The Kaspersky Security Symposium

Sep 21 – 23, 2011 | Munich | Germany

Digital Communism

Your Data is Owned by Everyone

Stefan Tanase, Senior Security Researcher, Kaspersky Lab

stefant@kaspersky.ro | twitter.com/stefant | pgp_keyid: 0xdd749e1b

Welcome

About myself

- **Stefan Tanase** - Senior Security Researcher,
  Global Research and Analysis Team, Kaspersky Lab

- Joined Kaspersky Lab in **2007**,
  based in **Bucharest, Romania**

- Special interest in web security,
  web based threats, malware 2.0

- Honeypots, web crawlers,
  distributed computing, AI

- Often speaking at **major security conferences** such as Virus Bulletin, RSA, AVAR or IDC.

Let’s start with a quiz!

How simple it is to analyze viruses?

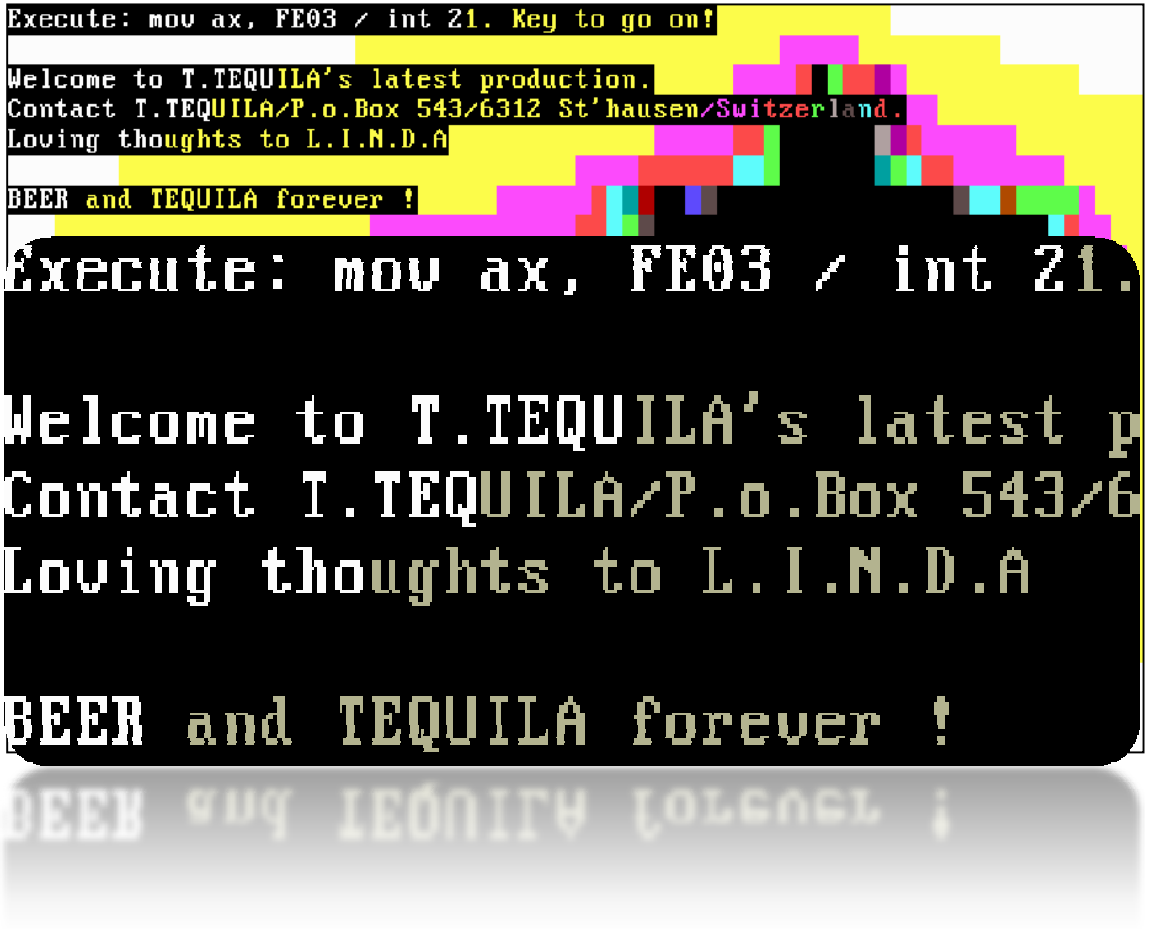
KASPERSKY lab

Name the virus! (1988)

The image on the left was displayed by which virus?

