



Current Threats

how big is the risk really?

Christos Ventouris

InfoSec Specialist
Symantec EMEA



Agenda

Show 7 typical attacks on the Internet
provide advice on how to survive them



Many possible attacks...



Different Motivation – Different Attacks



Common malware flood Today

**1.6 Million
new malware
variants / day**



**11'000 AntiVirus
signatures / day
=
AntiVirus alone
is not enough!**

Greece - Jan – Apr 2013 Stats

| Month | AV Pings | IPS Pings |
|---------------|----------|-----------|
| January 2013 | 33504 | 48993 |
| February 2013 | 28586 | 51334 |
| March 2013 | 29885 | 46701 |
| April 2013 | 35582 | 48488 |

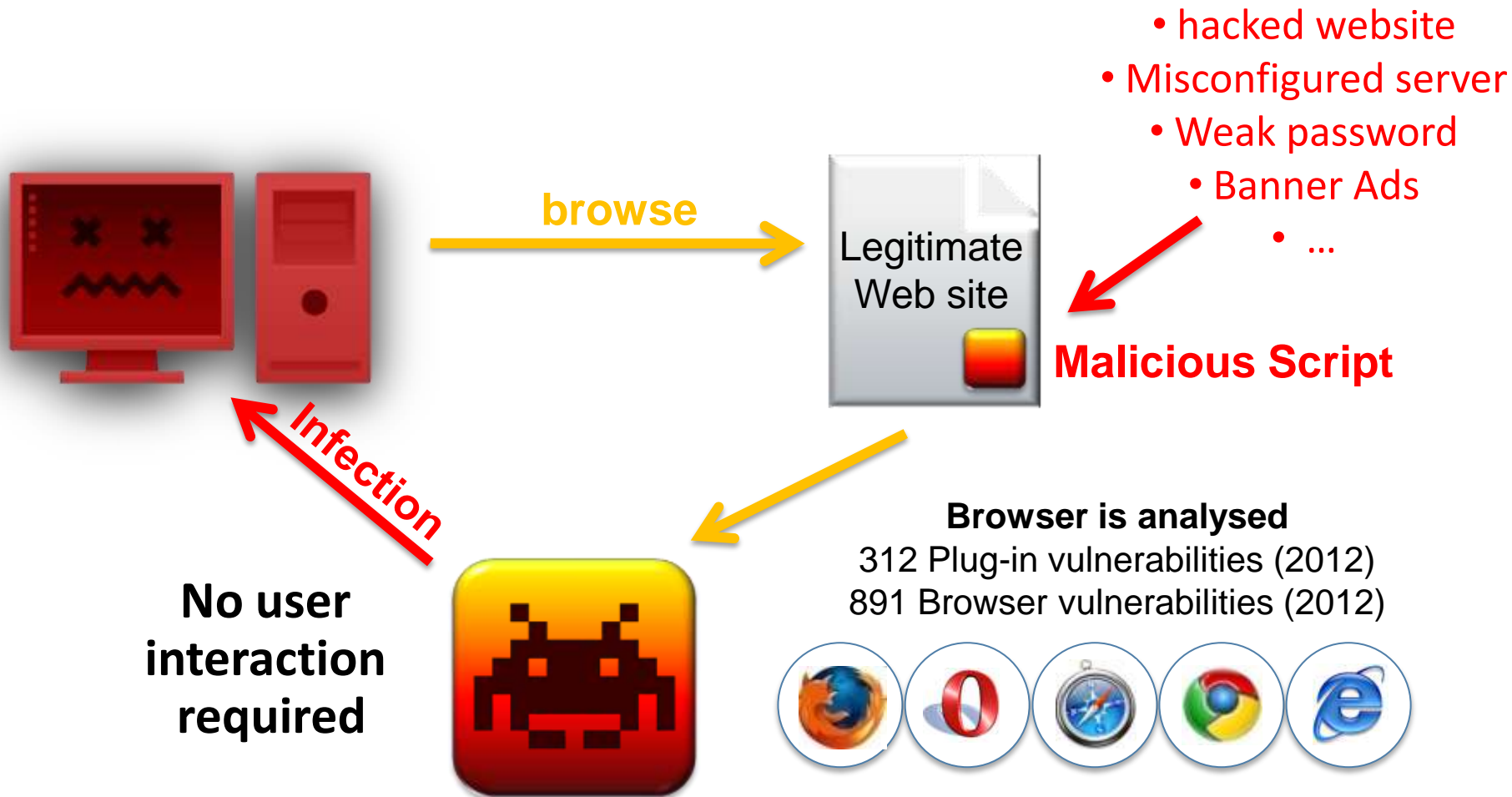
Greece - Apr 2013 Most Top Signatures

| IPS Signature | Hits | Global % |
|-------------------------------------------|-------|------------|
| Facebook Fake Survey 9 | 14947 | 3.3191036 |
| Facebook Fake Plugin 3 | 6745 | 1.3571265 |
| Blackhole Toolkit Website | 4923 | 1.27145486 |
| MSRPC Server Service RPC CVE-2008-4250 | 2001 | 1.20669707 |
| Facebook LikeJacking 13 | 1377 | 3.3993664 |
| Sakura Exploit Kit Website | 5593 | 0.82903105 |
| Malicious Website Accessed 2 | 1002 | 0.15382655 |
| Fake Codec Website 3 | 804 | 9.801292 |
| Sibhost Exploit Kit Website | 995 | 2.2526343 |
| Mass Injection Website 5 | 809 | 0.17133333 |

DriveBy Downloads still popular

- Increased by 30% to ~250'000 blocked Webattacks/day in 2012
 - 1 in 532 Websites was infected
 - 61% of all malicious websites were hijacked legitimate domains
- Blackhole Exploitkit responsible for ~41% of all the attacks
 - Evolution ongoing, fast in integrating new exploits like for Java

Most common: DriveBy Download infections





VIDEO
DriveBy Attack



Advice #1



Protect your computer when surfing!



FBI

FEDERAL BUREAU OF INVESTIGATION

All activity of this computer has been recorded.
If you use a webcam, videos and pictures were saved for identification.



Location:
Your IP-Address:
Your Hostname:

You can be clearly identified by resolving your IP address and the associated hostname.

Your Computer has been locked!

