

SECURITY 2013



21. ročník konference o bezpečnosti v ICT

MALWARE INDUSTRY THE NEW ERA OF MALWARE

Boris Cipot
F-Secure Corp.





How it all started

- **From geeks to...**
- **IN SHORT:**
 - Anti-malware
 - Data Privacy
 - PC Firewall
 - Social Engineering
 - Security Policies
 - Privacy Policy
 - Data Backup and Contingency



The beginning

■ Malware writers were known

Signatures in the code

```

brain.com | F1 Help | Commands: BFGHINPWK | Col 0 | Line 0 | 0%
Welcome to the Dungeon 1986 Basit * Amjad (put) Ltd. BRAIN COMPUTER SERVICES 73
3 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Bew
are of this VIRUS... Contact us for vaccination...

```

Malware was written mostly for fun to show off expertise in computer knowledge.



Visual logos or names written on display



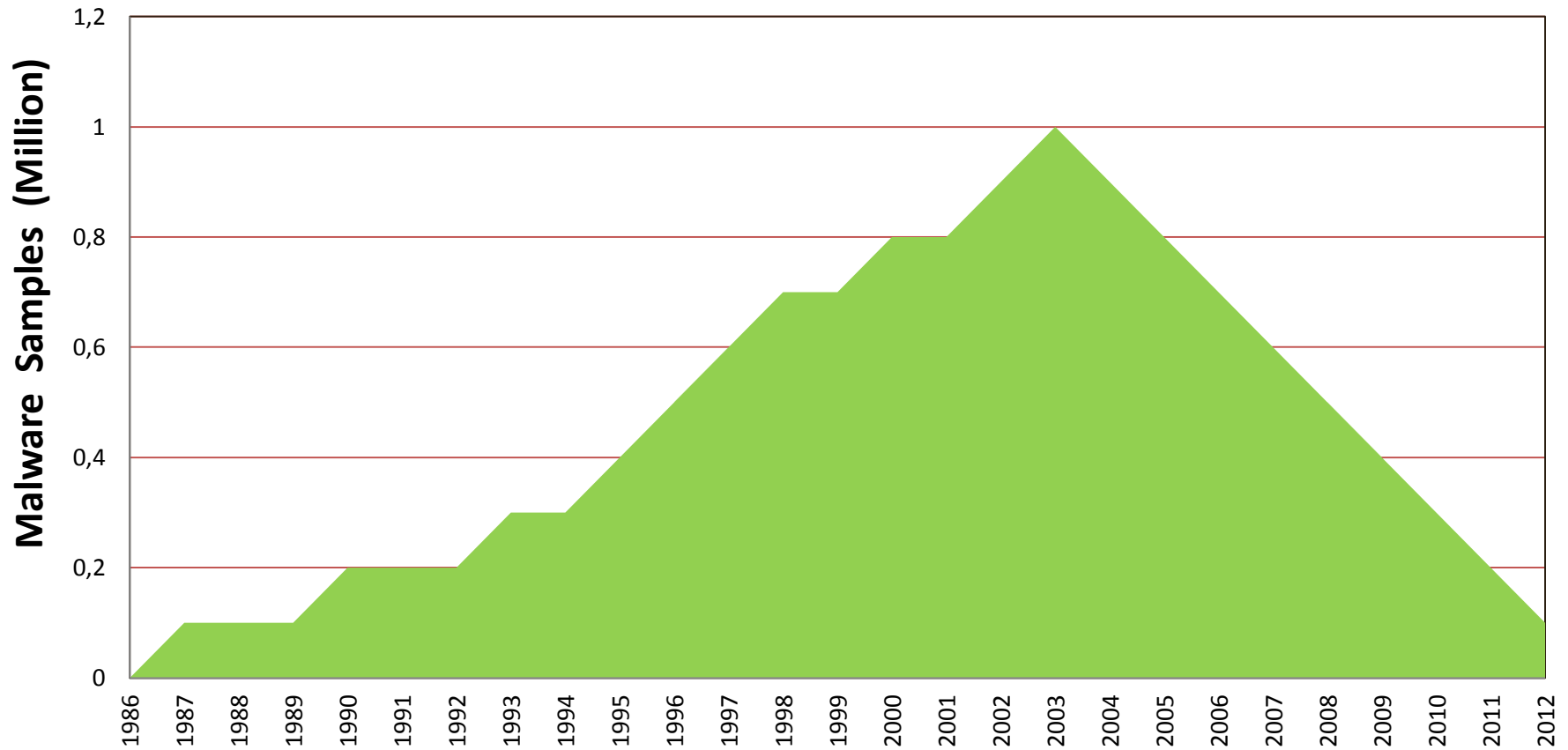
You knew that you are infected.



The beginning

■ Hobbyists

Malware was destructive





Evolution

■ Malware writers started hiding

Signatures were rare

```

8-FB 8E BC 07-02 3A FA 28
5-D7 04 1C D4-68 D7 E2 6E
C-DA CD E3 9F-16 7C 97 87
8-3A 7F C3 97-97 97 C7 75
0-6F FF F8 F9-97 97 FF E2
8-AD E8 34 00-00 00 8D 8E
4-6D 70 00 68-34 30 39 2E
A-5C 7E 8B EC-56 56 55 51
A-00 55 FF 57-F0 6A 00 FF
C-8B 4C 0B 78-03 CB 33 F6
2-03 D3 33 C0-C1 C0 07 32
8-C5 74 06 46-3B 71 18 72
7-14 72 8B 41-1C 03 C3 8B
8-74 74 70 3A-2F 2F 75 6E
E-63 6F 6D 2F-64 2F 69 6F
8-00 4F 36 30-30 4B 4F 37
7-07 07 07 07-90 90 90 90
8-90 90 90 90-90 90 90 90
8-90 90 90 90-90 90 90 90

```

;_~|||√ã|•@: <
 ΔF|N<Lü||L kh||r n
 L|ö±♦±_¼r=llf_üç
 üü|f-k&δ:Δ|üü||u
 éüüh Ló °-üü r
 rlmI W"ô:ô4 iã
 T 3÷htmp h409.
 hWRF0hC:\~iowUUQ
 U uδ Lu±j U W≡j
 W rQUò iK<iLδx♥u3÷
 ìñ|♥Q i±♥u3 LL•2
 0BÇ: uJ;|t±F;qtr
 ■iQ\$♥u*ññr iA-♥|i
 ÷é|±u|htp://an
 ionseek.com/d/io
 o.exe 0600K07
 8RUS.....ÉÉÉÉ
 ÉÉÉÉÉÉÉÉÉÉÉÉÉÉ
 ÉÉÉÉÉÉÉÉÉÉÉÉÉÉ

And encrypted in the code.

Malware started to be written for crime. It infected quietly and attempted to maintain a low profile.



