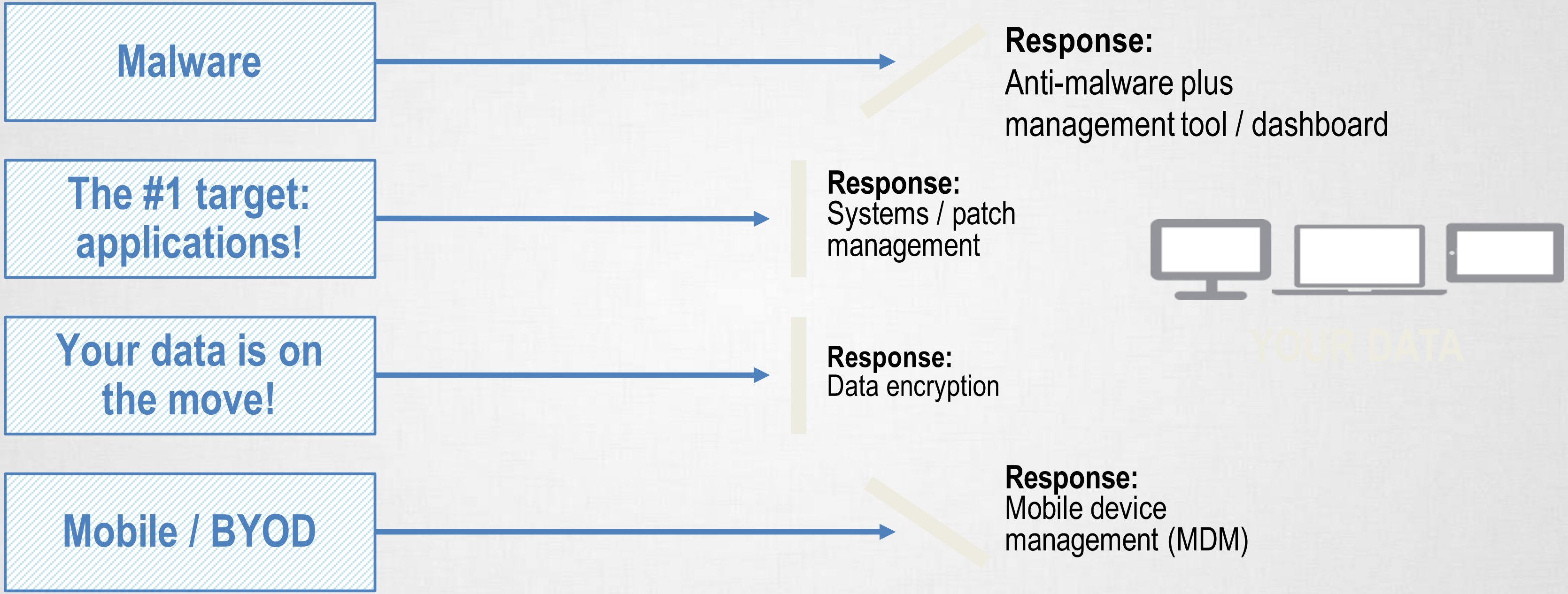
5) Reliance on Compliance

- Compliance… just one step north of negligence.

Josh Corman, the 451 Group

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

The impact on IT security



Malware

Response:
Anti-malware plus
management tool / dashboard

The #1 target: applications!

Response:
Systems / patch
management

Your data is on the move!

Response:
Data encryption

Mobile / BYOD

Response:
Mobile device
management (MDM)

The impact on IT security

Malware

Response:
Anti-malware plus
management tool / dashboard

The #1 target:
applications!

