

Kaspersky Lab Threats Update

Jesmond Chang
jesmond.chang@kaspersky.com





Kaspersky Lab Threats Update

Jesmond Chang

jesmond.chang@kaspersky.com



Mobile Malware Evolution

Rootcon 7

2013

Jesmond Chang

Corporate Communications Manager,

Kaspersky Lab Southeast Asia

KASPERSKY lab

Mobile Malware Evolution
Rootcon 7
2013

Jesmond Cheng
Corporate Communications Manager,
Kaspersky Lab Southeast Asia

KASPERSKY lab



10 Fast Facts about Kaspersky Lab

- 1 Founded in 1997 by a group of IT security experts headed by Eugene Kaspersky
- 2 Headed by Chairman, CEO and Co-founder, Eugene Kaspersky
- 3 Provides innovative security software and solutions for home and business users
- 4 Operates in almost 200 countries and territories with regional offices in 30 countries
- 5 Provides protection for over 300 million people worldwide
- 6 Employs more than 2,700 highly-qualified specialists
- 7 One of the 4 biggest endpoint security vendors in the world*
- 8 Named a "Leader" in the Gartner Magic Quadrant for Endpoint Protection Platforms**
- 9 Averages more than 20 million product activations per year
- 10 An official sponsor of the Scuderia Ferrari Formula One racing team

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2011. The rating was published in the IDC report "Worldwide Endpoint Security 2012-2016 Forecast and 2011 Vendor Shares (IDC #235930, July 2012). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2011.

** Gartner, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, John Girard, Neil MacDonald, January 2, 2013. The report is available at Kaspersky Lab upon request.

KASPERSKY lab

Mobile Malware Evolution
Rootcon 7
2013

Jesmond Cheng
Corporate Communications Manager,
Kaspersky Lab Southeast Asia

KASPERSKY lab



Sponsorship Projects



SCUDERIA FERRARI SPONSORSHIP

Kaspersky Lab first started cooperating with Scuderia Ferrari back in 2010, and the partnership has blossomed since then. During the 2012 and 2013 F1 racing seasons the Kaspersky Lab logo features on the car nose cones and sides, and on the drivers' overalls and team uniforms.



INVOLVING BRAND AMBASSADORS

As well as our global sponsorships, we try to build partnerships with local celebrities in the regions and cultures where we work like the legend of cricket Sachin Tendulkar and Taiwanese superstar Jay Chou.



SPONSORING OF GEOGRAPHIC EXPEDITIONS

Kaspersky Lab has sponsored a number of geographic expeditions to the world's most remote regions. The latest one, the Kaspersky One Transantarctic Expedition, saw renowned British explorer Felicity Aston making a 59-day, 1700 km journey across Antarctica via the South Pole.

KASPERSKY lab

Mobile Malware Evolution
Rootcon 7
2013

Jesmond Cheng
Corporate Communications Manager,
Kaspersky Lab Southeast Asia

KASPERSKY lab



What?



Evolution of Malware

1994

One new virus every hour



2006

One new virus every minute



2011

One new virus every second



Kaspersky Lab

is currently processing

200,000

unique malware samples

EVERY DAY

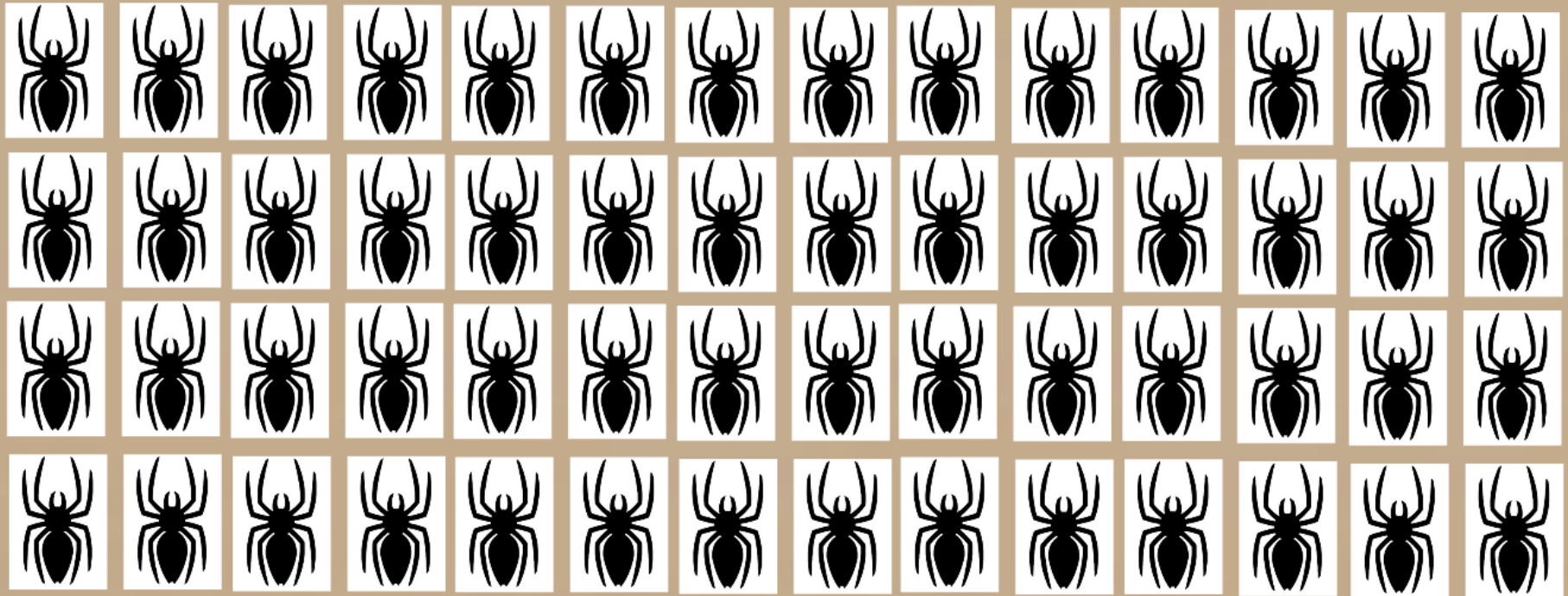
1994

One new virus every hour



2006

One new virus every minute



2011

One new virus every second

Or 70,000 samples/day

Or 70.000 samples/day

Kaspersky Lab
is currently processing
200.000

unique malware samples
EVERY DAY

What?