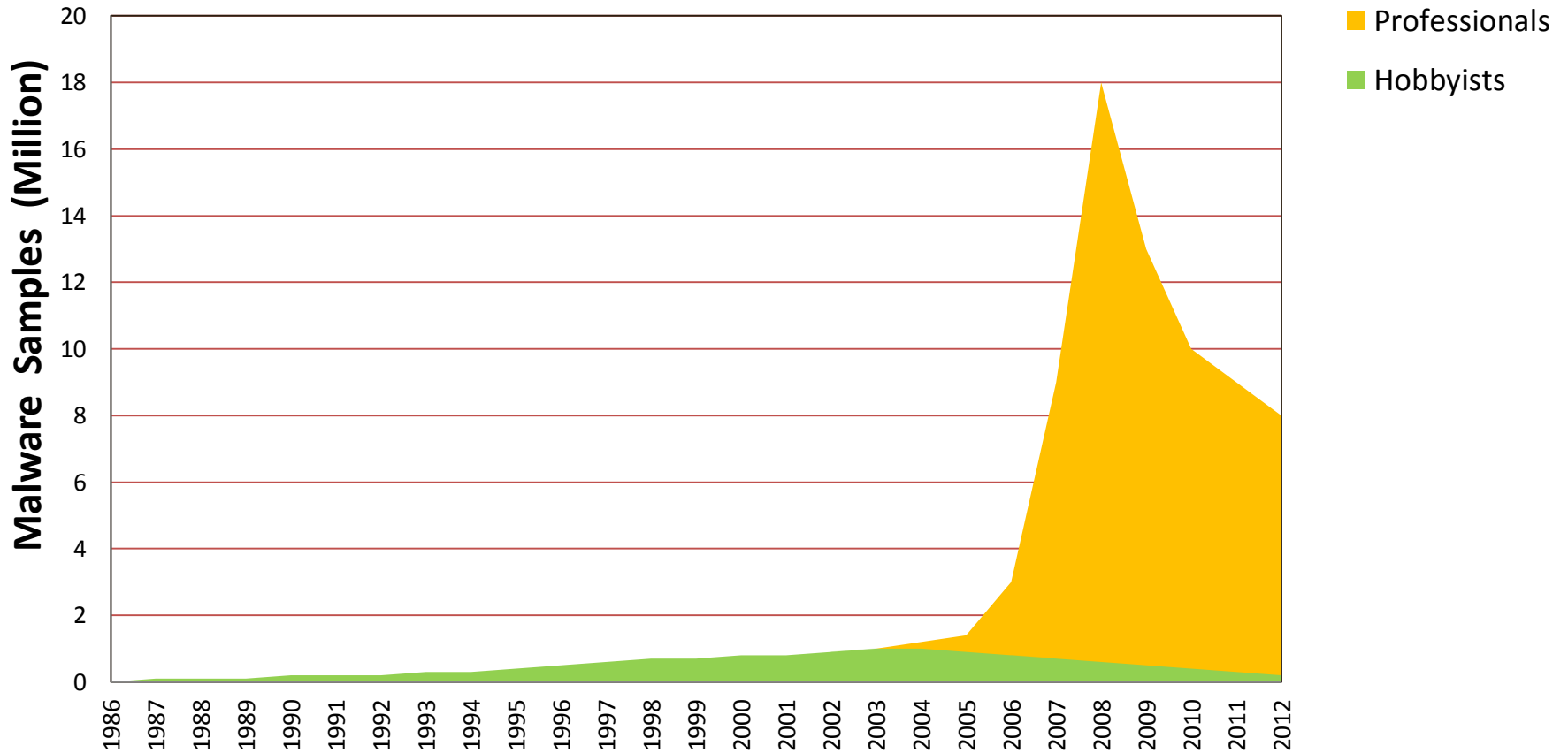
Infection was hidden to keep the infected computers running.



Evolution

■ Professionals

Malware was hidden





What are we facing today

- ... crime
- **IN SHORT:**
 - What we see as threats?
 - Where is this heading?

Malware writers today

- Malware writing today is an industry

Malware operators want to mislead you!



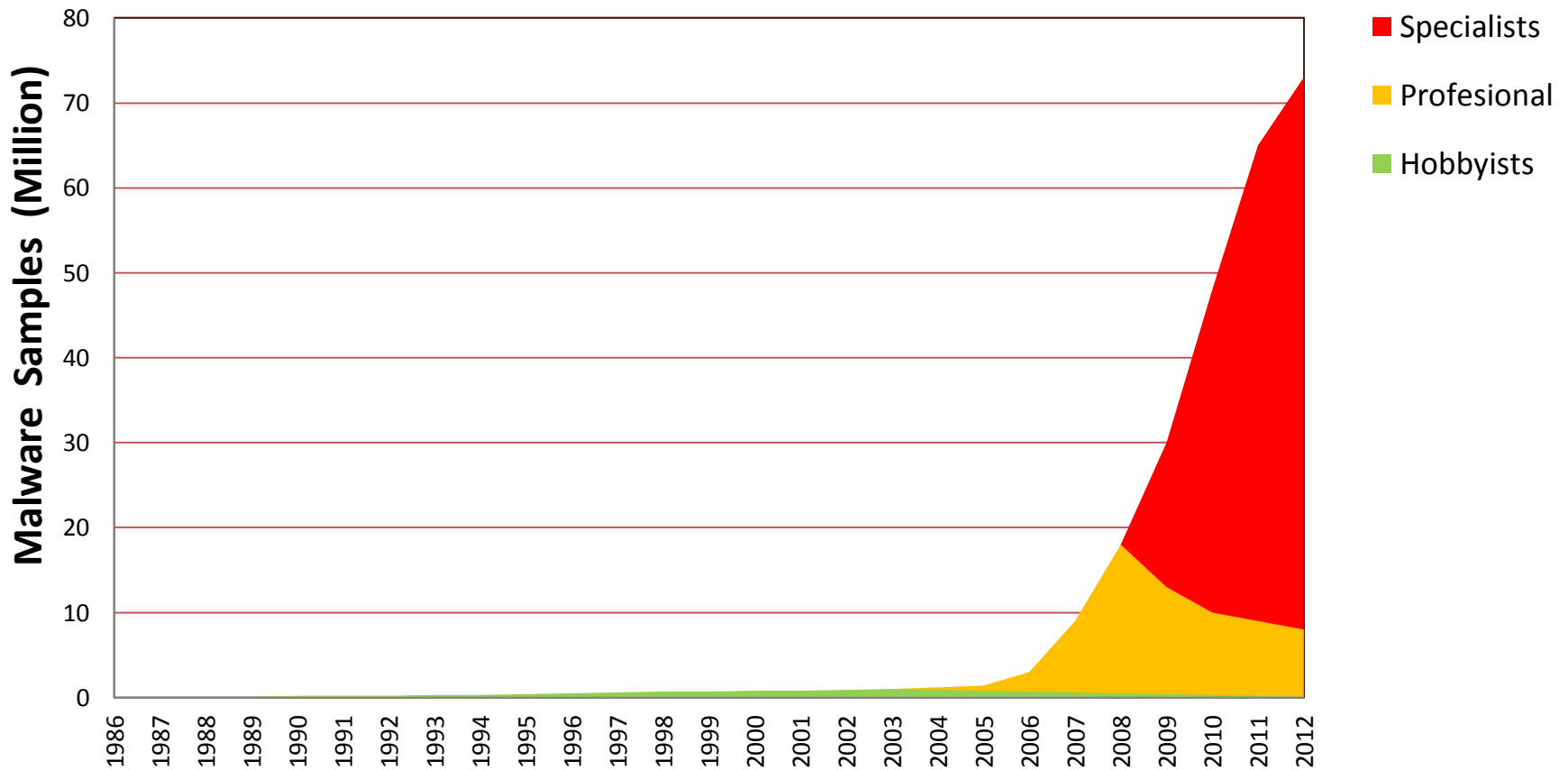
Malware is distributed to gain money.