- Melissa
- CodeRed
- DenZuk
- Michaelangelo

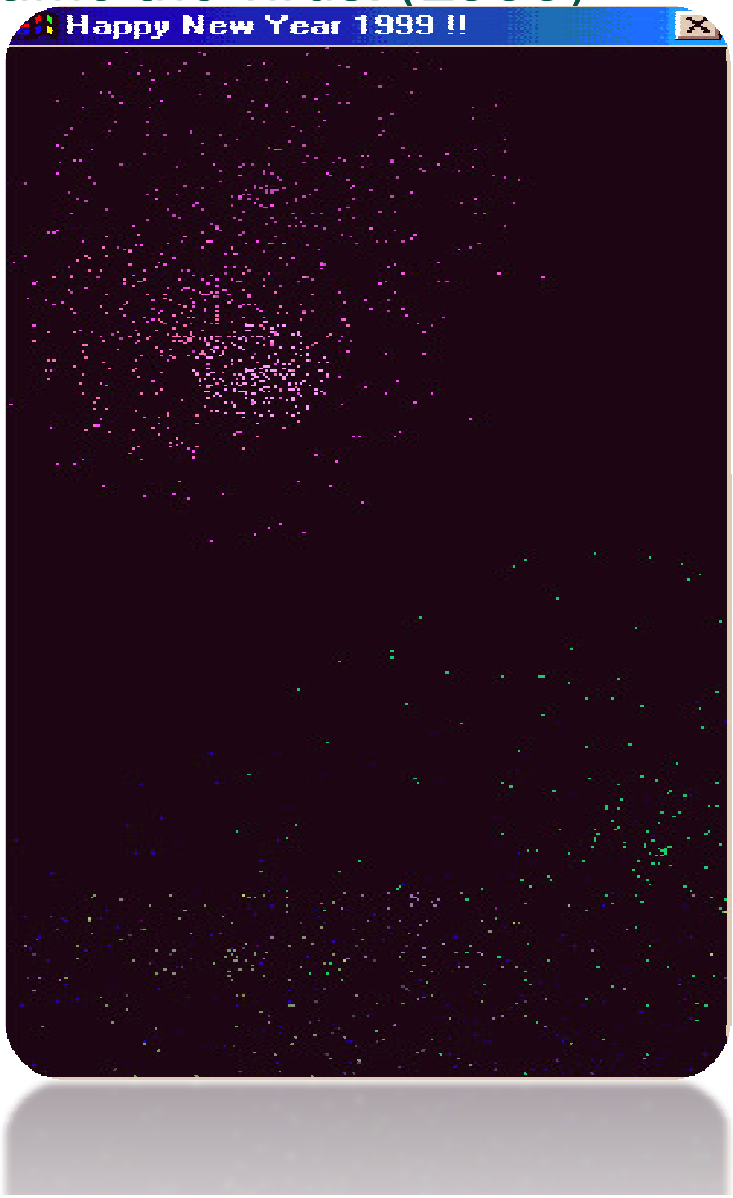
Name the virus! (1991)



The image on the left was displayed by which virus?

- Jabber
- Tequila
- BadSectors
- One_Half

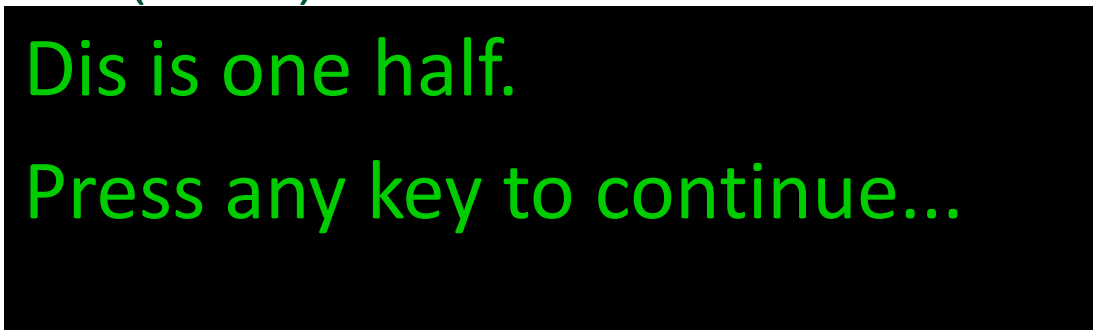
Name the virus! (1999)



The image on the left was displayed by which virus?

- CodeRed
- Melissa
- Happy99
- Cascade

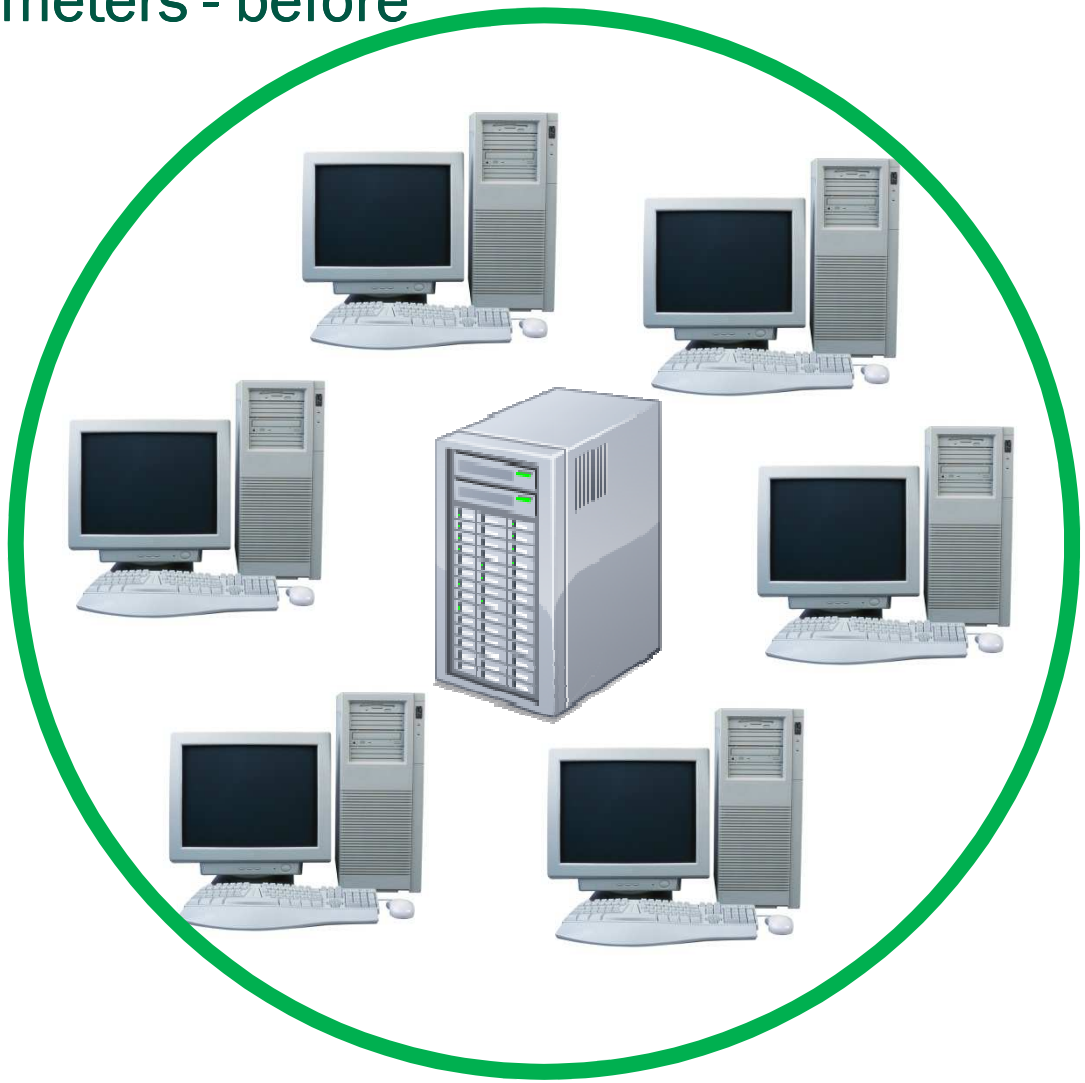
Name the virus! (2000)