Evolution of Malware

1994

One new virus every hour



2006

One new virus every minute



2011

One new virus every second



200,000 samples/day

Kaspersky Lab

is currently processing

200,000

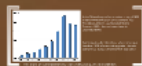
unique malware samples

EVERY DAY



Technical factors

Software Vulnerabilities



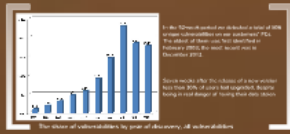
Advance Persistent Threats





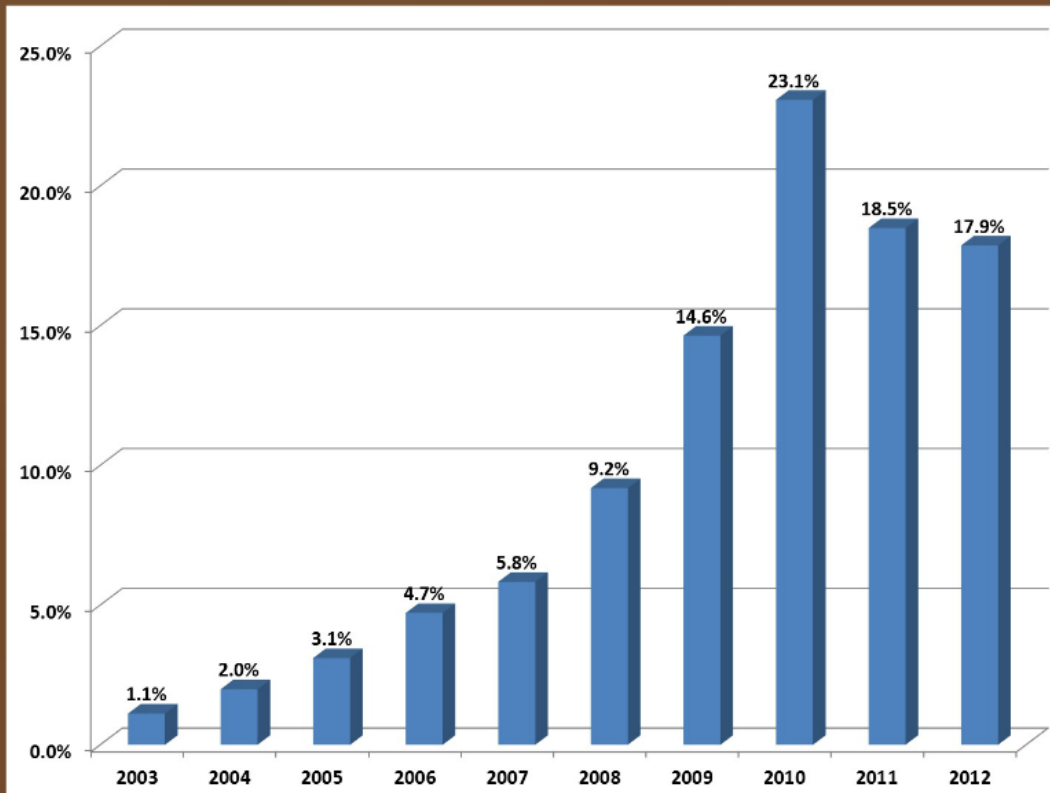
Technical factors

Software Vulnerabilities



Advance Persistent Thr

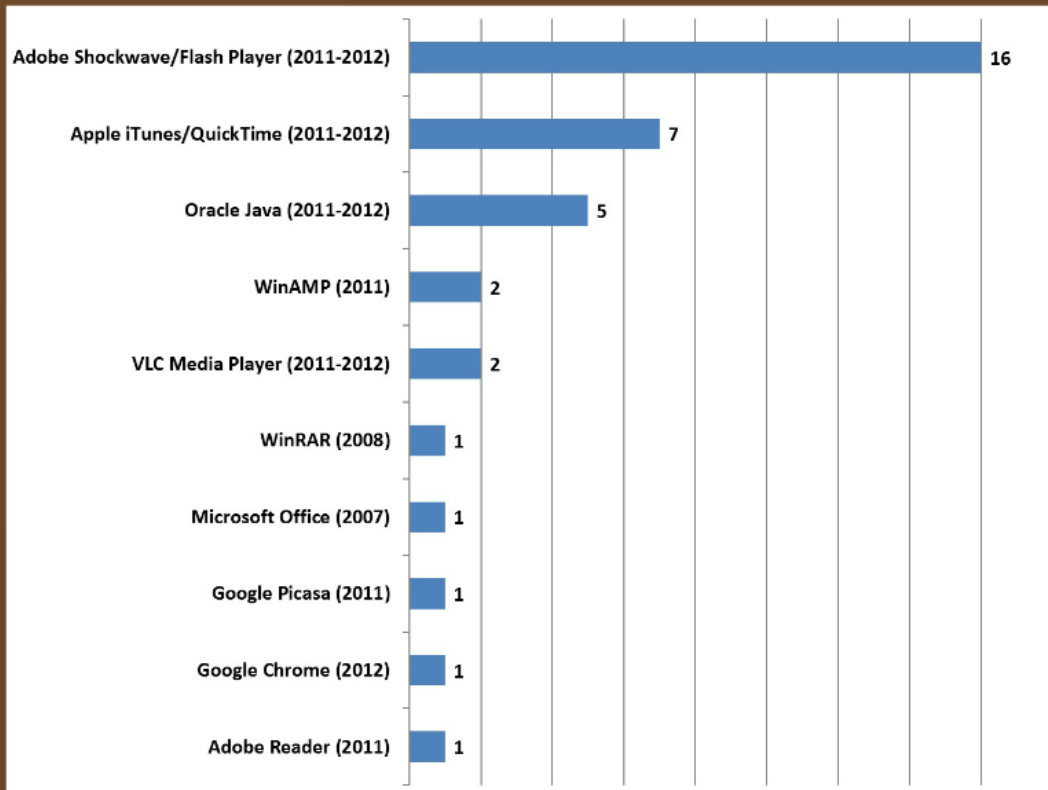




The share of vulnerabilities by year of discovery, all vulnerabilities

In the 52-week period we detected a total of 806 unique vulnerabilities on our customers' PCs. The oldest of them was first identified in February 2003; the most recent was in December 2012.

Seven weeks after the release of a new version less than 30% of users had upgraded, despite being in real danger of having their data stolen



The top 37 vulnerabilities are found in 10 different product families. The most vulnerable products are Adobe Shockwave/Flash Player, Apple iTunes/QuickTime and Oracle Java. Between them, they account for 28 vulnerabilities among those found on 10% or more of users' PCs during 2012.

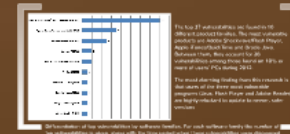
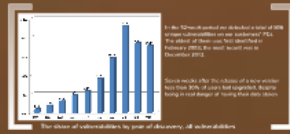
The most alarming finding from this research is that users of the three most vulnerable programs (Java, Flash Player and Adobe Reader) are highly reluctant to update to newer, safer versions

Differentiation of top vulnerabilities by software families. For each software family the number of top vulnerabilities is given, along with the time period when those vulnerabilities were discovered



Technical factors

Software Vulnerabilities



Advance Persistent Thr



The source of statistics: Kaspersky Security Network

Kaspersky Security Network (KSN) is a global exchange of information about malicious activity involving millions of users of Kaspersky Lab products from 213 countries around the world.

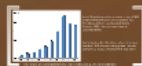
It is important to note that we do not collect any private data using KSN.





Technical factors

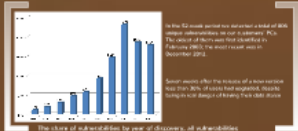
Software Vulnerabilities



Advance Persistent Threats



Software Vulnerabilities



Advance Persistent Threats



FLAME

DUQU

GAUSS

STUINET

FLAME is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

DUQU is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

GAUSS is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

STUINET is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

FLAME

DUQU

GAUSS

STUINET

FLAME is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

DUQU is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

GAUSS is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

STUINET is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

FLAME

DUQU

GAUSS

STUINET

FLAME is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

DUQU is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

GAUSS is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

STUINET is a malware family that targets Linux systems. It is a sophisticated malware that can steal sensitive information, including passwords, credit card numbers, and other personal data. It is designed to be persistent and difficult to detect.

Cyber weapons

6 cyber weapons are known – 5 were active in 2012.



DUQU

DUQU



CLASSIFICATION

Espionage Program



DETECTION TIME

September 2011



ACTIVE SINCE

August 2007

FACTS OF DUQU:

- built on same platform as Stuxnet (Tilded)
- destroys all traces of activity
- core module never detected
- no further modifications discovered since Feb. 2012

FLAME



CLASSIFICATION

Espionage Program



DETECTION TIME

May 2012



ACTIVE SINCE

2008

FACTS OF FLAME:

- complex set of operations, including analyzing the network traffic, taking screenshots, recording voice communications, keystroke logging, etc.
- can download extra modules to victim computers
- 20 extension modules detected
- sophisticated toolkit, far more complex than Duqu
- module used in 2009 for the Stuxnet worm
- module in Flame used in Stuxnet 2009 version shows: developers of Flame and Stuxnet/Duqu collaborated at least once



Flame incorporated **a unique functionality** to propagate itself across the LAN; to that end, **it intercepted Windows update requests** and **substituted** them with its own module signed with a Microsoft certificate. Analysis of this certificate revealed **a unique cryptographic attack** which enabled cybercriminals to generate their **own bogus certificate** that was **indistinguishable** from a legal one.