Today

■ Specialists

Malware industry





Today

■ Specialists

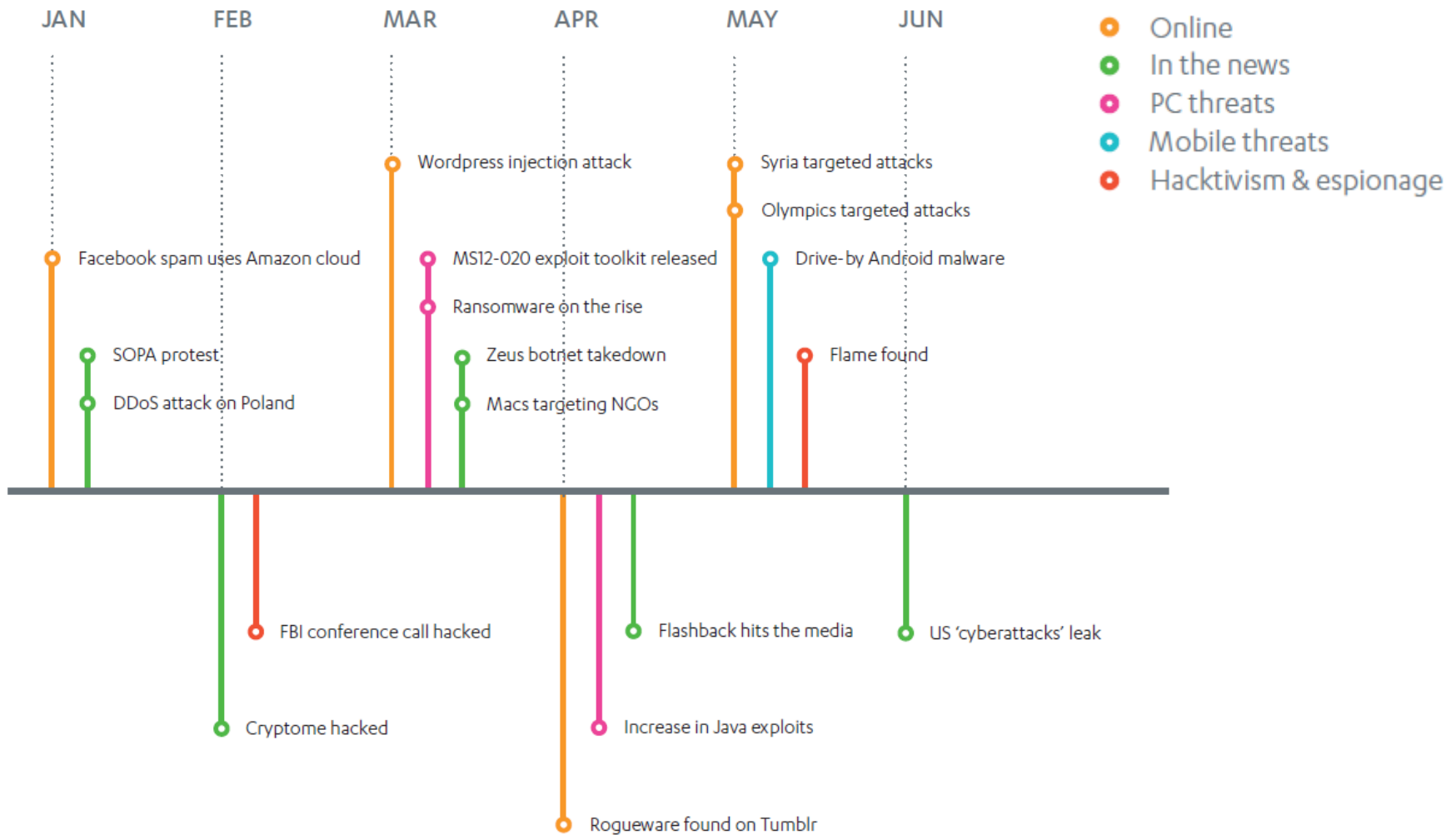
Malware has become an industry

- Not only new malware but **reused** malware
- Software holes are exploited more and more
- Malware offered as services
- Banking Trojans sold as products
- Ransom malware
- Rouge software
- Online game password stealers
- Credit card frauds and services sold
- Targeted attacks and phishing
- Social network frauds and phishing
- Malware for mobile phones and other mobile devices
- Hactivists
- Attacks on infrastructure and governments
- ...



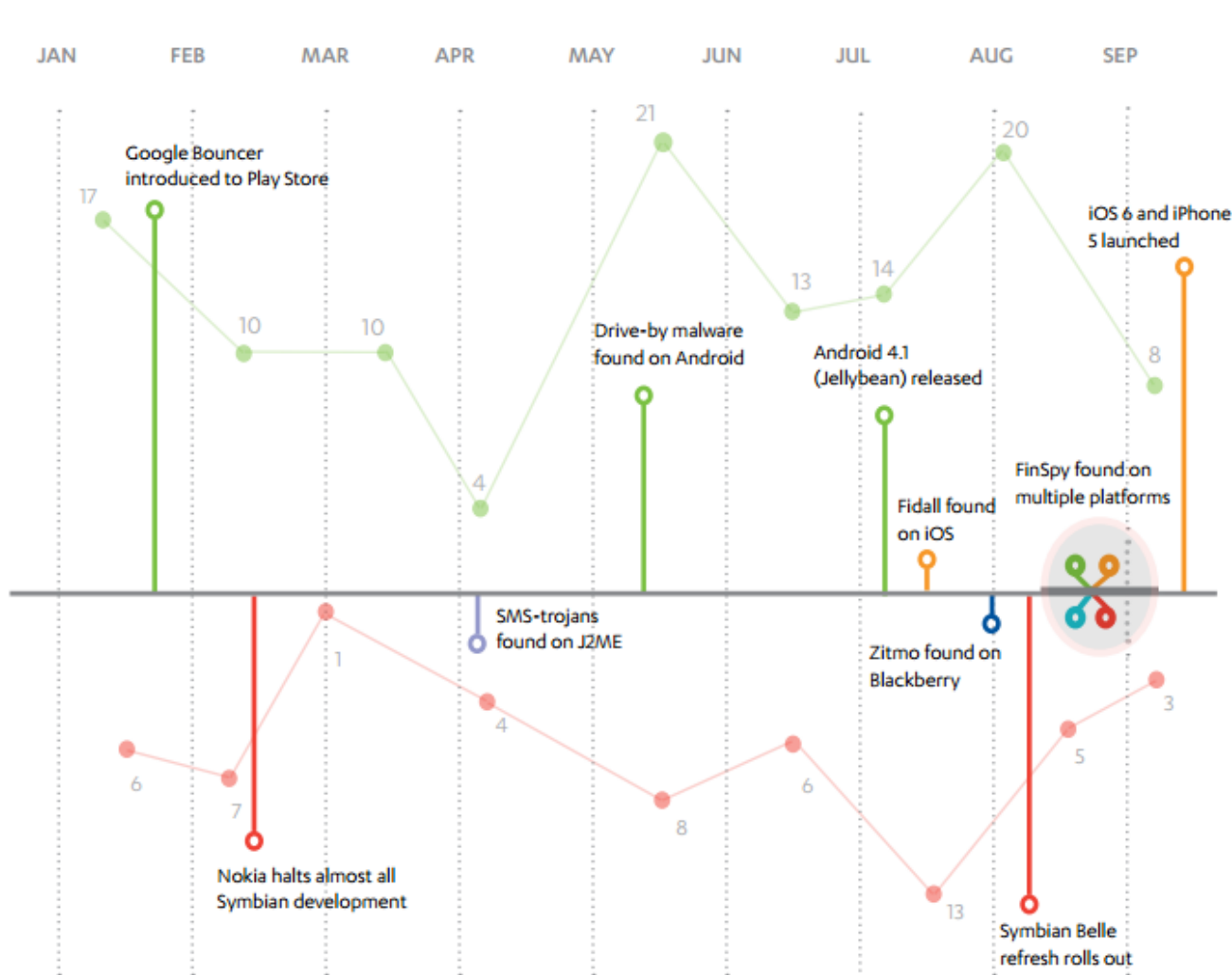


Last year highlights



Last year highlights

2012 MOBILE LANDSCAPE CALENDAR



THREAT STATISTICS

- New families/variants on Android
- New families/variants on Symbian

NOTABLE EVENTS

- Android
- Blackberry
- iOS
- J2ME
- Windows Mobile
- Symbian



Malware As A Service (MAAS)