Response:
Systems / patch

This is complexity

COMPLEXITY IS THE ENEMY OF IT SECURITY

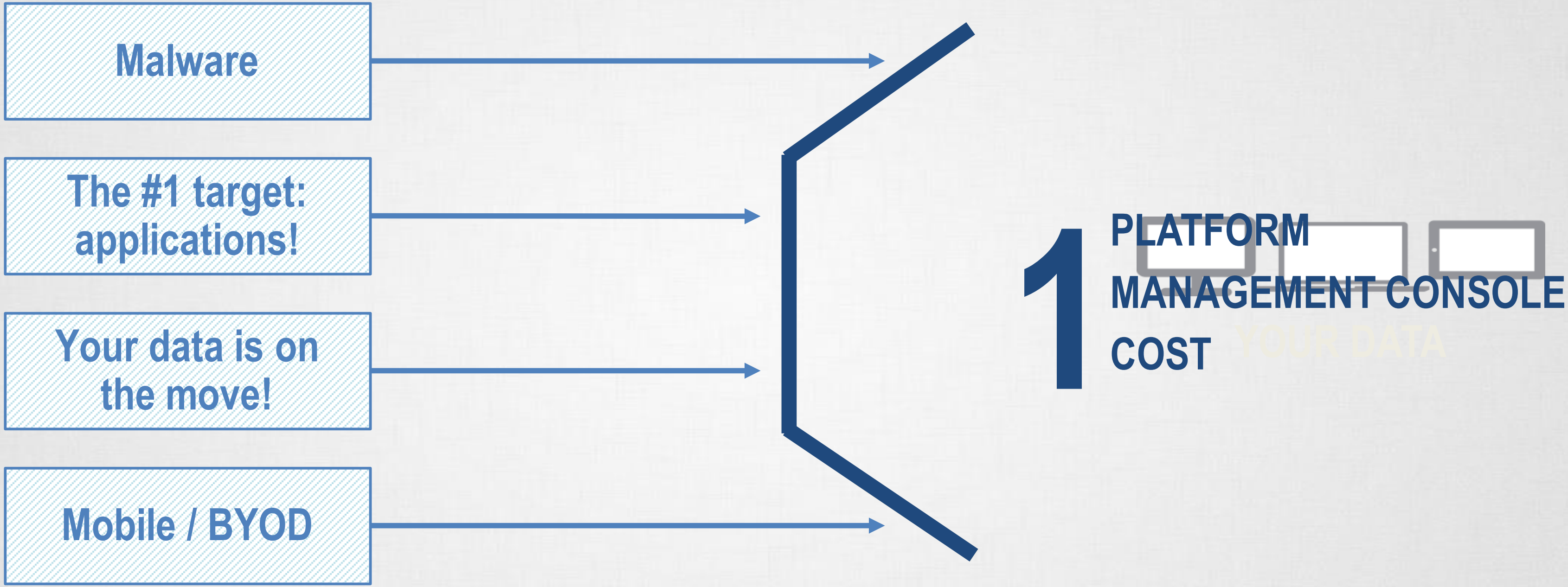
Your data is on
the move!

Response:
Data encryption

Mobile / BYOD

Response:
Mobile device
management (MDM)

What if?



Malware

The #1 target: applications!

Your data is on the move!