MINIFLAME



CLASSIFICATION

Espionage Program



DETECTION TIME

October 2012



ACTIVE SINCE

Aug./Sept. 2011

FACTS OF MINIFLAME:

- created on the Flame platform
- miniature fully-fledged spyware module
- used for highly-targeted attacks against select victims
- can be implemented as stand-alone malware or as a plug-in for Flame



Remarkably, miniFlame **can also be used in conjunction with Gauss**, another spyware program. MiniFlame's primary purpose is to function as a **backdoor on infected systems**, enabling attackers to directly manage them.

GAUSS



CLASSIFICATION

Espionage Program



DETECTION TIME

July 2012



ACTIVE SINCE

Aug./Sept. 2011

FACTS OF GAUSS:

- sophisticated toolkit for conducting cyber espionage
- implemented by the same group that created the Flame platform
- modules perform a variety of functions



Intercept cookie-files and passwords in the web browser



Infect USB storage drives to steal data



Steal banking system accesses in the Middle East

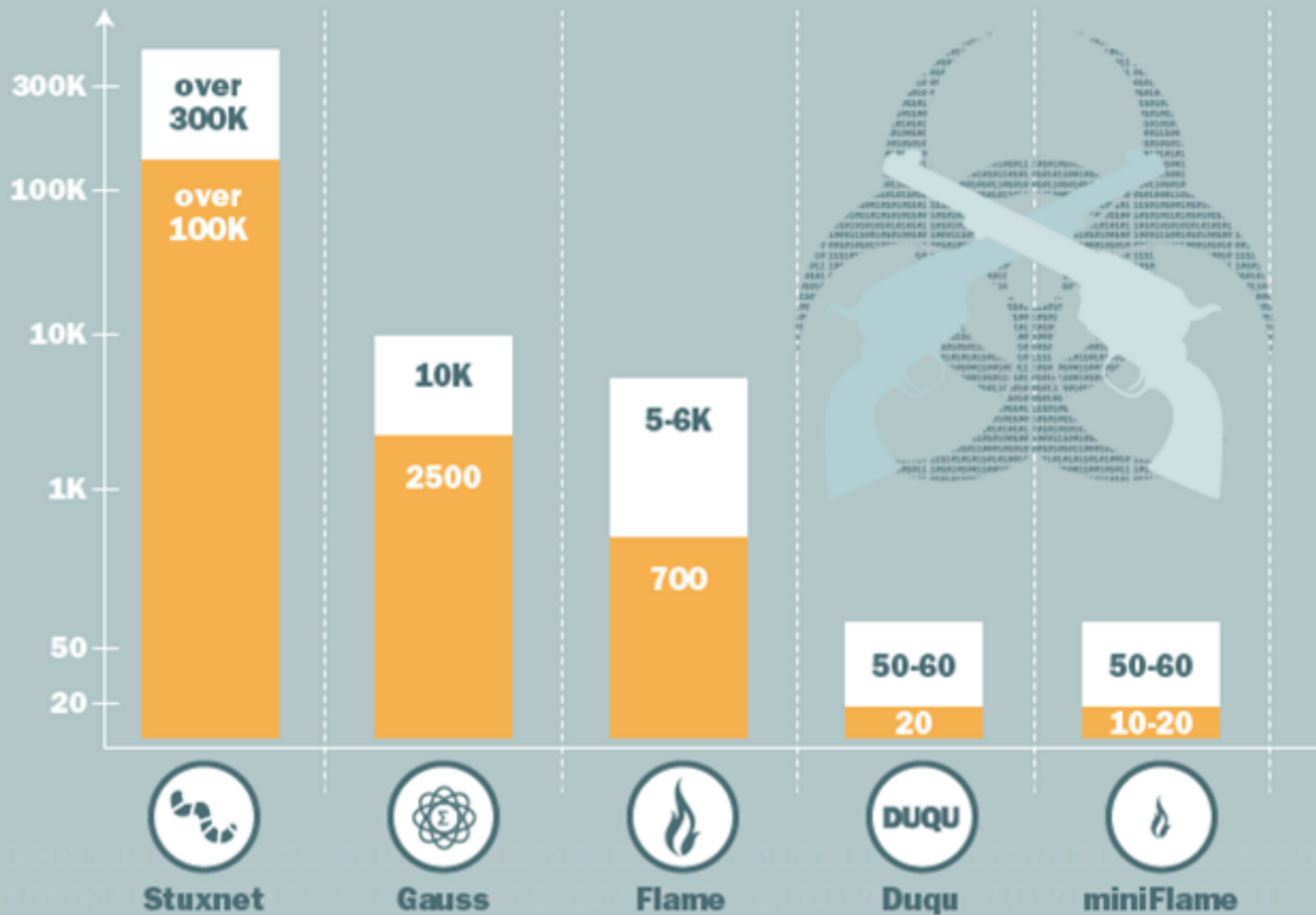


Intercept account data in social networks, mailing



Since late May 2012, Kaspersky Lab's cloud-based security service has registered **over 2500 Gauss infections**; We estimate that the **actual number of Gauss victims** may be in the **tens of thousands**.

Number of victims



Number of incidents (Kaspersky Lab statistics)

Approximate number of victims



W

E

R

G 
GAUSS

F 
FLAME

D 
DUQU

S 
STUXNET

Z

X

C

V

B



Human factors



Social Engineering



Social Network





Social Engineering



Social Network



Activate
 Ultimate protection

Recommended:
 Activate Personal Internet Security 2011 to get ultimate protection against Identity Theft, Viruses, Malware and other threats!



Advanced Security Center

- Home
- Firewall
- Automatic Updates
- Antivirus Protection

Other Security Tools

Antivirus Scanner

- Quick Scan
- Deep Scan
- Custom Scan
- History

Settings

- Options
- Website

Scan results

Scan results 20 potential threats found.

Name	Alert level	Action	Status
Trojan-PSW.Win32.Fantast	Critical	Remove	Not cleaned
Trojan-PSW.Win32.Dripper	Medium	Remove	Not cleaned
Trojan-Spy.HTML.Paypal.hn	Critical	Remove	Not cleaned
Trojan-Spy.HTML.Bankfraud.ra	Critical	Fix	Infected
Trojan-PSW.Win32.Antigen.a	Medium	Remove	Not cleaned
Trojan.BAT.AnitV.a	High	Remove	Not cleaned
Trojan-PSW.Win32.Delf.d	Critical	Remove	Not cleaned
Virus.Win32.Faker.a	Critical	Remove	Not cleaned
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
Virus.Win32.Faker.a	Critical	Remove	Not cleaned

Virus name: **Virus.Win32.Faker.a**
Security Risk:

Infected file: C:\Documents and Settings\user\Recent\cid.exe
Description: These programs steal MSN Messenger passwords using a fake dialogue box for entering MSN password. The program terminates connection and advises re-connecting, and info entered is sent to the virus writer.

Recommended: Please click "Remove all" button to erase all infected files and protect your PC



Social Engineering



Social Network

From: Tijuana Womack <[REDACTED]@tconl.com>

Sent: Bt 10.04.2012 13:05

To: [REDACTED]

Cc:
Subject: Need your help!

Hello! Look, I've received an unfamiliar bill, have you ordered anything?

[Here is the bill](#)

Please reply as soon as possible, because the amount is large and they demand the payment urgently.