■ Malware has become a service

- Malware writers offer exploit kits
- Hackers offer their services to configure kits
- Competition between different malware kits
- Malware kits reused and rebranded
- Exploits even attacking “safe OS” 😊
- ...

This is a big problem for the future!





It is a crime wave

Sponsored and lead by criminals

Hosting providers offering “special services

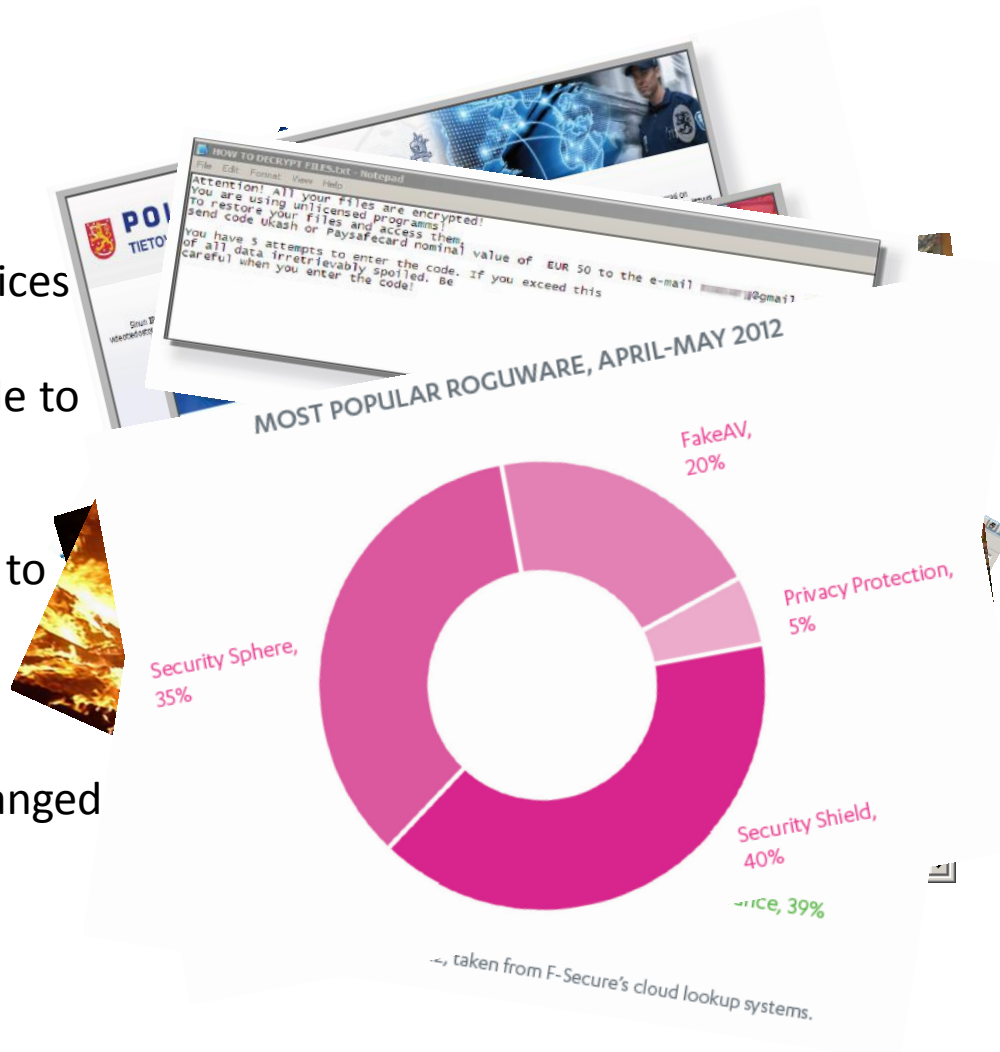
And sometimes hosting providers decide to clean up malicious websites but...

Social engineering techniques are used to scare you into paying

Malware has changed...

The motive for malware writing has changed

The only logical step is...





The logical step





What now about mobile?

- Is it still safe?
 - **IN SHORT:**
 - What is happening with this platform?



In the future

Eventually, virus writers will realize it's easier to make money by infecting phones than by infecting computers!

Guess what? The future is here!