Illegally downloaded material (MP3's, Movies or Software) has been located on your computer.

By downloading, those were reproduced, thereby involving a criminal offense under **Section 106 of the Copyright Act.**

The downloading of copyrighted material via the Internet or music-sharing networks is illegal and is in accordance with **Section 106 of the Copyright Act** subject to a **fine or imprisonment for a penalty of up to 3 years.**

Furthermore, possession of illegally downloaded material is punishable under **Section 184 paragraph 3 of the Criminal Code** and may also lead to the **confiscation of the computer**, with which the files were downloaded.



Please follow the instructions on the right.

Code:

Please enter your Code utilizing the Pin-Pad below.

1 2 3 4 5 6 7 8 9 0

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.



1 Take your cash to one of these retail locations:



2 Pick up a _____ and purchase it with cash at the register.

3 Come back and enter your _____ code to unlock your Computer.

unlock computer:

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$200. Payable through _____. After successful payment, your computer will automatically unlock.

Failure to adhere to this request could involve criminal charges and possible imprisonment.

To perform the payment, enter the acquired _____ code in the designated payment field and press the "Submit" button.



POLICE

ATTENTION!

Pour des raisons de securite, votre systeme Windows a ete bloque.

La raison peut etre la visite des sites infectes ou pornographiques. L'ordinateur est dans un etat critique, en cause de cela le systeme peut perdre tous vos documents et fichiers. Pour avoir la possibilite de restaurer la systeme, vous aurez besoin de telecharger la mise a jour complementaire pour le systeme de securite.

Cette mise a jour paye est destinee egalement pour les systemes infectes. Cette mise a jour va proteger completement votre systeme contre les virus et les logiciels malveillants, va stabiliser votre systeme informatique et va eviter la perte de donnees.

