



Malware = business risk

The evolving threatscape

Ryan Naraine, *Security Evangelist*

ryan.naraine@kaspersky.com

September 2008

Who am I?

My background

- Security Evangelist – Kaspersky Lab USA
 - Liaison with virus analysts and threat watchers in Moscow HQ
 - Write about malware-related alerts, warnings and interim mitigations
 - Advise customers on risk-management procedures
- Editor, ZDNet Zero Day (<http://blogs.zdnet.com/security>)
 - Daily tracking of malicious hacker activity, malware outbreaks, vulnerability warnings
- Former editor-at-Large/Security, eWEEK Magazine

Five years as researcher/writer tracking Internet and computer security issues and trends.

Kaspersky Lab



- The world's largest privately-held anti-malware company
- 70+% annual growth in 2004-2006
- 130% growth in 2007 Sales
- Over 250 million protected users worldwide
 - 100,000 new users added each week!
- Global market leader in technology licensing
- 900+ employees
 - ~1/3 in R&D; ~1/5 in customer support

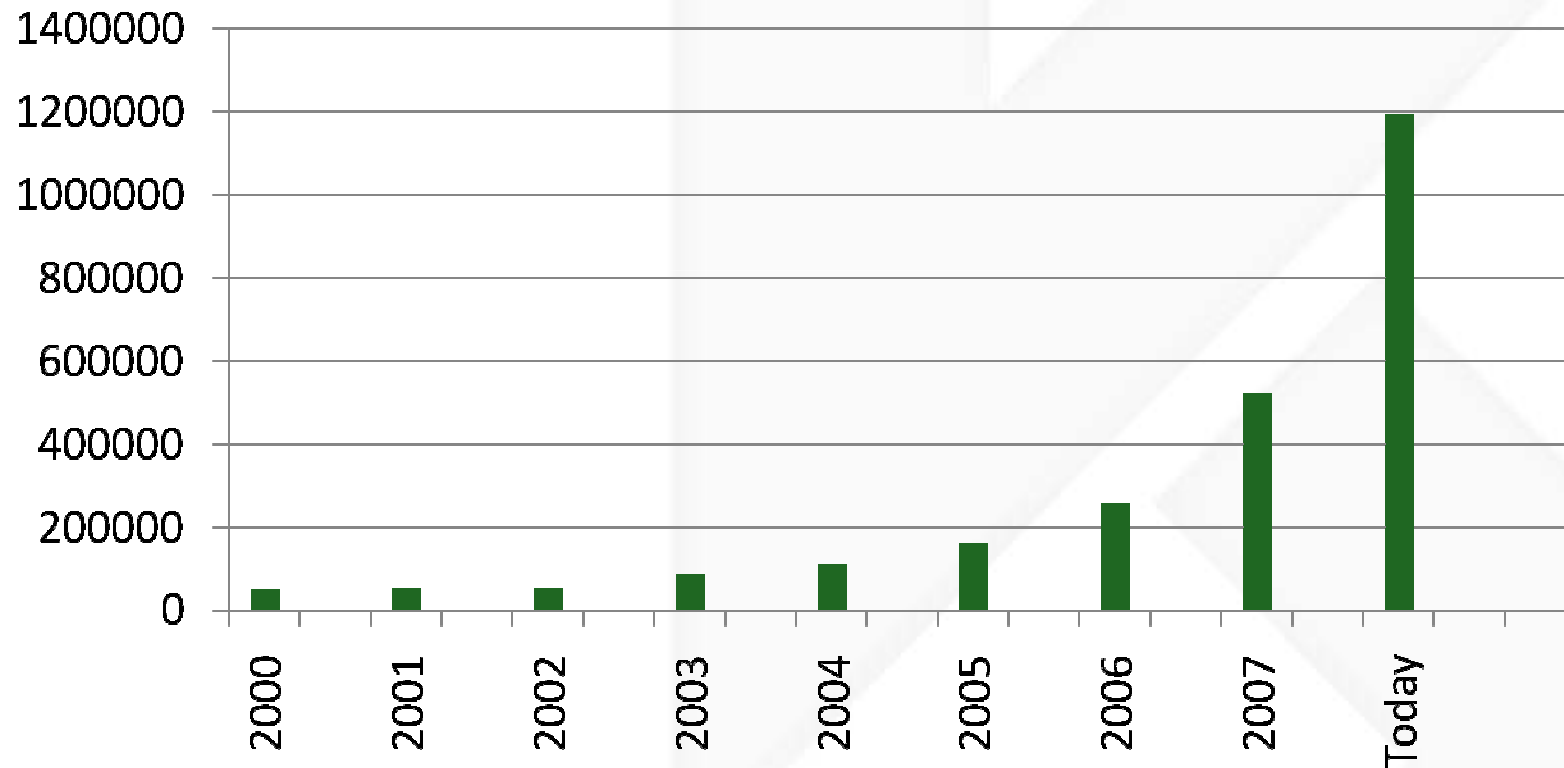
Agenda

Cybercrime: From nuisance to billion-dollar business

- Malware growth rates
- The Web = preferred malware delivery mechanism
- Designer Malware
- Drive-by downloads, exploits
- Weakest Links
- Risk management