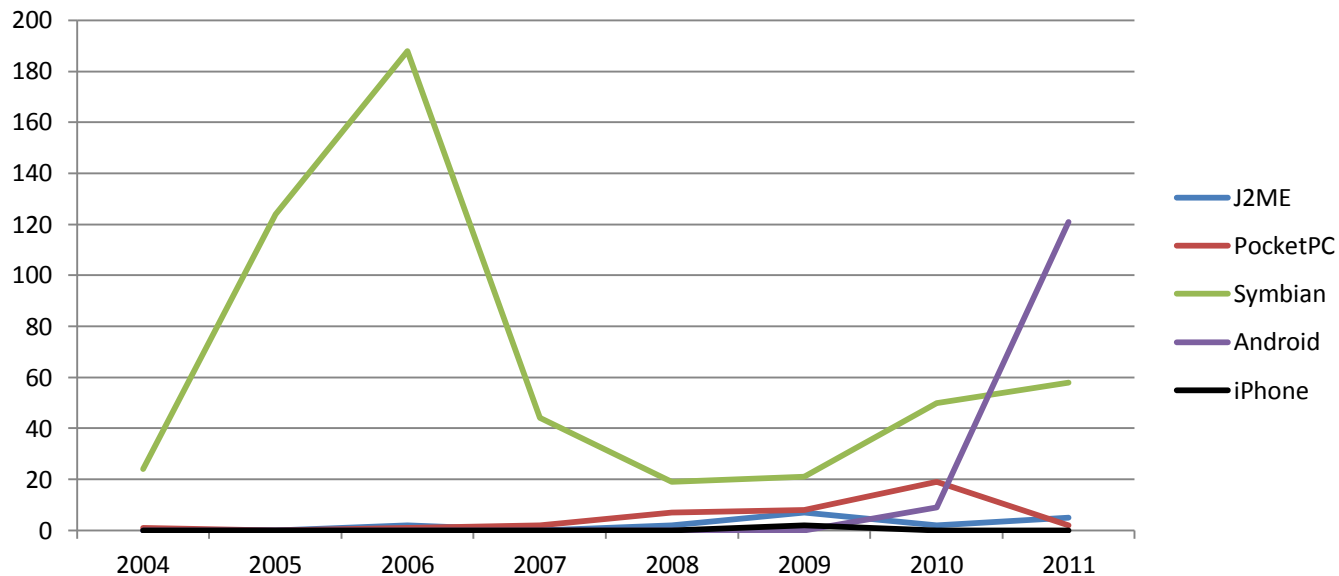
Mobile Security Landscape



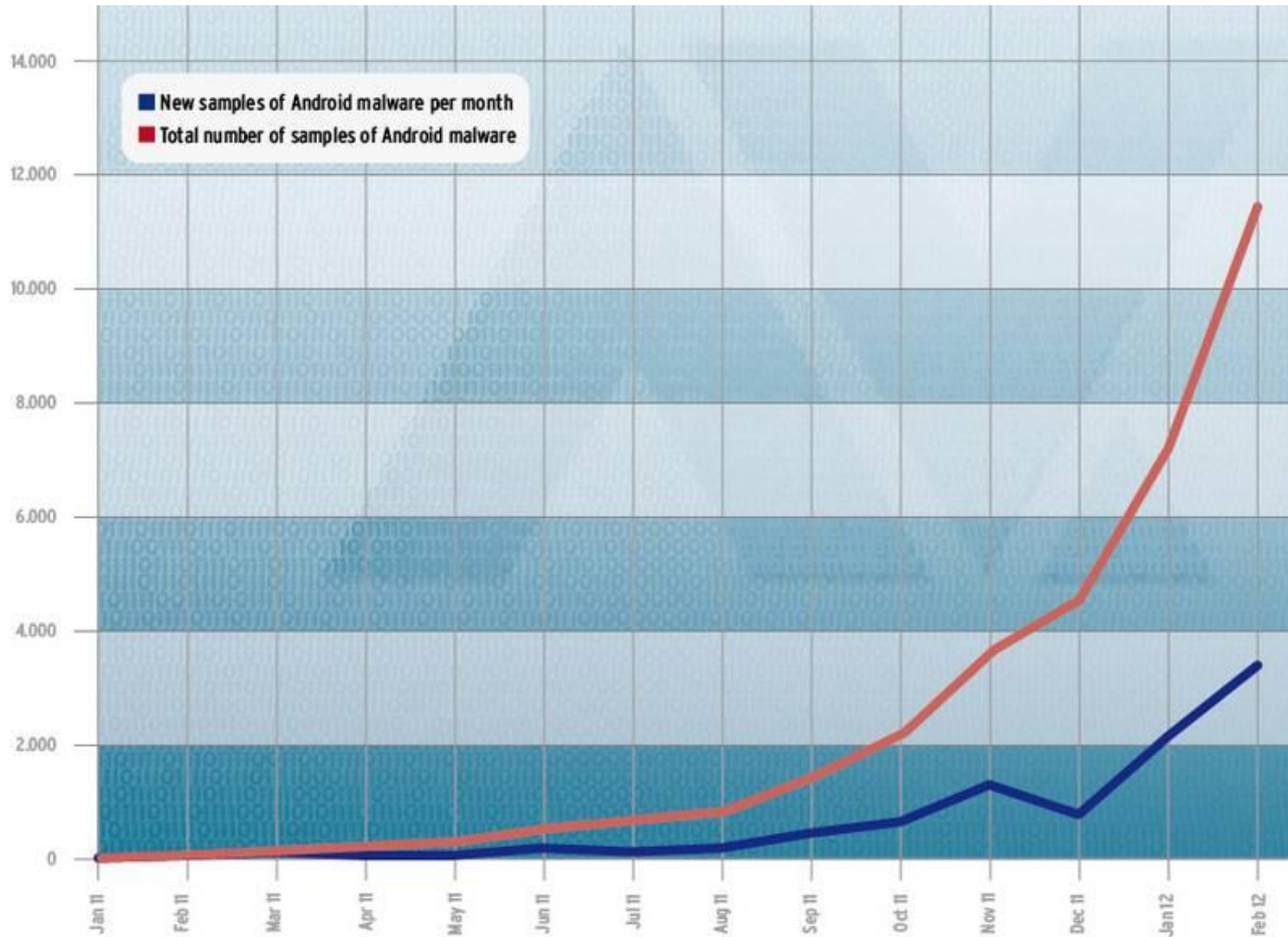
Total amount of Mobile Malware

- Total amount 7500 (February 2012)
- Android now #2 OS after Win XP for viruses

Yearly new malware amounts by platform



And the trend continues



Copyright © AV-TEST GmbH, www.av-test.org



One of the most known

Cabir outbreak in the 10th World Championships in Athletics





Menu

36



Messages



Phonebo...



Logs



Gallery



Camcorder



Media



Calendar

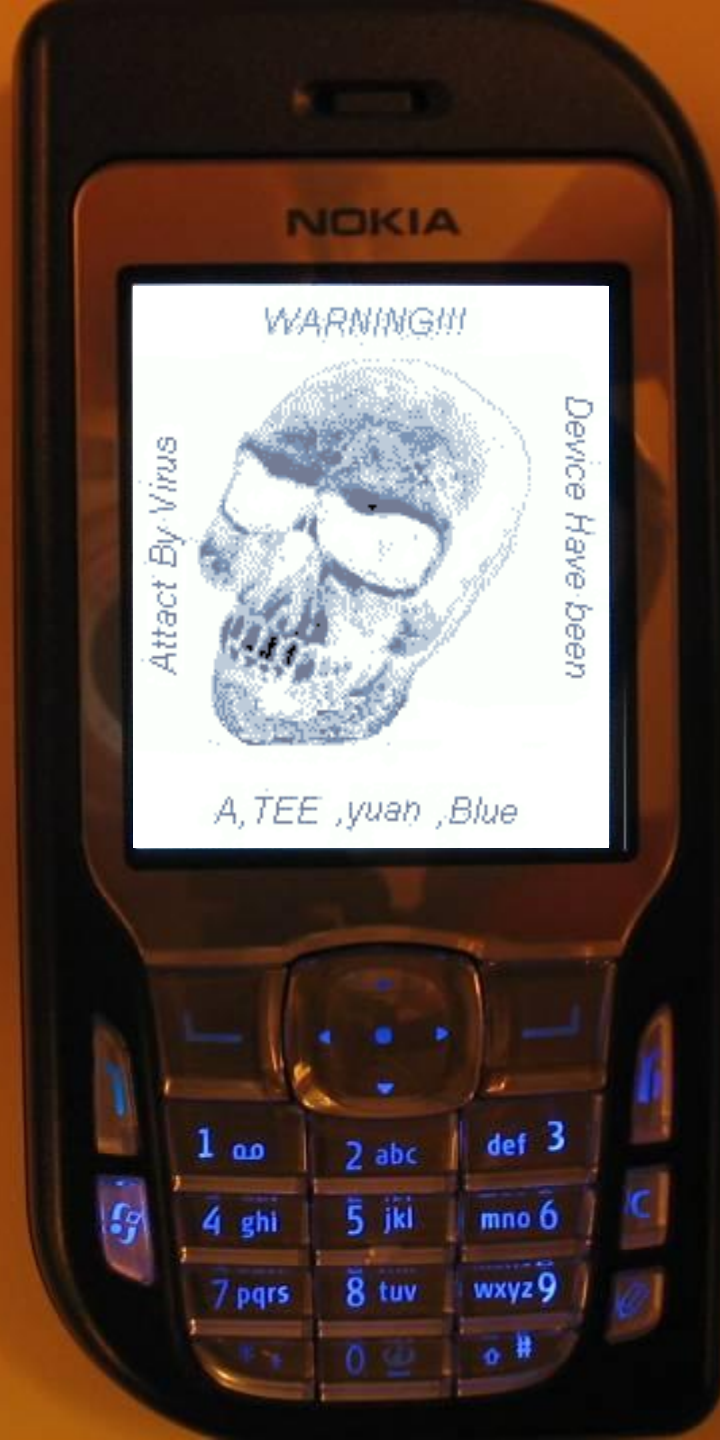


Browser



Clock

Skulls.D





But...