[http://sleeksmiles.com/page12.htm?
94i55mj=nehjn3tl6cdfpw5&wtko=y5vqks
ekqzrs7hhwfah0&mycm3ca=t2p30qnrqa
08&evgew3w=8se40t1dh3uzu&](http://sleeksmiles.com/page12.htm?94i55mj=nehjn3tl6cdfpw5&wtko=y5vqks&ekqzrs7hhwfah0&mycm3ca=t2p30qnrqa08&evgew3w=8se40t1dh3uzu&)
Click to follow link

With Best Wishes
Tijuana Womack

MD5 check sum: 98883ca51e93caf9830e983c7256af93

Video posted by -WizArD-



From: [-WizArD-](#)
Joined: 1 year ago
Videos: 5

[Subscribe](#)

Embed: [Customize](#)

```
<object width="425" height="344"><param name="movie"
```

[More From user](#)

[Related Videos](#)

Kaspersky Internet Security 2009 Help

Alarm

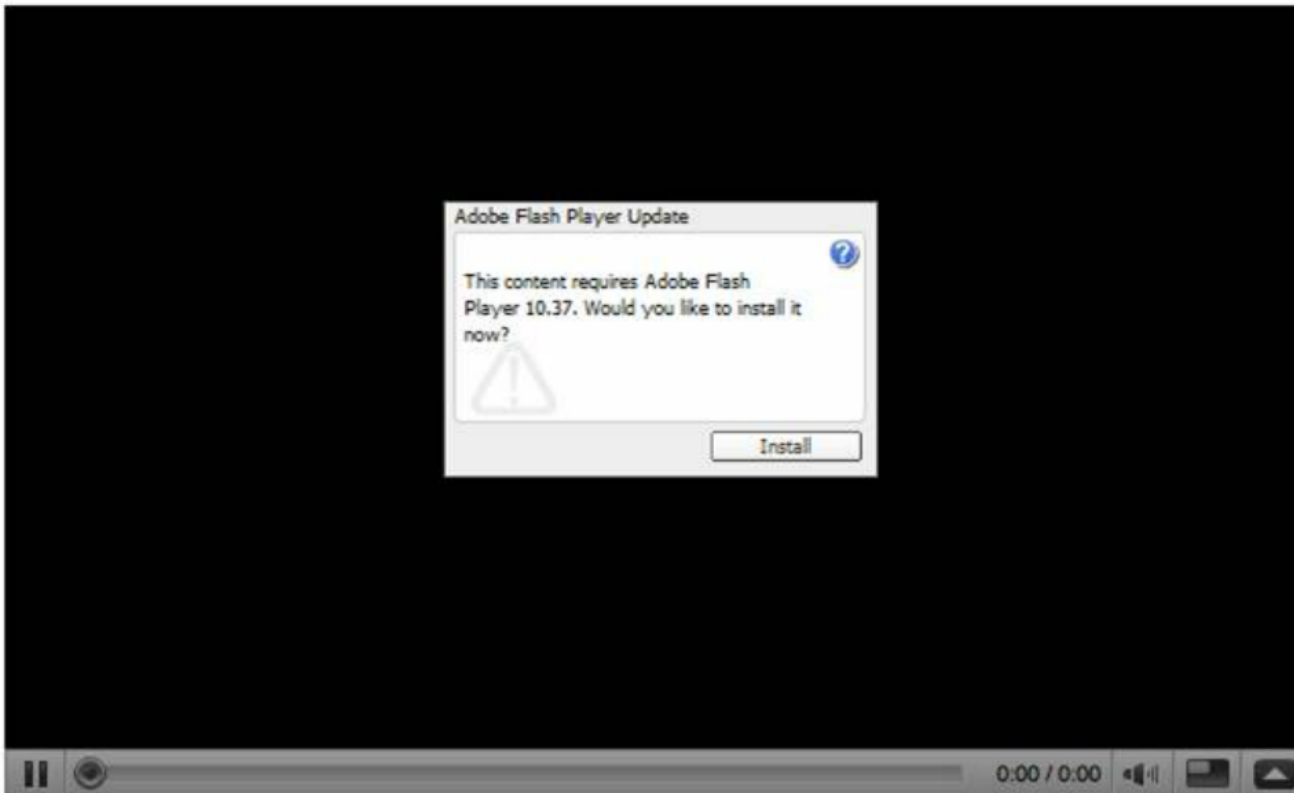
 Attempt to download malicious software.

Object:
http://[redacted].setup.exe

[→ Allow](#)
The action will be allowed

[→ Block \(recommended\)](#)
Action will be blocked

[Apply to all objects](#)



Video Responses: 10 **Text Comments:** 70

[babachat](#) (4 hours ago)
Funniest thing EVER!!

[csmith1199](#) (6 hours ago)
WooHoo!! Love this vid!!! Congrats on the front page!!!! :-)

[sinmike1](#) (7 hours ago)
that.... wasGREAT !!!

[ah17](#) (10 hours ago)
Nice vid :)



Social Engineering



Social Network



Social Network





Joseph Dylan Llewelyn
Edit My Profile

News Feed

Messages

Events 1

Friends

I have the beste... 1

Create group

See all

NetworkedBlogs

Applications

Photos

Games

More

Friends on Chat



News Feed

Top news · Most recent

What's on your mind?



Amazing! see who has viewed your profile! ---->

<http://bit.ly/WhosViewedYourProfile>

about a minute ago via Who's Viewed You? · Comment · Like



Joseph Dylan Llewelyn Crikey fell for that one. Some security bod you are ;)

2 seconds ago · Like

Write a comment...



Joseph Dylan Llewelyn is at Kaspersky Europe HQ.

6 minutes ago · Comment · Like · Tag friends



Rebecca Oliver A lovely morning here, sausage sandwiches then to go horse riding on the beach..

9 minutes ago via Mobile Web · Comment · Like



Jenny Oliver enjoy. poppy had very good night slept on my bed. she didnt like frost on grass this morning. dry and sunny here but cold. love to all mumxxx

5 minutes ago · Like

Write a comment...



Alan J Gill is now a Mac user!

Events

View all

What are you planning?

1 event invitation

Jenny Beddis's birthday See all

Sponsored

Create an advert

Hurry! Offer ends Thurs



Enjoy Sky TV, broadband, and calls for under £20 a month! Plus Free Sky+ box when you join Sky TV before 28th Oct. Hurry - join now!

Requests

View all

1 group invitation

2 Page suggestions

Pokes

Sarah Naylor · Poke back

Get connected

Who's on Facebook? Find your Friends

Who's not on Facebook? Invite them now

Chat (17)


 **Joseph Dylan Llewelyn**
Edit My Profile

- News Feed**
- Messages
- Events
- Friends

- I have the beste...
- Create group
- See all

- NetworkedBlogs
- Applications
- Photos
- Games
- More

Friends on Chat




News Feed

Top news • Most recent

What's on your mind?

 **Jenny Beddis** Amazing! see who has viewed your profile! ---->
<http://bit.ly/WhosViewedYourProfile>
about a minute ago via Who's Viewed You? · Comment · Like

 **Joseph Dylan Llewelyn** Crikey fell for that one. Some security bod you are ;)
2 seconds ago · Like

Write a comment...

 **Joseph Dylan Llewelyn** is at Kaspersky Europe HQ.
6 minutes ago · Comment · Like · Tag friends

 **Rebecca Oliver** A lovely morning here, sausage sandwiches then to go horse riding on the beach..
9 minutes ago via Mobile Web · Comment · Like

 **Jenny Oliver** enjoy. poppy had very good night slept on my bed. she didnt like frost on grass this morning. dry and sunny here but cold. love to all mumxx
5 minutes ago · Like

Write a comment...

 **Alan J Gill** is now a Mac user!

Events

What are you planning?

- 1 event invitation
- Jenny Beddis's birthday See all

Sponsored

Hurry! Offer ends Thurs

Free Sky+ box
£30 std set-up

Enjoy Sky TV, broadband, and calls for under £20 a month! Plus Free Sky+ box when you join Sky TV before 28th Oct. Hurry - join now!

Requests

- 1 group invitation
- 2 Page suggestions

Pokes

 Sarah Naylor · Poke back

Get connected

- Who's on Facebook? Find your Friends
- Who's not on Facebook? Invite them now

Chat (17)

Malicious links spreading on Twitter

Redirect #1

Redirect #2

Realtime results for My home video :)

0.05 seconds

1 more results since you started searching. [Refresh](#) to see them.



[BabbyBolton](#): My home video :) [http://\[redacted\].youtube/](http://[redacted].youtube/)

4 minutes ago from web · [Reply](#) · [View Tweet](#)



[ravengoatzz](#): My home video :) [http://\[redacted\].youtube/](http://[redacted].youtube/)

8 minutes ago from web · [Reply](#) · [View Tweet](#)



[straitcashhome](#): My home video :) [http://\[redacted\].youtube/](http://[redacted].youtube/)

10 minutes ago from web · [Reply](#) · [View Tweet](#)

```
<html><head>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1"></head>
<body>[redacted]
<script src="youtube files/abc.js">
[redacted]
</script>
</body></html>
```

```
location = "http://[redacted].com/go/tw.php";
```




Social Network



Hey [username],

Because of the measures taken to provide safety to our clients,
your password has been changed.