Mobile / BYOD

1

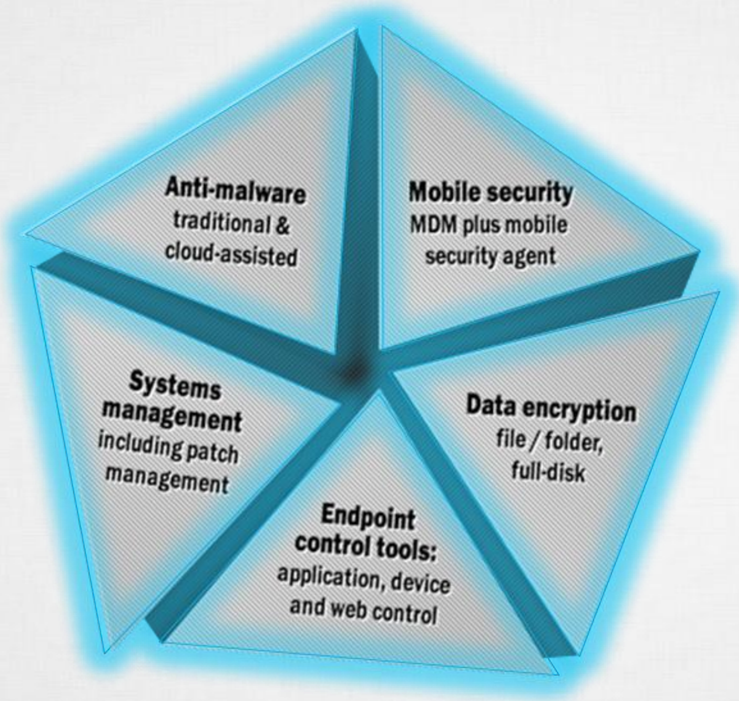
PLATFORM

MANAGEMENT CONSOLE

COST

KASPERSKY SECURITY FOR BUSINESS

- Physical
- Virtual
- Mobile



Anti-malware
traditional &
cloud-assisted

Mobile security
MDM plus mobile
security agent

Systems management
including patch
management

Data encryption
file / folder,
full-disk

Endpoint control tools:
application, device
and web control

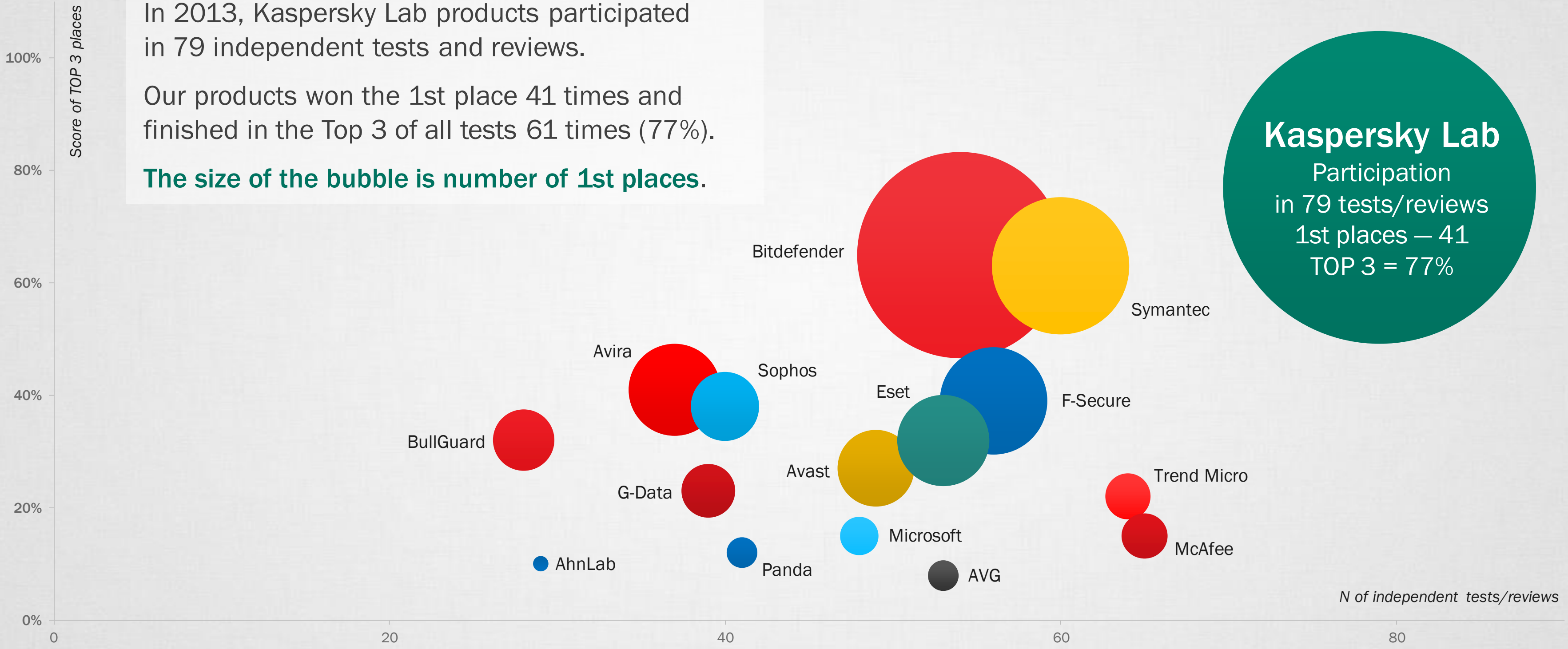
- Vulnerability Scan
- Patch Management
- Remote Tools
- License Management
- System Provisioning
- NAC Network Admission Control

OUR LEADERSHIP IS PROVEN BY INDEPENDENT TESTS

In 2013, Kaspersky Lab products participated in 79 independent tests and reviews.

Our products won the 1st place 41 times and finished in the Top 3 of all tests 61 times (77%).

The size of the bubble is number of 1st places.



Kaspersky Lab
Participation
in 79 tests/reviews
1st places — 41
TOP 3 = 77%