Easy to imagine a smartphone or a tablet as a mobile device

What about...





Caution

The transmission  lock mechanism is abnormal. Park your car on a flat surface, and fully apply the hand brake.

12:52

H
M



ODO
TRIP



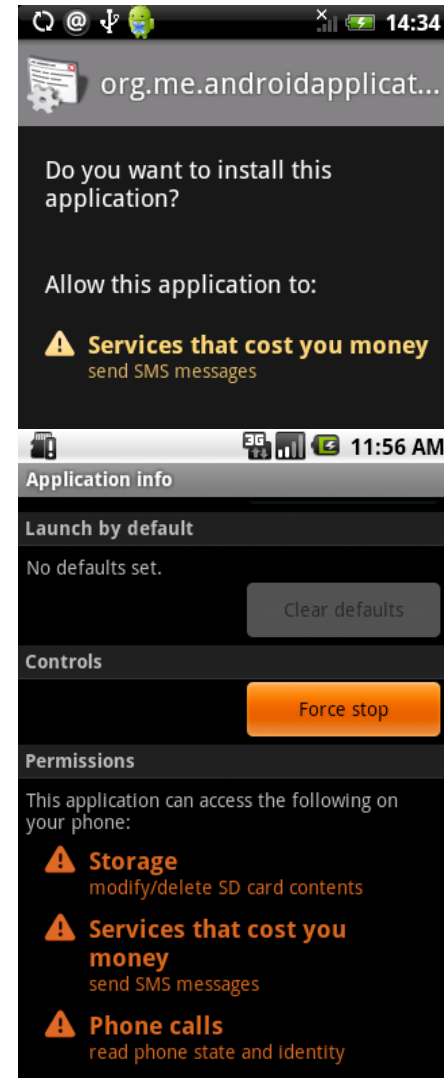
LOAD





Fakeplayer

- Fakeplayer variants are Android trojans that pretend to be media player application
- On installation Android will ask for permissions that include sending SMS messages
- Upon start up Fakeplayer sends a premium rate message to a Russian short number, without country code
- Unfortunately just about every Android app asks for a ton of permissions so user will probably not react to this
- When application is run it displays Russian text which translates as "Wait, seeking access to video library..."



22nd March 2010, 08:52 AM


#1

smudgelab  [OP]

Member

Join Date: Jan 2010

Posts: 38

** Phone dialled out internaionally without permission!**

Really wierd one this. Last night, I was woken by a repetitive voice telling me that "International dialling is not currently permitted from this device". As this was at aprox' 02.40 on SudaY AM, it fair shook me out of a deep sleep! On checking the phone I found the following call history:

+88213213214 @ 02:44

+88213213214 @ 02:36

+1(767)503-3611 @ 02:36

+1(767)503-3611 @ 02:36

+1(767)503-3611 @ 02:36

+8823460777 @ 02:35

I have absolutely no idea who or what these numbers are for (Google suggests +882 may be something to do with satellite phones(!?) & +1767 appears to be a Dominican country code(!??) but it was very unnerving to see my phone has been trying to ring these without any input from me. I'll be onto Virgin mobile later to see if they can help but thought I'd try the collective wisdom of you guys first. Virus / dialler maybe? Do these even exist for win mo phones? Any help will be very much appreciated. Thank you.



中文 **ENGLISH**

[留言板 >>](#)

首页

游戏

3D第一人称射击

3D赛车

动作类

飞行射击

角色扮演

休闲益智

冒险解谜

公司

关于我们

合作伙伴

招聘信息

联系方式



热门推荐

[more >>](#)

死镇逃生



死镇逃生

蓬莱仙侠传



蓬莱仙侠传



热3D街头赛车

反恐特警真3D版



反恐特警真3D版

即将发布

[more >>](#)



玛雅宝石



谍影危机



超级保龄球



街头篮球

Search for:



Search

» [Advanced](#)**SAVE BIG: 25% OFF Site Wide*****Current Device**
No device selected[Add device](#)**Software**

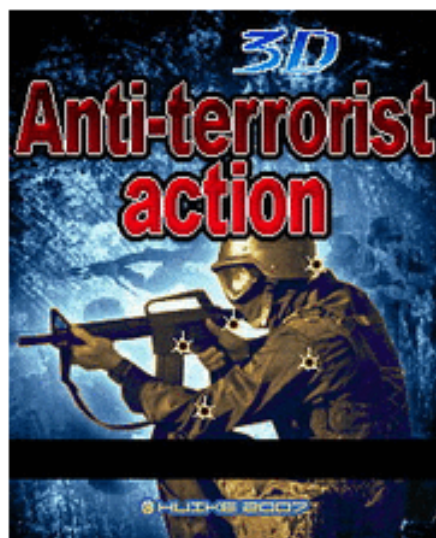
- » [New Software](#)
- » [Updated Software](#)
- » [Top Sellers](#)
- » [Top Downloads](#)
- » [Special Offers](#)
- » [Top Free Apps](#)

Categories

- » [Tools](#)
- » [Games](#)
- » [Travel & Holiday](#)
- » [Communications](#)
- » [Organization](#)
- » [Show all categories](#)

Now acceptingYou are here: [Home](#) » [Games](#) » [Adventure](#) » [3D Anti-terrorist action WM2003SE 1.0.1](#)

3D Anti-terrorist action WM2003SE 1.0.1

by [Beijing Huike Technology Co.,Ltd](#)[Details](#)[Compatible devices](#)[Ratings & Comments](#)