You can find your new password in attached document.

Thanks,

The Facebook Team

- ▶ Spam mail claims that the recipient's Facebook password has been restored
- ▶ The „new password“ can be found in the attached PDF document
- ▶ The malicious PDF installs a trojan (Backdoor.Win32.Bredolab)



Social Network





Human factors



Social Engineering



Social Network





Human factors



Social Engineering



Social Network





Technical factors



Mobile malware



Mobile malware

Where?



Why?



How?



What?



are

Where?





 **BlackBerry**



symbian

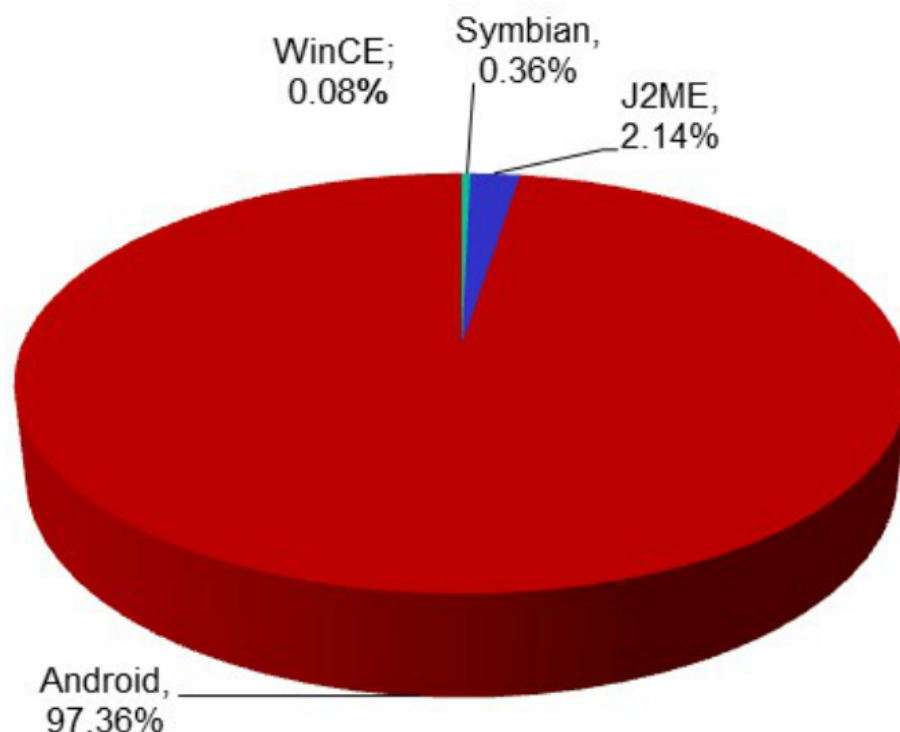


Mobile malware

Some statistics

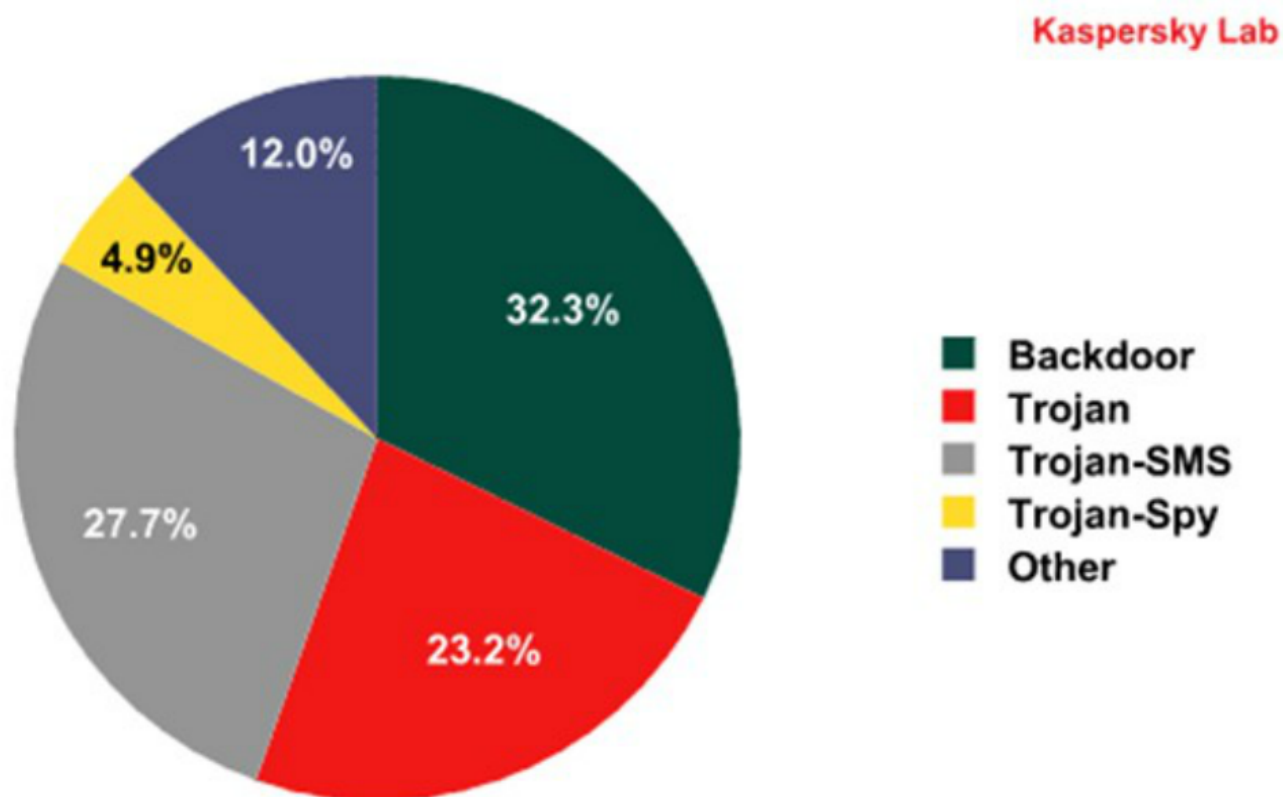
- ▶ Number of mobile malware families to-date: **679**
- ▶ Number of mobile malware modifications to-date: **107,068**
- ▶ Mobile malware found in July 2013: **4,181 new modifications**
- ▶ 99.96 per cent of all mobile malware found in 2012 targeted Android
- ▶ The number of samples gathered in 2012 alone is more than six times higher than in the previous 7 years altogether

Mobile malware written for specific platforms:



Mobile malware

- ▶ Distribution of malware targeting Android OS detected on user devices by behavior, Q2 2013