What virus displays the following message after **encrypting 50% of your HDD?**

- NetSky
- OneHalf
- Ebola
- 50 Cent

Security perimeters - before

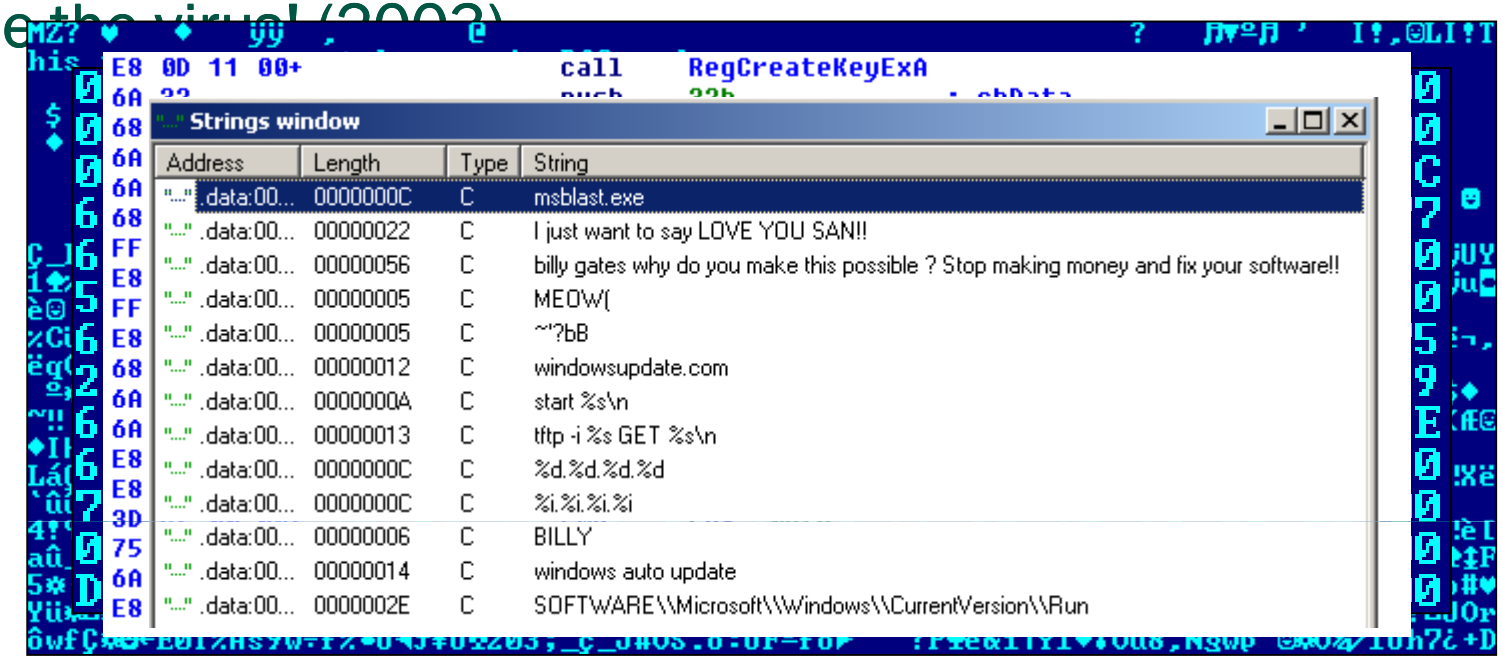


That was simple!

But what about nowadays?