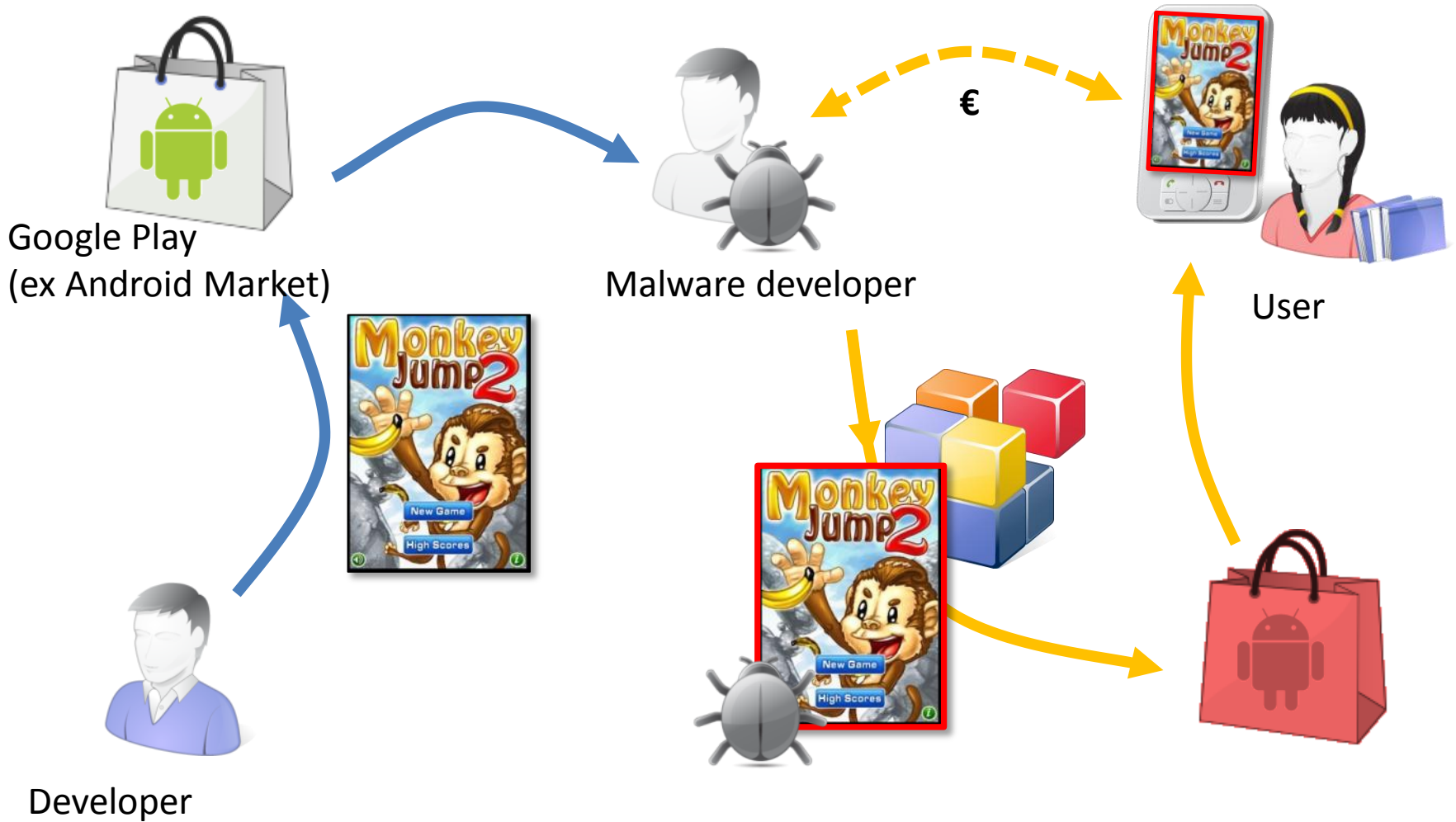
Product image for 3D Anti-terrorist action WM2003SE 1.0.1

Short description for 3D Anti-terrorist action WM2003SE 1.0.1:

This is a classic 3D first person perspective shooting game.

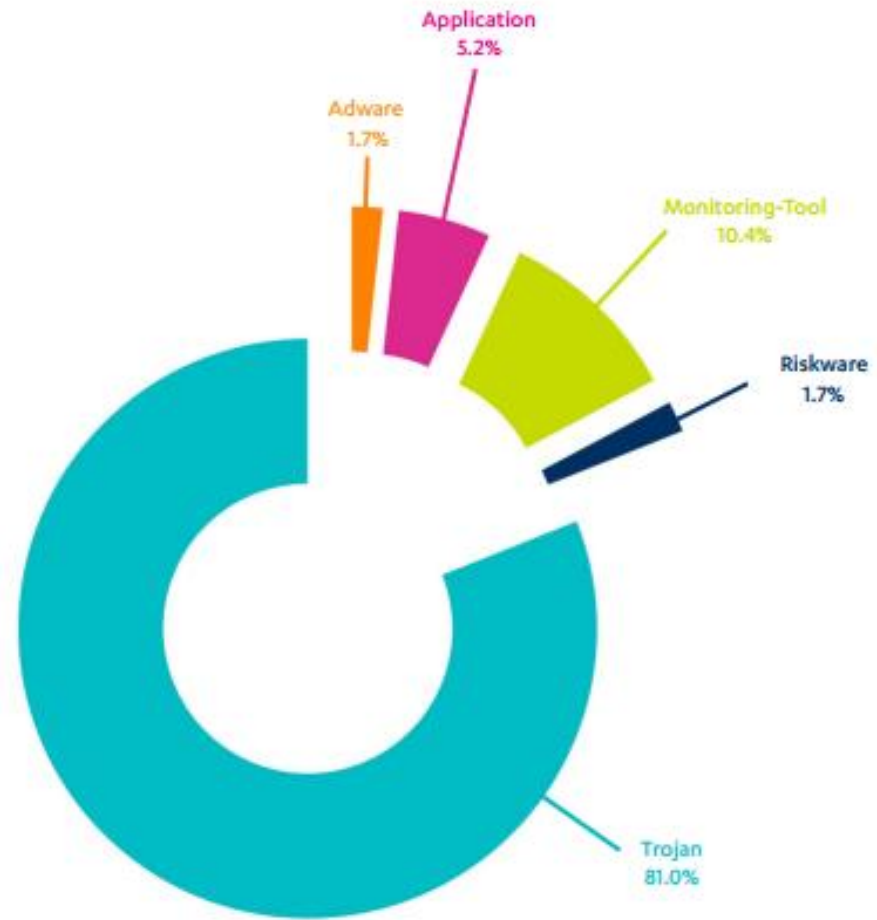
Rating: [Rate now - Recommend software](#)**For:** [Show compatible devices](#)**Downloads:** 272**License:** Commercial**Last updated:** 10/15/2009**Languages:** **Category:** [Games](#) » [Adventure](#)[Games](#) » [Action](#)[Games](#) » [Other](#)**Registration Key:** will be delivered on purchase**Trial version:** [Download](#)