Selectionnez la methode preferable de paiement



POSSIBLE



POSSIBLE

Votre systeme informatique sera restaure (gueri) bientot, pour ce faire vous avez besoin d'entrer un code pour le transfert de 100 euros dans les systemes de Paysafecard ou de Ukash. Vous pouvez l'acheter (code) a n'importe quelle station de gaz ou kiosque a journaux. Ces codes peuvent egalement etre achetes ou les cartes de recharge sont vendu.

Immediatement apres avoir entre un code et la verification de son exactitude, votre systeme informatique sera mis a jour et protege - tous les chevaux de Troie et les virus seront supprimes.



ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΑΤΤΙΚΗΣ

Διωξης Ηλεκτρονικού Εγκλήματος

ΔΙΕΥΘΥΝΣΗ ΑΣΦΑΛΕΙΑΣ ΑΤΤΙΚΗΣ
ΥΠΟΒΑΘΜΟ ΤΜΗΜΑ 5ο
Διωξης Ηλεκτρονικού Εγκλήματος

Προσοχή!

Αυτό το λειτουργικό σύστημα μπλοκάρεται λόγω παραβίασης των νόμων της Ελλάδας! Σημειώθηκαν οι ακόλουθες παραβιάσεις:

Η IP διεύθυνσή σας είναι "109.242.133.156". Από αυτή την IP διεύθυνση επισκέφτηκαν ιστοσελίδες που περιέχουν πορνογραφία, την παιδική πορνογραφία, κτηνοβοσκία, και τη βία κατά των παιδιών. Ο υπολογιστής σας επίσης περιείχε βίντεο που περιλαμβάνει πορνογραφία, βία και παιδική πορνογραφία! Επιπλέον, από το ηλεκτρονικό ταχυδρομείο σας αποστέλλονται μηνύματα με τη μορφή spam, τα οποία περιείχαν τρομοκρατική πρόθεση.

Αυτό το μπλοκάρισμα του υπολογιστή έγινε για να σταματήσουν οι παράνομες δραστηριότητές σας.

Τα στοιχεία σας:

IP:109.242.133.156

Τοποθεσία: Greece, Athens
ISP:

Για να ξεκλειδώσετε τον υπολογιστή, πρέπει να πληρώσετε πρόστιμο 100 ευρώ.

Μπορείτε να πληρώσετε ποινή με δύο τρόπους:

1) Μέσω του συστήματος Ukash:

Για να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής 19-ψήφιο κωδικό και να πατήσετε OK (αν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο OK).

Εάν στη διαδικασία πληρωμής θα γίνει σφάλμα, θα πρέπει να στείλετε τους κωδικούς στη διεύθυνση: economic-crime@hellenicpolice.gr

2) Πληρωμή μέσω Paysafecard:

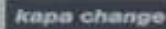
Για να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής ένα 16-ψήφιο κωδικό (αν είναι αναγκαίο, με έναν κωδικό πρόσβασης), και στη συνέχεια κάντε κλικ στο OK (εάν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο OK).

Ukash Πού μπορώ να αγοράσω Ukash?

Μπορείτε να προμηθευτείτε Ukash σε εκατοντάδες σημεία παγκοσμίως, online, από πορτοφόλια, καταστήματα φιλικών και μηχανήματα αυτόματης ανάληψης.



KKT - KKT Αγοραστή την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περίπτερα και καταστήματα τροφίμων & φιλικών



Kapa - Αγοραστή την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περίπτερα και καταστήματα τροφίμων & φιλικών