KASPERSKY lab

Name the virus! (2003)



What's the name of the virus above?

a) MyDoom

b) MyTob

c) Rbot

d) Blaster

Security perimeters - now

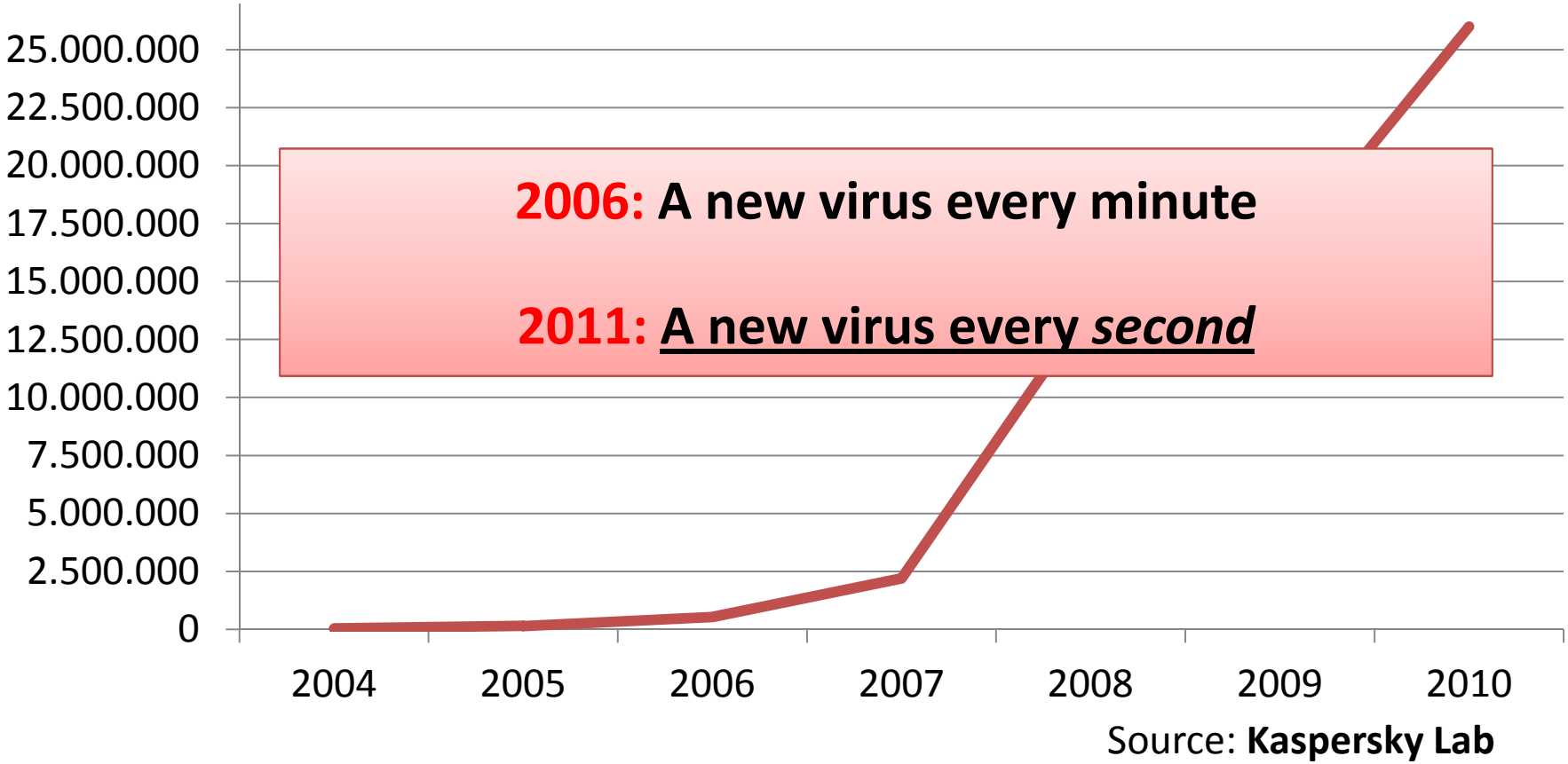
Cybercrime today

Big numbers, sophisticated threats

KASPERSKY lab

Worrying numbers

- **Kaspersky Lab** processes **more than 70,000** new malicious programs (viruses, Trojans, worms, adware, etc.) **every day**