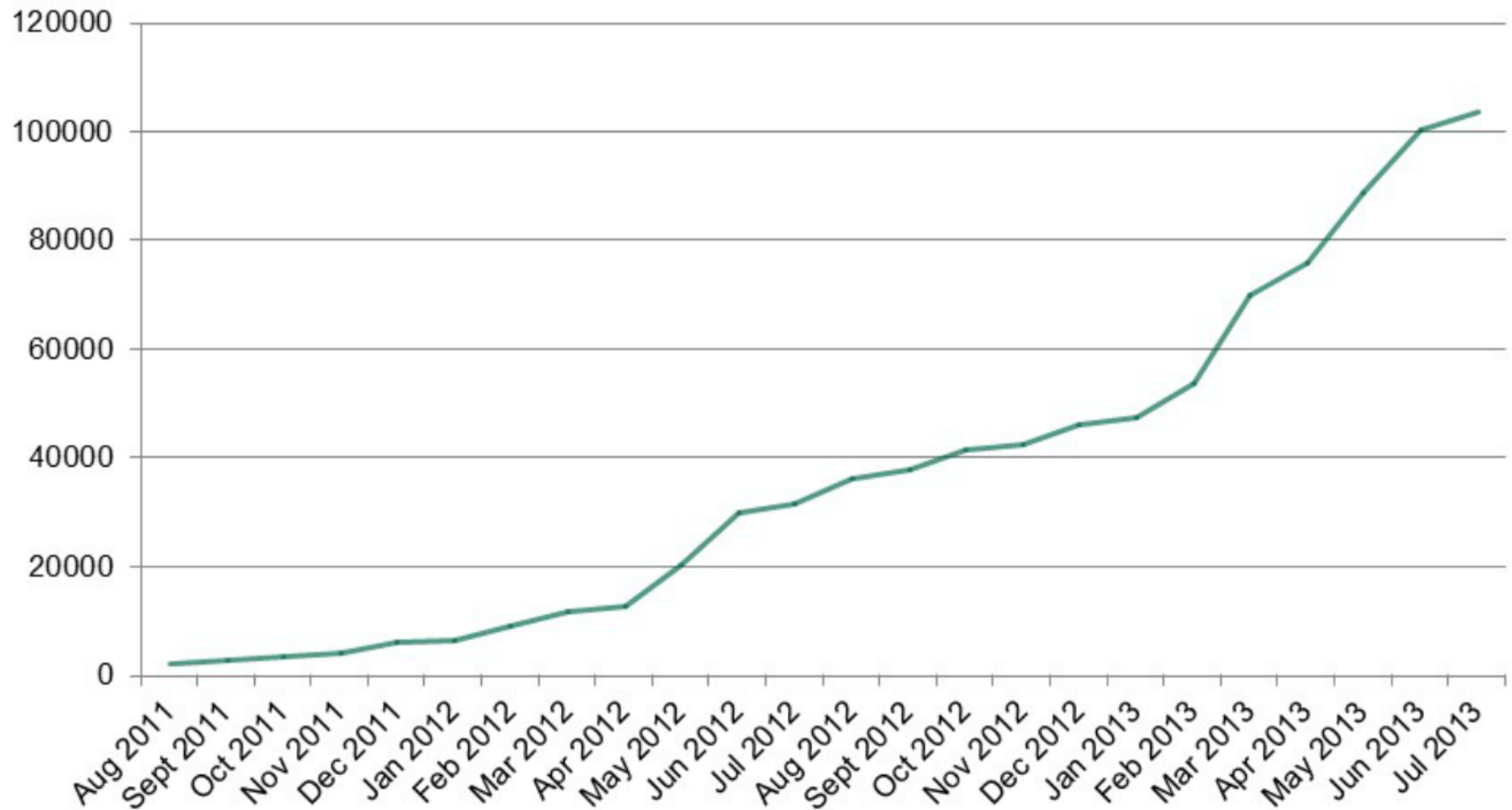


Source: Kaspersky Lab July 2013

Mobile Malware Sample Collection

Number of unique samples

Number of unique Samples



Source: Kaspersky Lab August 2013

Where?



Why?



Your device contains a lot of 'interesting' things:



incoming and outgoing SMS messages



work emails



business contacts



personal photos



GPS coordinates



online banking credentials



trip calendar



various installed apps



**Smartphones are becoming very similar
to classic PCs**

Why?



what?



SMS Trojans (or dialers)

Money

'Targeted' malware

Target

**'Steal-everything'
malware**

Spyware

Data

[O]bad news!

- ▶ Obad – the most sophisticated Android Trojan
- ▶ Exploits three vulnerabilities
 - ▶ Including one that gives it 'superuser' privileges on the device
 - ▶ So it can't be manually deleted
- ▶ Sophisticated backdoor Trojan
 - ▶ Runs silently in the background
 - ▶ No icon or other indicator of its presence
 - ▶ Remote control over compromised device
 - ▶ Receives commands from C2 server via SMS messages
 - ▶ Uploads data from device to the C2 server
 - ▶ Silently sends SMS messages to premium-rate numbers
 - ▶ Able to download and install additional malware
 - ▶ And spread to other devices via Bluetooth

How?



'Good' friends

Targeted email/IM/SMS

Apps from untrusted sources

Fake apps

Pirated apps

Apps from trusted sources

Android Market incidents

How?







BEFORE YOU
CLICK

PICK ME! PICK ME!

APP

APP

APP

APP

APP



How?





Technical factors



Mobile malware



Mobile malware

Where?



Why?



How?



What?