OK

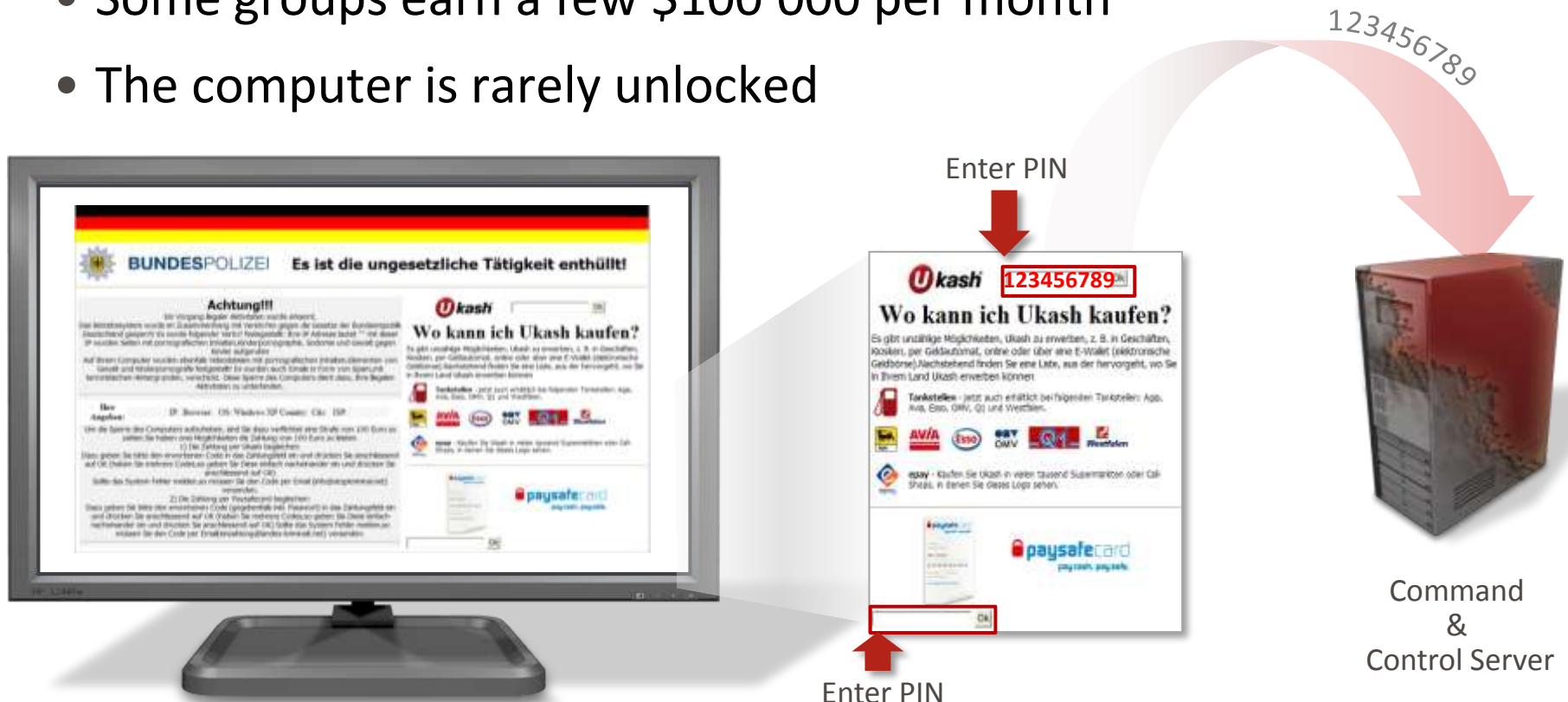
paysafecard Πού μπορώ να αγοράσω Paysafecard?



Payzone Hellas είναι η μεγαλύτερη εταιρεία κινητής τηλεφωνίας top-up δικτύου στην Ελλάδα με εγκατεστημένη πάνω από 11.000 τερματικά POS. Payzone Hellas πρωτογωνιστεί, επίσης, πλήρως λαογραφισμένη και υπηρεσιών κοινής ωφέλειας για την προκαταβολή

Ransomware

- Blocks a user's PC and demands money (2.9% of victims pay)
- User pays \$50-200 by paysafe/UCash/MoneyPak
- Some groups earn a few \$100'000 per month
- The computer is rarely unlocked



Advice #2



Don't pay ransom to malware

Bait Messages in Social Networks



Click-Jacking

The screenshot shows a YouTube interface with a video player and a list of suggestions. The video player is currently paused at 0:00 / 5:00. The video title is "Shocking! April fools day prank turns fatal!" and it is part of an "ExclusiveVideos" playlist with 936 videos. The video is by "BadRrankVids" and has 6,397 likes and 586 dislikes. The video description reads "im never going to play a prank on anyone again after watching this!". The suggestions list includes:

- Running Dog by euphorial, 2,335,501 views, 0:24
- Strip Poker by euphorial, 3,237,339 views, 0:40
- Shoe Thrown at President Bush by euphorial, 341,232 views, 3:40
- Benny Hinn by euphorial, 300,842 views, 2:06
- Adult Prank Gone Wrong by PrankVote, 9,604,987 views, 1:13
- FUNNIEST PRANK YOU WILL EVER SEE! 100% BEST by andyme21, 11,551,556 views, 0:31
- Head in the toilet prank - Just For Laughs by JustForLaughsTV, 19,154,353 views, 1:09

Click-Jacking

FouTube Search Browse Upload Create Account Sign In

Shocking! April fools day prank turns fatal!

Exclusive Videos 936 videos Subscribe

User clicks on invisible LIKE Button

38K

0:00 / 5:00

BadRrankVids April 24, 2010 | 6,397 likes, 586 dislikes

im never going to play a prank on anyone again after watching this!

All Comments (0) see all

Suggestions

- Running Dog**
by euphorial
2,335,501 views
0:24
- Strip Poker**
by euphorial
3,237,339 views
0:40
- Shoe Thrown at President Bush**
by euphorial
341,232 views
3:40
- Benny Hinn**
by euphorial
300,842 views
2:06
- Adult Prank Gone Wrong**
by PrankVote
9,604,987 views
1:13
- FUNNIEST PRANK YOU WILL EVER SEE! 100% BEST**
by andyme21
11,551,556 views
0:31
- Head in the toilet prank - Just For Laughs**
by JustForLaughsTV
19,154,353 views
1:09

Advice #3



**Don't believe every message
you see (in Social Networks)**

A lot of information in social networks

- „Luca2013“ could be my password
- Service to reset lost passwords

Security Question

Name of your pet:

- Also for spammers

Hey, here you get cheap rabbit food

- or for Phishing

Hey, is that your bunny in that picture?
[Fake Facebook <login>](#)



Advice #4



„12345“ is not a good password!

Data Breaches - again and again

- **Twitter** - 250'000 user records stolen in 2013
 - **Scribd** - 500'000 user records stolen in 2013
 - **Evernote** resets 50 Mio accounts after data breach in 2013
 - **LinkedIn** - 6.5 Mio user records stolen in 2012
 - ...
-
- Many of them happen due to SQL injection on the website
 - Very old attack, could be protected by following the best practice

Are you sure that your data is well protected?

Advice #5



**For different services,
use different passwords**

A crowd of people at night, seen from behind, holding up their smartphones. The screens of the phones are lit up and display a blue checkmark inside a yellow circle. The background is dark with some blurred lights, suggesting an outdoor event or concert.

Smartphones

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

Top mobile threats

Web- & Network-based Attacks

Launched by malicious websites or compromised legitimate sites

Attacking site exploits device's browser

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

Malware

Includes traditional computer viruses, computer worms and Trojan horse programs

Example: Ikee worm targeted iOS-based devices

Example: Pjapps enrolled infected Android devices in botnet

Social Engineering Attacks

Leverage social engineering to trick users

Attempts to get users to disclose sensitive info or install malware

Examples include phishing and targeted attacks



Resource Abuse

Attempt to misuse network, device or identity resources

Example: Sending spam from compromised devices

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

Data Loss

Employee or hacker exfiltrates sensitive info from device or network

Can be unintentional or malicious

Remains biggest threat to mobile devices

Data Integrity Threats

Attempts to corrupt or modify data

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

Can also occur unintentionally

Android Malware

- Making money with premium SMS
 - Profit with SMS between \$1.6K-9K / day
- Mobile BotNets exist already
- DriveBy Downloads possible
- Privacy is also an issue
- Mobile vulnerabilities
 - 416 (2012) / 315 (2011)