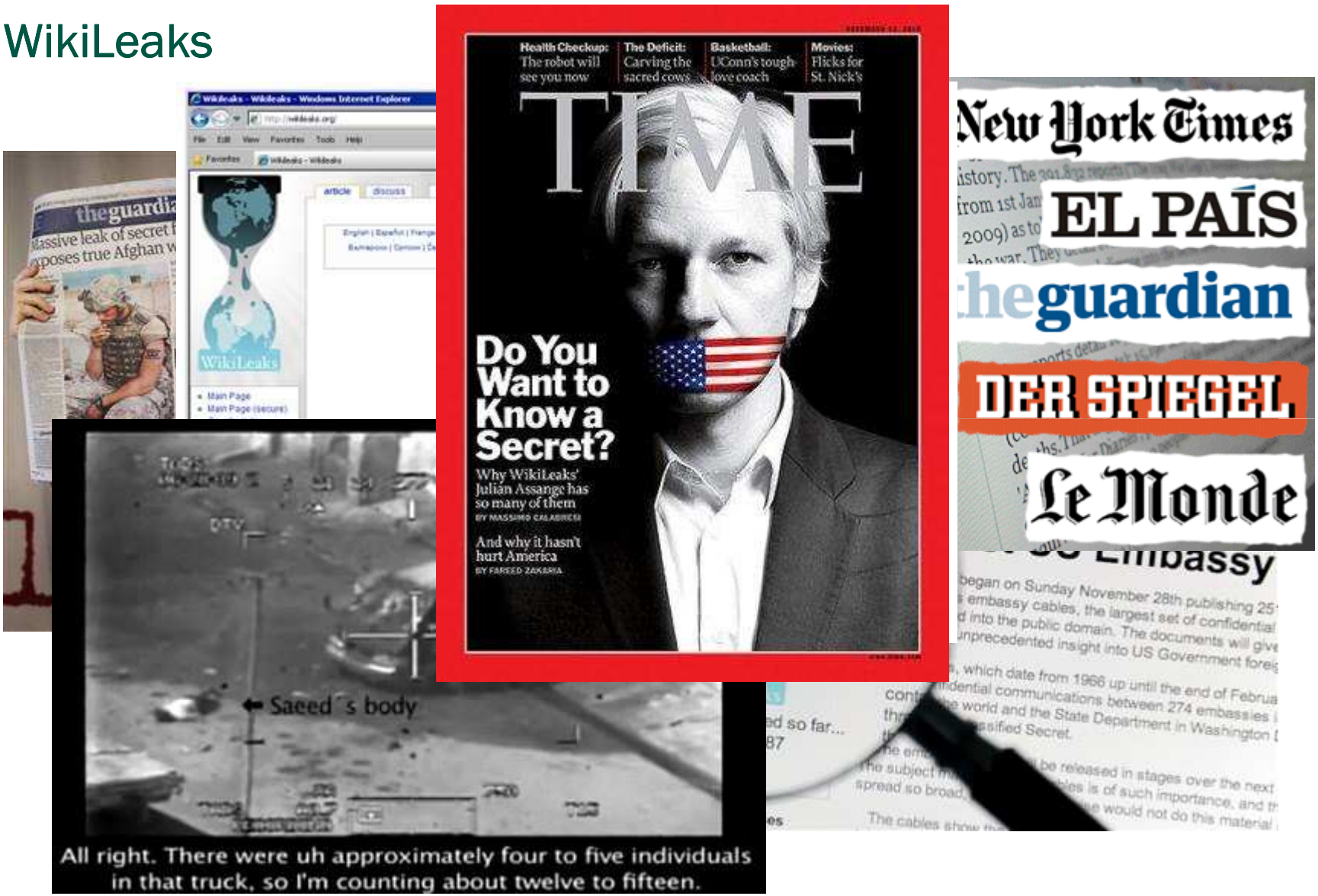
Raising the stakes in the cybercrime game in 2011

- Guessing game:
  - For **thousands of years** we've been willing to go to extraordinary lengths and **travel far and wide** to get our hands on it
  - We like it **fresh, crystal clear** and **uncontaminated**
  - We're **thirsty** for it

Information is like water…

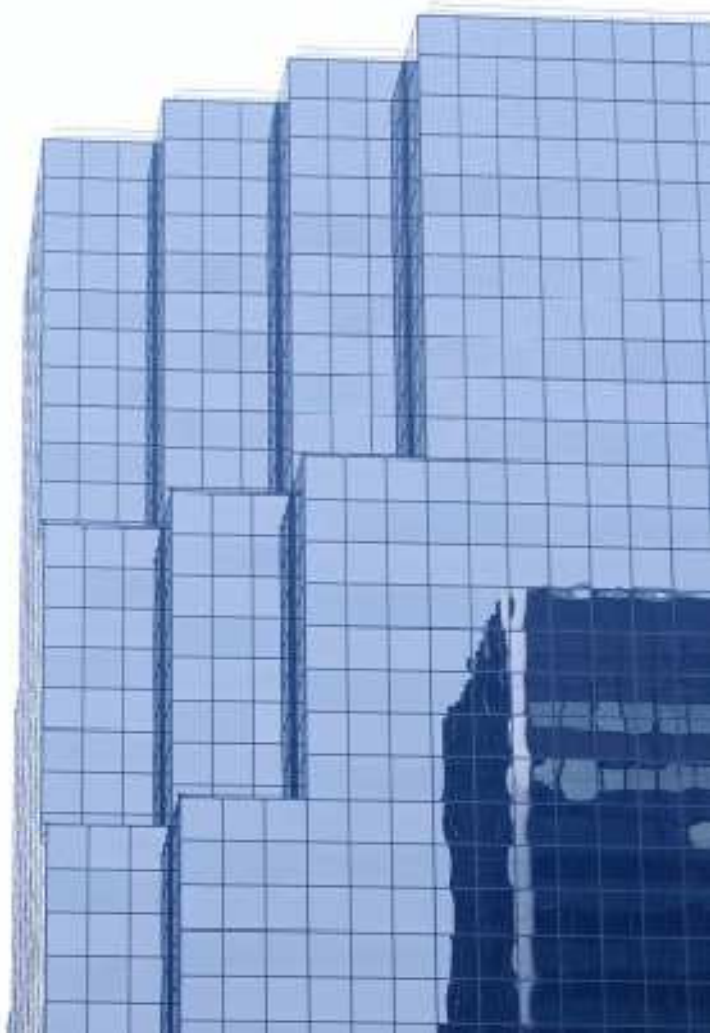
It leaks

WikiLeaks


Health Checkup: The robot will see you now
The Deficit: Carving the sacred cows
Basketball: UConn's tough-love coach
Movies: Flicks for St. Nick's
TIME
Do You Want to Know a Secret?
Why WikiLeaks' Julian Assange has so many of them
BY MASSIMO CALABRESI
And why it hasn't hurt America
BY FAREED ZAKARIA
New York Times
EL PAÍS
theguardian
DER SPIEGEL
Le Monde
WikiLeaks
Saeed's body
All right. There were uh approximately four to five individuals in that truck, so I'm counting about twelve to fifteen.

Where do leaks come from?
The big players

- One notable source is *governments and corporations.* What's leaking from them?
  - Diplomatic cables, intelligence reports, telephone intercepts, companies' internal documentation, etc.
- High stakes: national security, global economy
  - Hundreds of billions of dollars invested in protecting data like this
- Very secure infrastructure
  - …or is it?