are



Summary



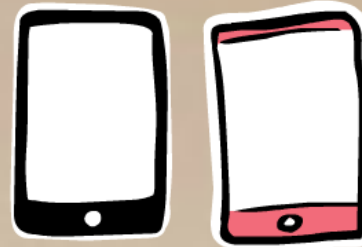
Evolution of malware



Technical factors

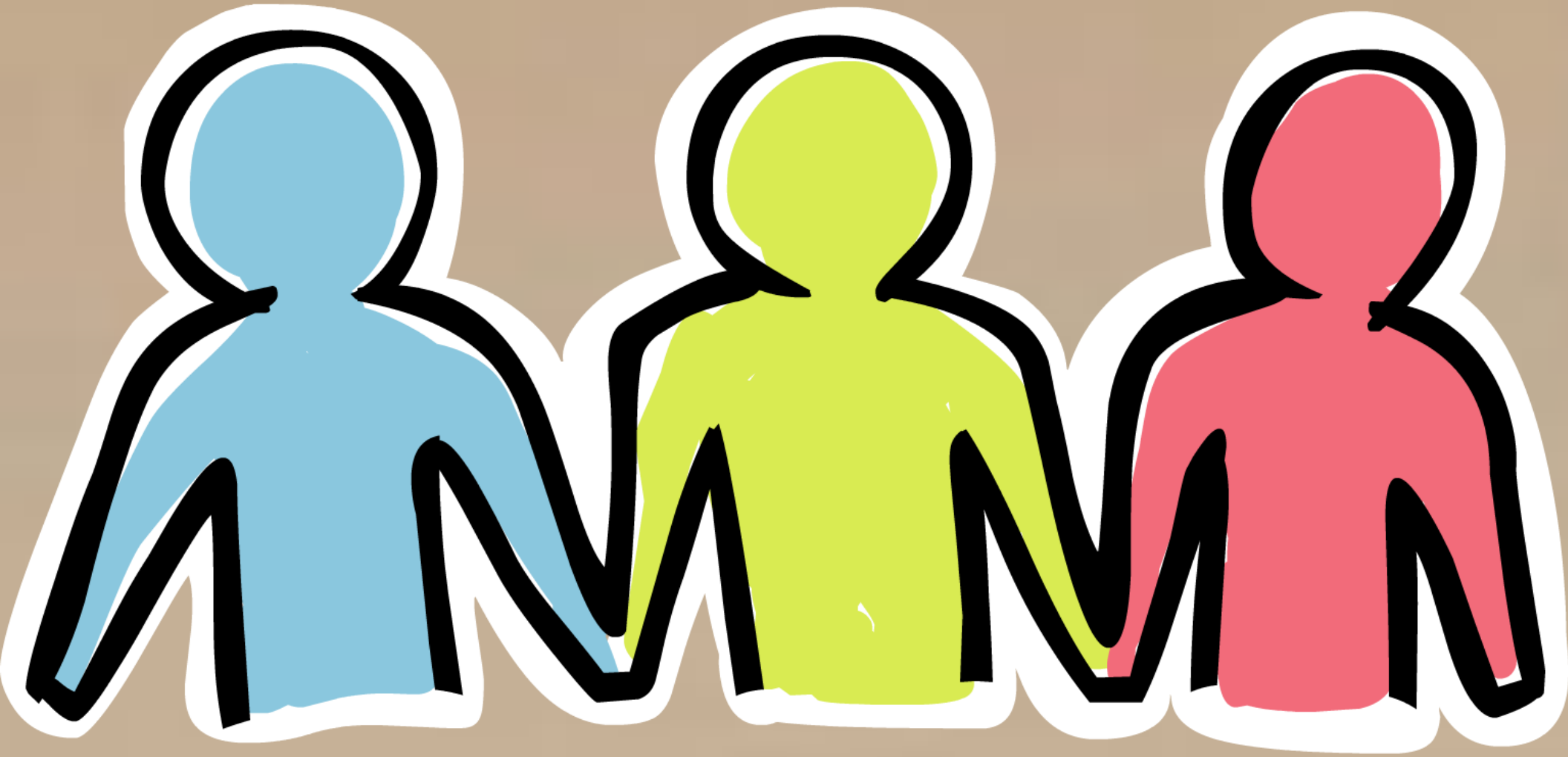


Human factors



Mobile malware

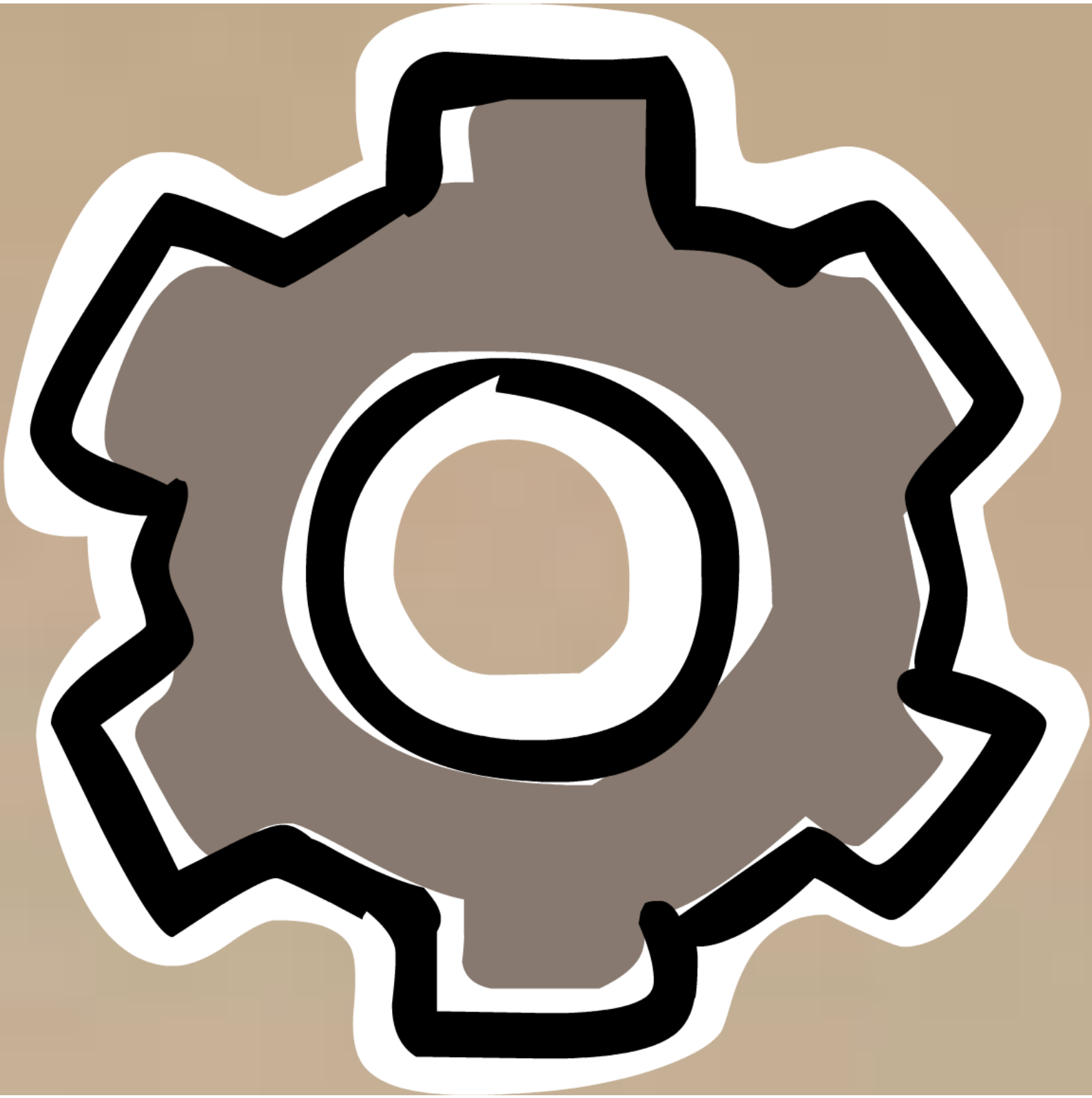




Evolution of malware

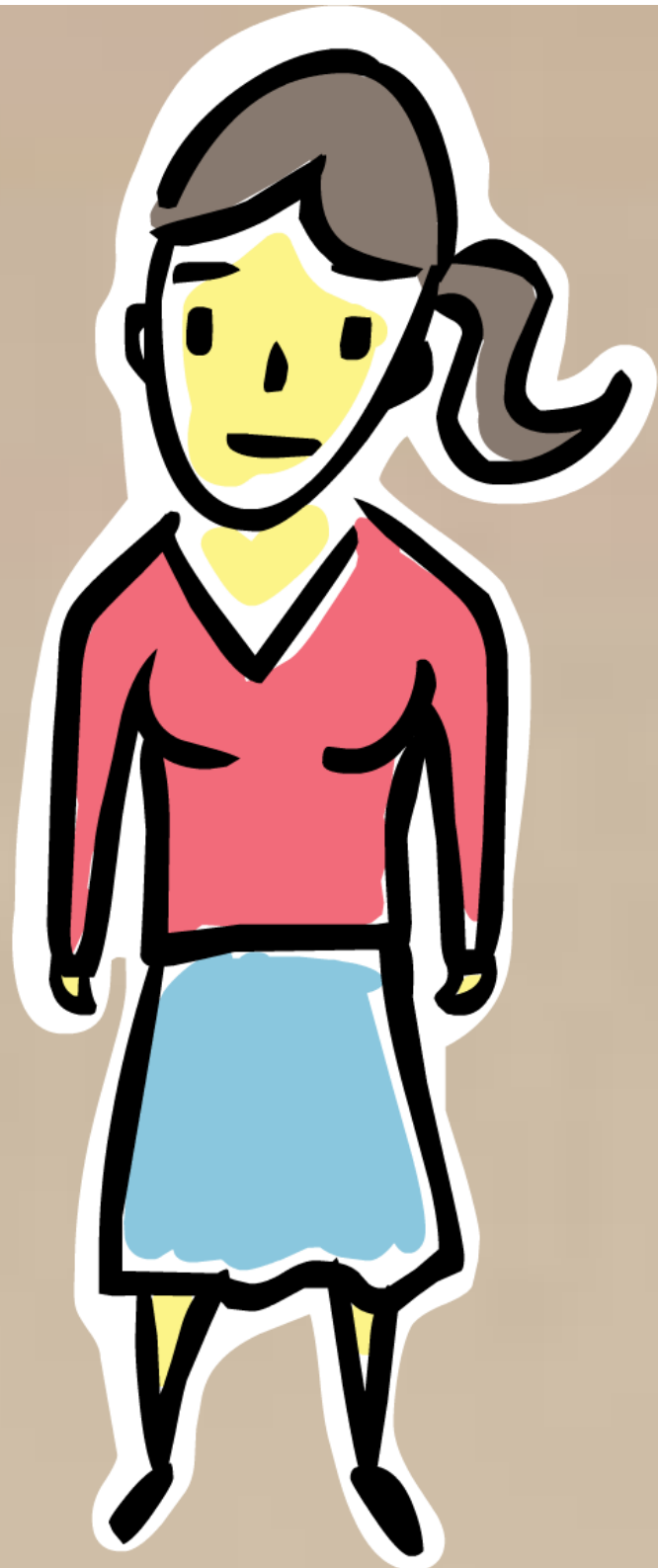


Evolution of malware



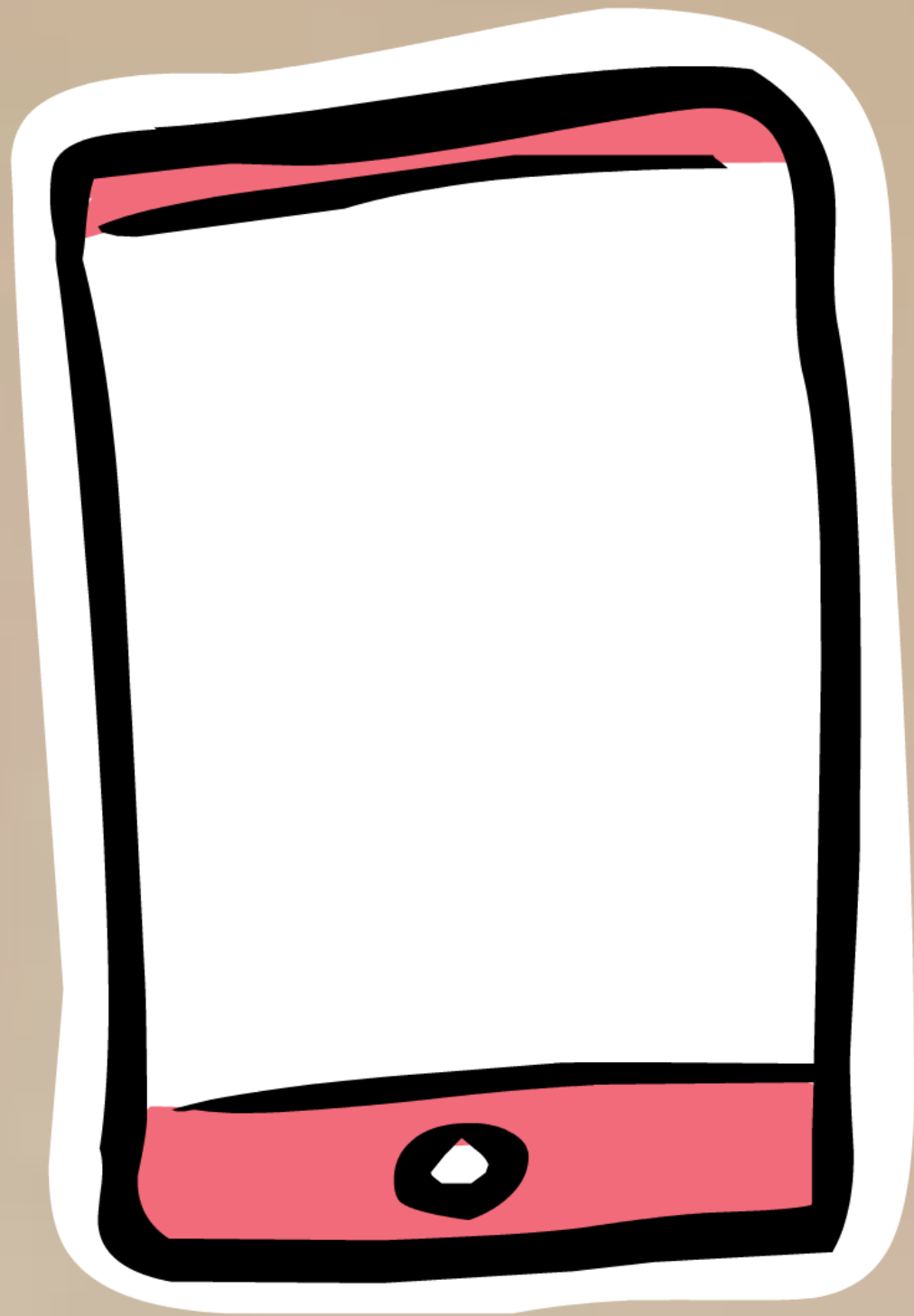