Heavy use of
social engineering



Fake app markets



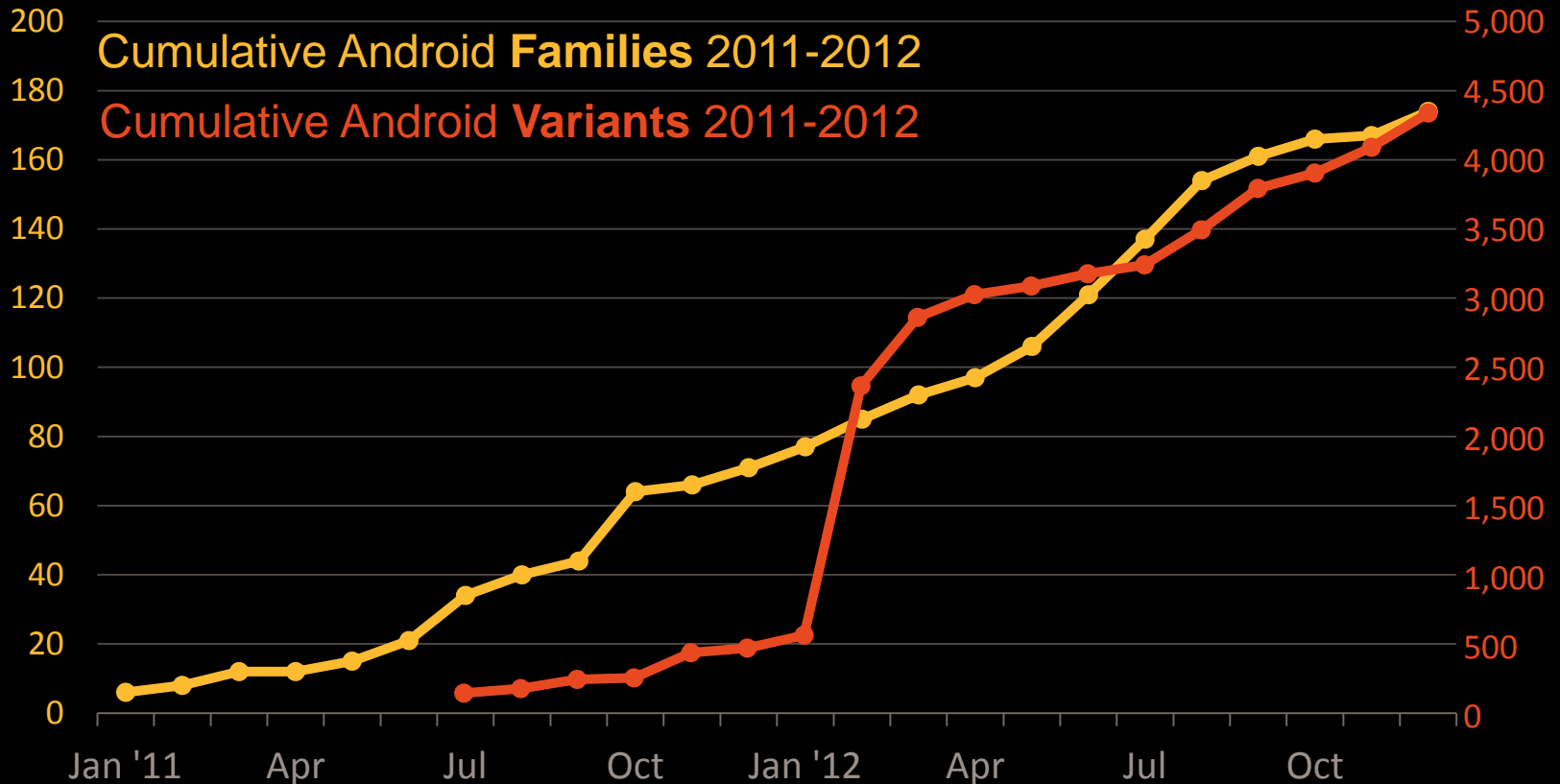
Unique (bad) APK
every time



Sends Premium
SMSs



Android Malware Growth



Advice #6



Don't blindly install mobile Apps

SMS Spam

10.11.2012 20:09

Sie wurden für ein
Gratis-Geschenk von
Apple ausgewählt.
Besuchen Sie
[http://\[REDACTED\].rc7.cc/?
p=0114179](http://[REDACTED].rc7.cc/?p=0114179) [REDACTED]
und geben Sie 3923 ein,
um es anzufordern!