Where do leaks come from?
The small players

- And another source is the *average computer user.*
  - Passwords, bank account details and credit card numbers
  - Chat logs, family photos, personal documents

- The stakes are **lower**, but they are always **relative:**
  - You don't need to be anyone special to own data which is important to **you**

- How secure is an **average personal computer**?

Data-stealing malware

Big numbers, sophisticated threats

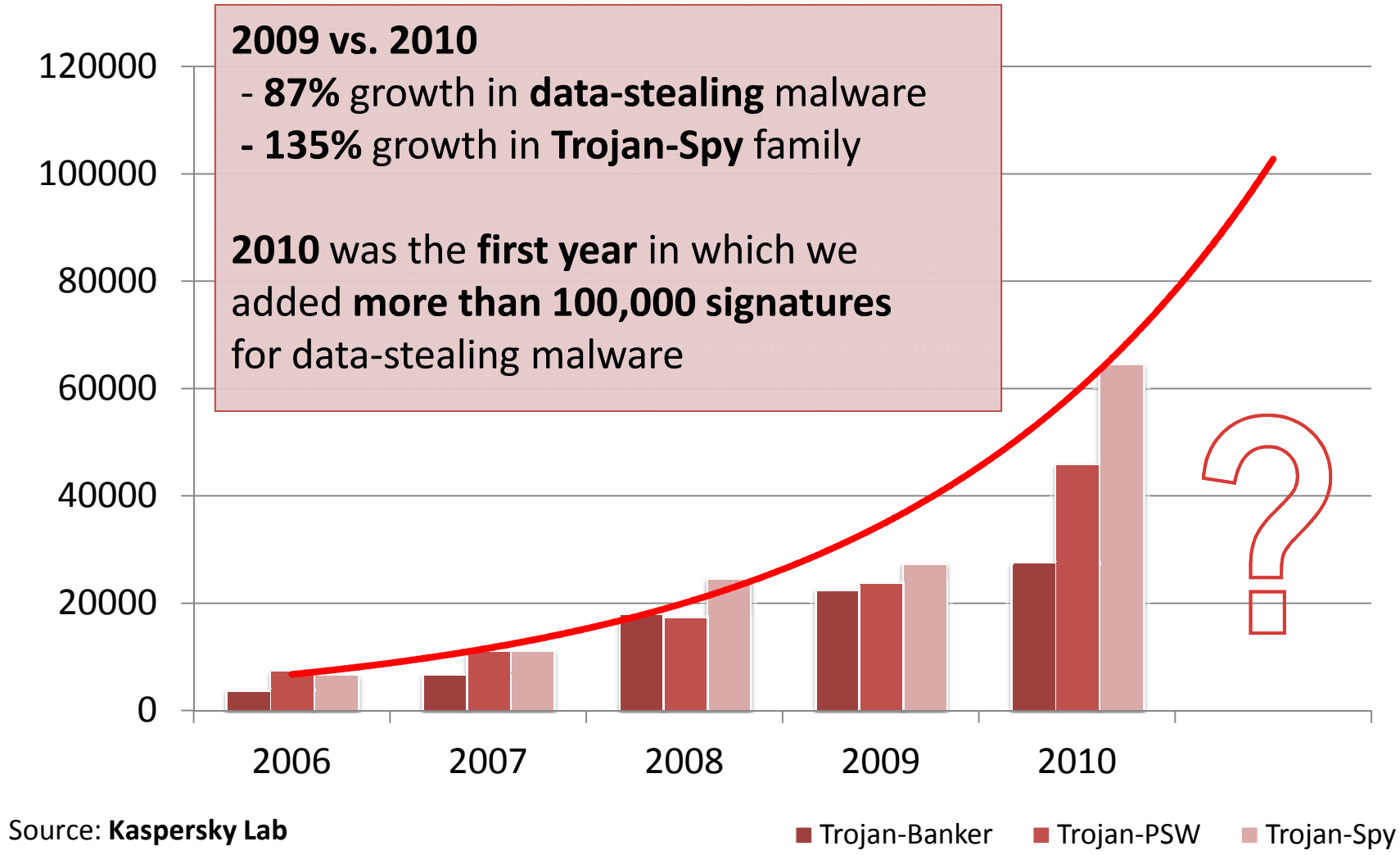
KASPERSKY lab

The data-stealing malware landscape

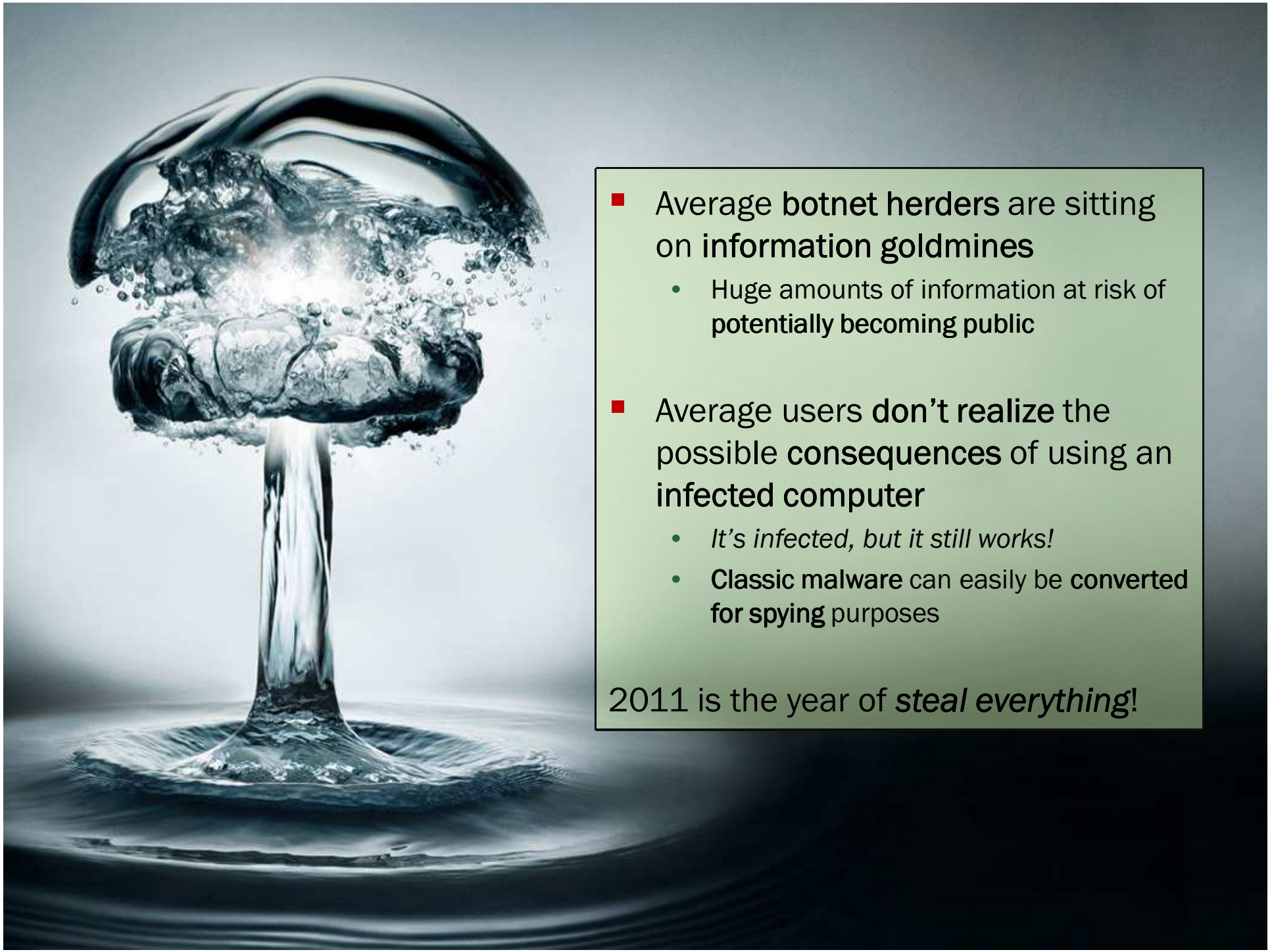
- **How many infected computers are out there?**
  - Literally **hundreds of millions** of infected computers
  - **Classic botnet operations**
  - Stay **under the radar**
  - Classic **monetization** techniques

  - **Trojan-Banker** programs are designed to steal user account data relating to **online banking** systems, **e-payment** systems and plastic card systems