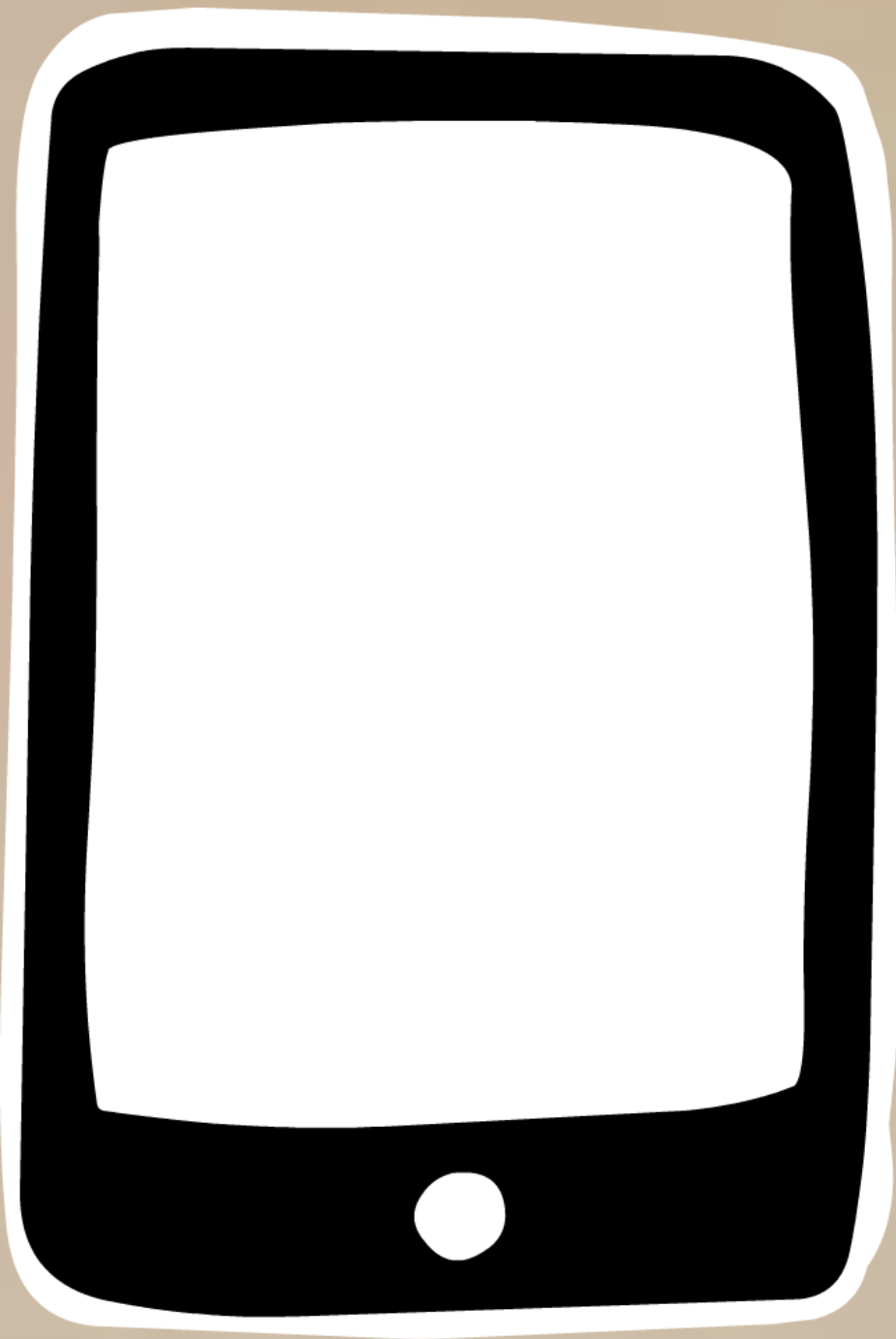


Technical factors





Human factors



Mobile malware



Summary



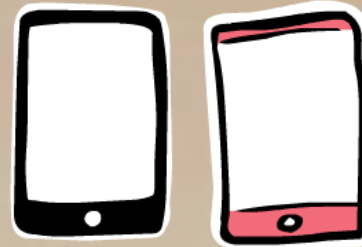
Evolution of malware



Technical factors



Human factors



Mobile malware





Any questions?

Jesmond Chang

Jesmond.chang@kaspersky.com





Kaspersky Lab Threats Update

Jesmond Chang

jesmond.chang@kaspersky.com