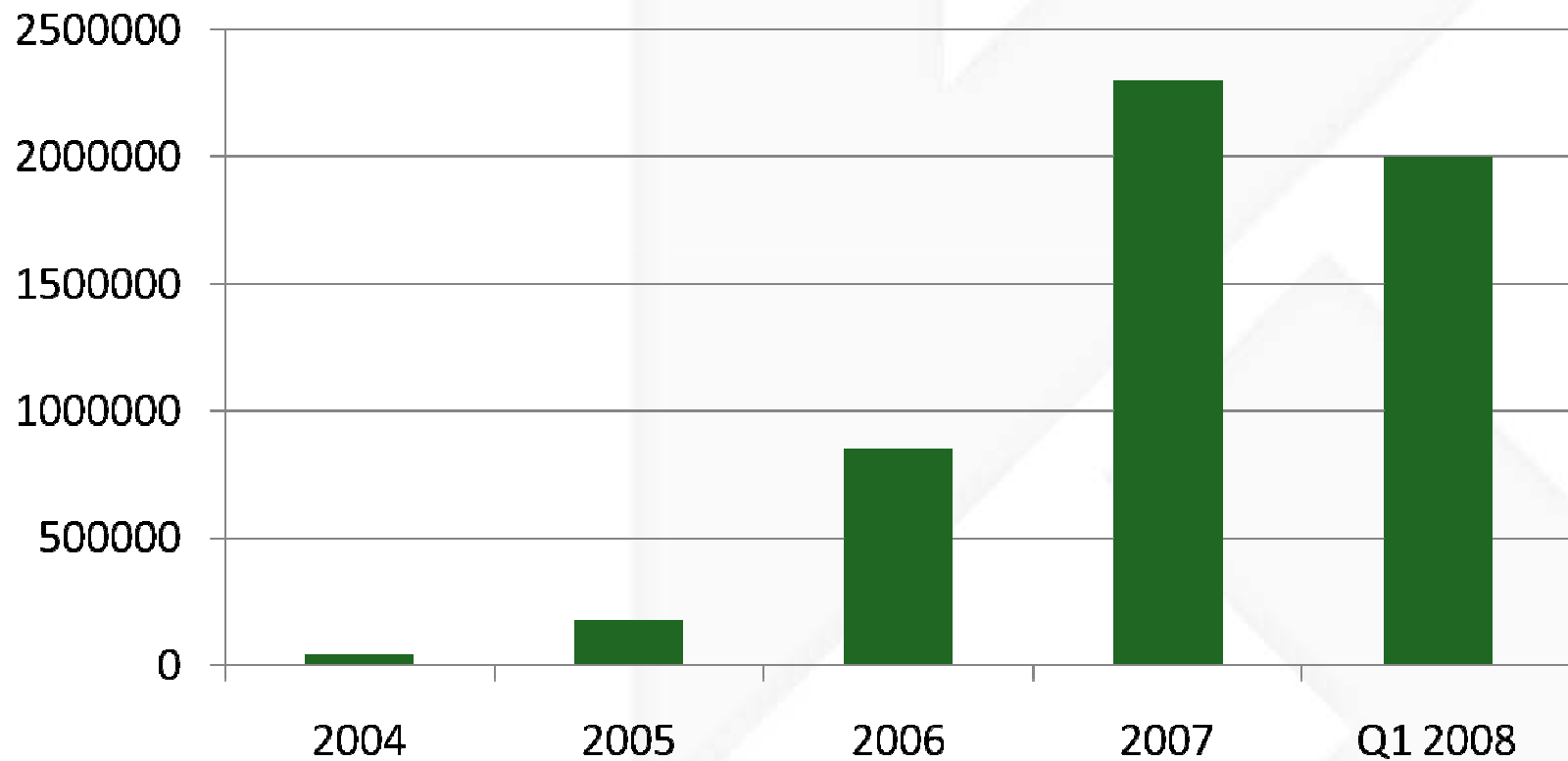
Malware growth rates

Signatures Added – Yearly



Malware growth rates

Objects Detected – Yearly



A bird's eye view from Microsoft

- Microsoft Malicious Software Removal Tool (MSRT)
 - Released every month -- Patch Tuesday
 - Performs automated disinfections of malware families on fully-patched Windows machines
 - Latest version includes signatures for *140+ different* malware families
- 2H07: MSRT removed malware from 15.8 million computers worldwide – 80% increase over 1H07
- Total number of disinfections in 2H07 rose to 42.2 million, an increase of ~120% over 1H07

A bird's eye view from Microsoft

Other highlights:

- *In 2H07, the MSRT cleaned about 8 computers for every 1,000 executions (1 out of every 123 computers on which it ran each month).*
- *There was a Trojan or a Trojan downloader (crimeware) on more than half of those machines.*
- *Over 90% of all e-mail sent over the Internet is spam. The majority of these e-mails are lures for malware.*

1998 - 2003

- **E-mail worms**

Melissa, VBS/Loveletter, Sircam, Bropia

- **Network worms**

Code Red, Blaster, Sasser, Slammer, Sobig, Nimda

(Targeted servers, mail systems, network shares – causing billions of dollars in damages, cleanup)



After the worm...



- **Adware and Spyware**

Pop-up advertising nuisance

- **Spam**

Fake Rolexes, pharmaceuticals,
Nigerian scams

No longer a nuisance, profit is now