  - **Trojan-PSW** programs are designed to steal user account information such as **logins and passwords** from infected computers
  - Trojan-Spy programs are used to **spy on a user's actions** (to track data entered via the keyboard, make screen shots, retrieve a list of running applications, etc.)

Growth in data-stealing malware



Source: **Kaspersky Lab**

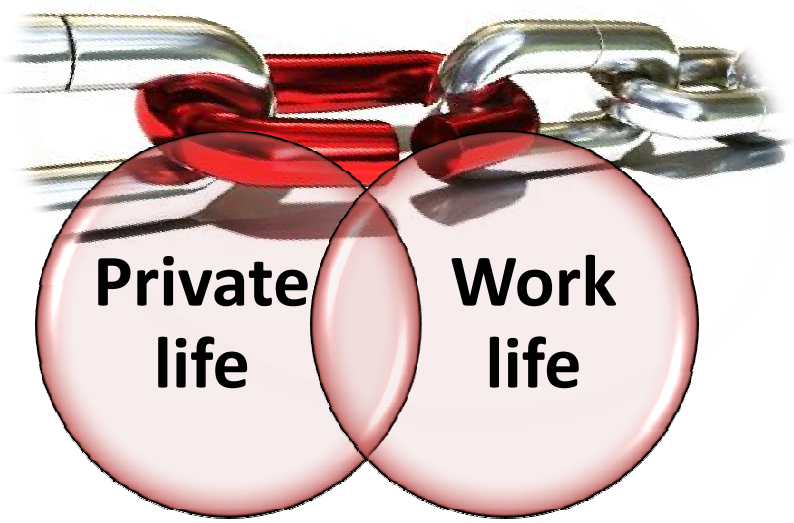


- Average **botnet herders** are sitting on **information goldmines**
  - Huge amounts of information at risk of **potentially becoming public**
- Average users **don't realize** the possible **consequences** of using an **infected computer**
  - *It's infected, but it still works!*
  - **Classic malware** can easily be **converted for spying** purposes

2011 is the year of ***steal everything***!

Work life vs. private life

- Have you ever used your **personal email** for **business purposes?**
- What kind of **topics** have you discussed?
- Did you at least **delete** those emails?