A simple way to do it



Mobile threats by type

- Adware
- Applocation
- Monitoring tool
- Riskware
- **Trojan**

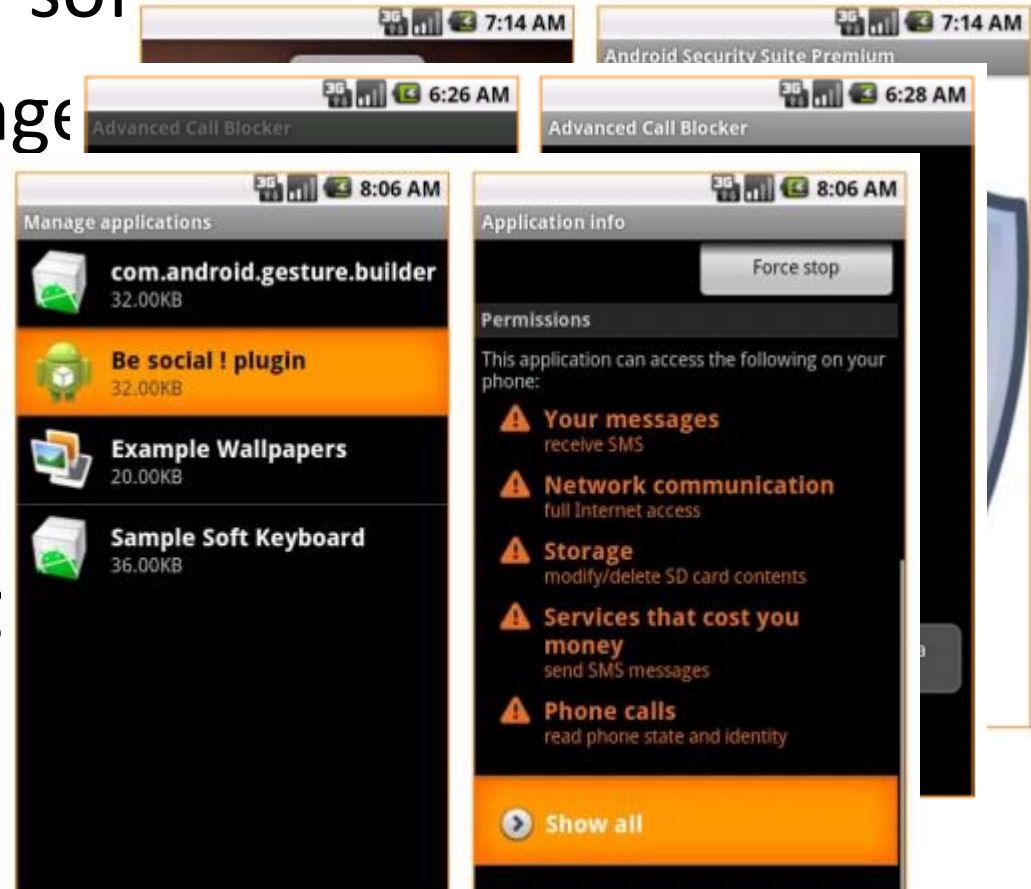




What do they do

- Posing as security software
- Sends SMS messages
- Data harvesting
- ...

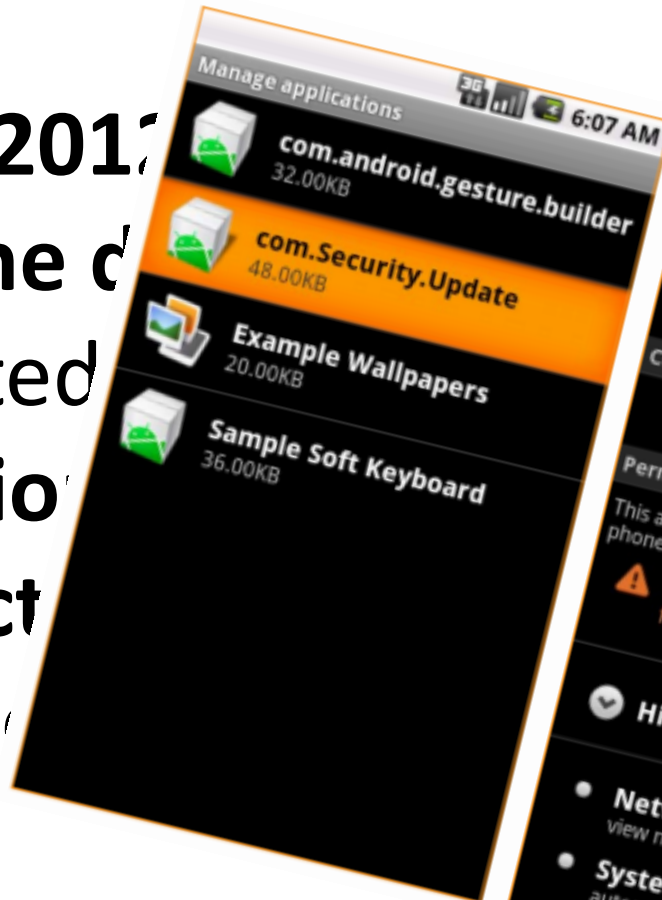
And the interesting
is also the distribut



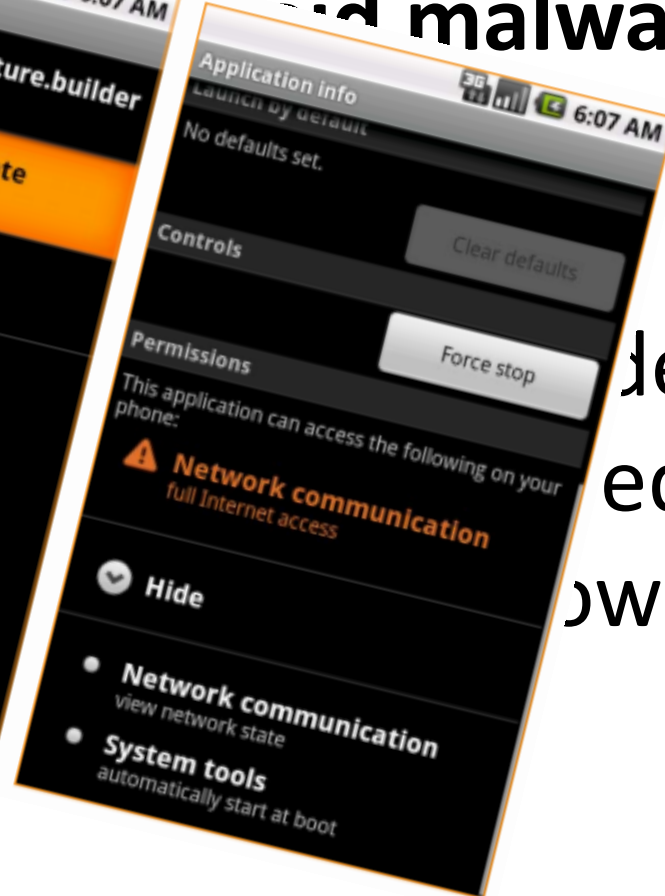


Is this not interesting?

In May 2012, researchers used the device to spot a malicious application that infected all



malware to infect a device and to own





RESTRICTED AREA
NO ENTRY
UNAUTHORIZED PERSONNEL
ONLY

RESTRICTED AREA
NO ENTRY
UNAUTHORIZED PERSONNEL
ONLY

F-SECURE



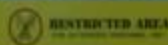


WARNING!

LIVE WIRELESS VIRUSES

DO NOT OPEN THE DOOR!

**IF THE DOOR IS CLOSED THERE IS VIRUS TESTING
IN PROGRESS**



RESTRICTED AREA



Q&A

- Ask if you want to know more
 - **IN SHORT:**
 - What do you want to talk about?

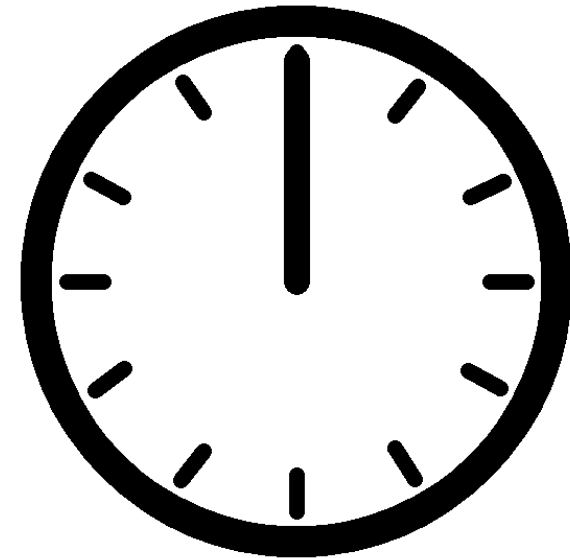


UNFORTUNATE

- We run out of time...

- **IN SHORT:**

- Look me up later





THANK YOU!

boris.cipot@f-secure.com



SECURITY 2013



21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Boris Cipot

F-Secure Corp.

Boris.cipot@f-secure.com