the motive. Target: OS, DBs

2008: The Web under siege

- **Phishing attacks**

Trawling for credit card data

- **Fake security software**

Social engineering, scareware

- **Malvertisements**

Flash ads on legit sites launching exploits

- **Drive-by downloads**

Botnets, rootkits, exploit kits...



The next wave...

facebook

Ryan Naraine

Friends

Applications

Inbox

Application Directory

Applications You May Like

Most Active Users

Newest



Slide FunSpace

By Slide, Inc.

Over 6 BILLION videos and more exchanged on Slide FunSpace! Find & share videos, posters, graffiti, and more with all your friends!

22,153,751 monthly active users — 200 friends — 1,090 reviews



Movies

By Flixster

Compare your taste in movies with friends. Share reviews. Discover new movies. Test your movie knowledge with the Never-Ending Movie Quiz.

5,136,331 monthly active users — 146 friends — 157 reviews



Top Friends

By Slide, Inc.

Own your profile with Top Friends! Now you can CUSTOMIZE your Top Friends Profile! Choose your skin, add music and more. Give and receive exclusive awards, show off your mood and keep tabs on the people you really care about with Top Friends News!

19,358,432 monthly active users — 124 friends — 1,093 reviews



SuperPoke!

By Slide, Inc.

Why just poke when you can SuperPoke!? Hug, throw a sheep or choose from over 180 other actions to do to your friends!

4,924,673 monthly active users — 101 friends — 328 reviews