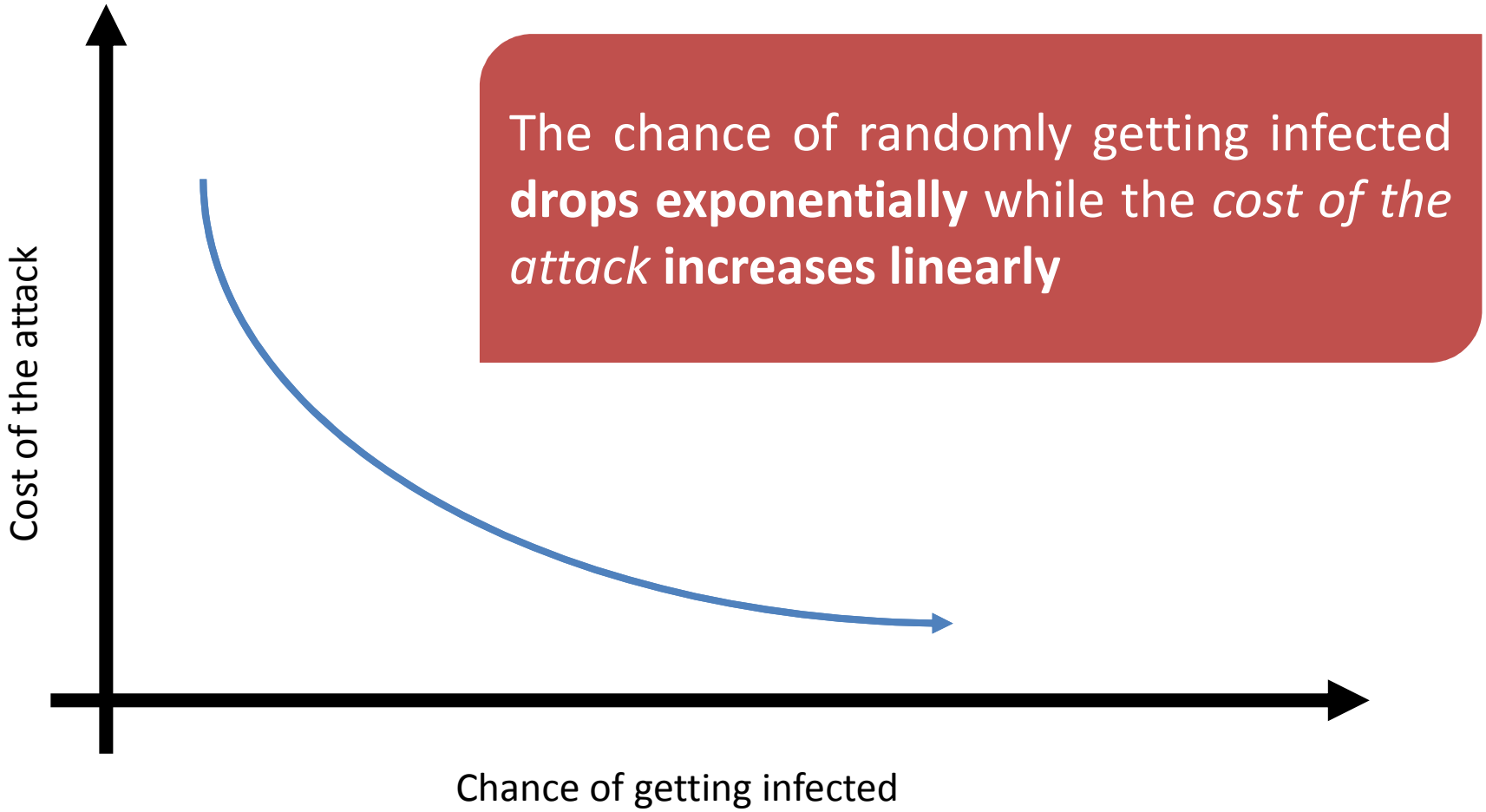


Staying alive

Or how to increase the *cost of an attack*

KASPERSKY lab

Simple math for advanced protection
The basic theory for staying secure



The chance of randomly getting infected **drops exponentially** while the *cost of the attack* **increases linearly**

Achieving a higher *cost of attack* (aka technical advice)

KB SSL Enforcer

- Use Windows 7 x64 (64 bits)
  - CPU with NX support, **64 bits**
  - Macs are NOT safer (they're just less targeted)
- Use modern browsers for accessing the Internet
  - Chrome's unique sandboxing of plugins provide higher securit
  - Install the **KB SSL Enforcer plugin** to force HTTPS links
- Keep Windows, MS Office, Adobe Reader, Flash updated
  - Also: JAVA, QuickTime, Winamp, VLC, etc.
  - Any other application, especially if used on the Internet or with files downloaded from the Internet
- Rely on more than one layer of defense
  - The more defense layers, the higher the cost for the attacker
- Use a VPN to access the Internet while traveling
  - Especially at **WiFi spots**
  - Though it's more expensive, **2G networks can be sniffed too!**

Google Chrome

Some more advice, not just technical

- Only use secure environments
  - **Public computers** are a **no-no**
  - If you *have* to use them to send a message, consider using a **disposable mailbox**!
- Securing your own environments
  - **Keep malware off** your computers and smartphones
- Use complex passwords, unique for each account
  - Uppercase, lowercase, numbers and symbols
  - At least 8 characters (the more, the better!)
- Physical security
  - What if you **lose the device**? What if you're traveling?
  - **Encryption** - data (storage and transmission channels)
  - **Backup** - you can't have encryption without backing up
- Education
  - How many parents teach their children **not to talk to strangers**? How many parents teach their children **not to share their personal documents on P2P networks**?

KASPERSKY

Thank you

Stefan Tanase, Senior Security Researcher, Kaspersky Lab
stefant@kaspersky.ro | twitter.com/stefant | pgp_keyid: 0xdd749e1b