21.03.2013 22:19

Your mobile number
was selected as a
winner of £2,000000.00
with Winning No [03 11
15 20 21 34 35](#). Email:
[andersond \[REDACTED\]@gmail.co
m](#) for claims.

Ihr Mobilfunkbetreiber hat Sie für ein iPhone 5 ausgewählt!



Bitte geben Sie den unten stehenden Code ein

fortsetzen

There is no iPhone, it is just a scam site

Afmelden

Many People clicked it...

0:06 Erhalten Sie ein gratis Apple iPhone 5!
+ Ruti, CH

0:07 Erhalten Sie ein gratis Apple iPhone 5!
+ Saint Gallen, CH

0:11 Erhalten Sie ein gratis Apple iPhone 5!
+ Baar, CH

0:11 Erhalten Sie ein gratis Apple iPhone 5!
+ CH

0:13 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

0:17 Erhalten Sie ein gratis Apple iPhone 5!
+ Sarmenstorf, CH

0:19 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

0:19 Erhalten Sie ein gratis Apple iPhone 5!
+ Bruttisellen, CH

0:19 Erhalten Sie ein gratis Apple iPhone 5!
+ CH

0:24 Erhalten Sie ein gratis Apple iPhone 5!
+ Luzern, CH

0:25 Erhalten Sie ein gratis Apple iPhone 5!
+ Geneve, CH

0:27 Ontvang een gratis Apple iPhone 5!
+ Schaffhausen, CH

0:27 Erhalten Sie ein gratis Apple iPhone 5!
+ Zurich, CH

0:28 Erhalten Sie ein gratis Apple iPhone 5!
+ Geneve, CH

0:32 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

0:32 Erhalten Sie ein gratis Apple iPhone 5!
+ Zurich, CH

0:33 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

0:36 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

0:39 Erhalten Sie ein gratis Apple iPhone 5!
+ Baden, CH

0:43 Erhalten Sie ein gratis Apple iPhone 5!
+ Wabern, CH

0:44 Erhalten Sie ein gratis Apple iPhone 5!
+ Derendingen, CH

0:48 Erhalten Sie ein gratis Apple iPhone 5!
+ CH

0:50 Erhalten Sie ein gratis Apple iPhone 5!
+ Bern, CH

0:51 Erhalten Sie ein gratis Apple iPhone 5!
+ Luzern, CH

0:52 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

0:53 Erhalten Sie ein gratis Apple iPhone 5!
+ CH

1:02 Erhalten Sie ein gratis Apple iPhone 5!
+ Bern, CH

1:03 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

1:08 Erhalten Sie ein gratis Apple iPhone 5!
+ Volketswil, CH

1:09 Erhalten Sie ein gratis Apple iPhone 5!
+ Schaffhausen, CH

1:11 Erhalten Sie ein gratis Apple iPhone 5!
+ CH

1:28 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

1:30 Erhalten Sie ein gratis Apple iPhone 5!
+ CH

1:35 Erhalten Sie ein gratis Apple iPhone 5!
+ Full, CH

1:37 Erhalten Sie ein gratis Apple iPhone 5!
+ Castagnola, CH

Advice #7



Don't fall for (mobile) scams

Summary

1. **Protect your computer (when surfing)**
2. **Don't pay ransom to malware**
3. **Don't believe every message you see (in Social Networks)**
4. **Use strong passwords and not ,123456'**
5. **For different services, use different passwords**
6. **Pay attention when installing mobile apps**
7. **Don't fall for (mobile) scams**



A nighttime photograph of a city skyline with several illuminated skyscrapers. In the foreground, a multi-lane highway shows long-exposure light trails from cars, with white and red streaks indicating traffic flow. A yellow rounded rectangular box is superimposed over the middle of the image, containing the text.

Which questions are open?

Thank you for your attention!

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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