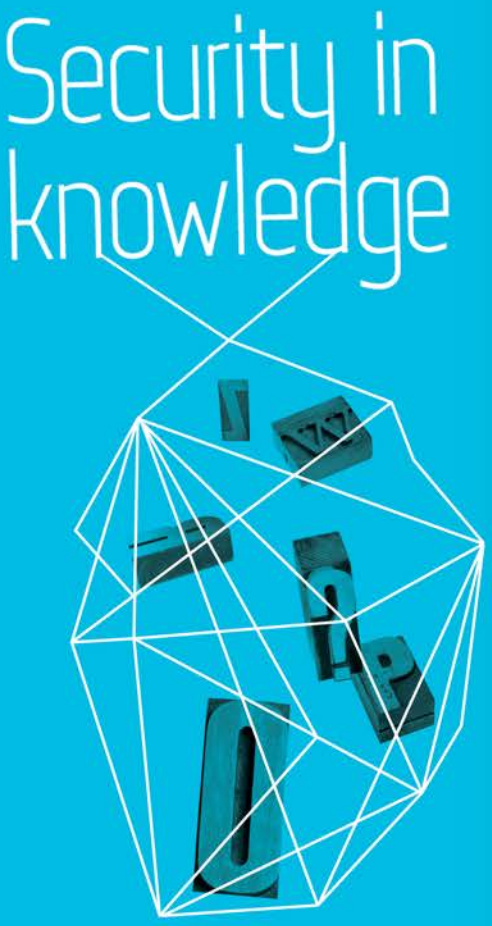


THE IT SECURITY INDUSTRY: SURVIVAL IN THE AGE OF CYBERWARFARE

Eugene Kaspersky
Kaspersky Lab

Session ID: EXP-T19
Session Classification: General Interest

SOURCES OF ATTACKS

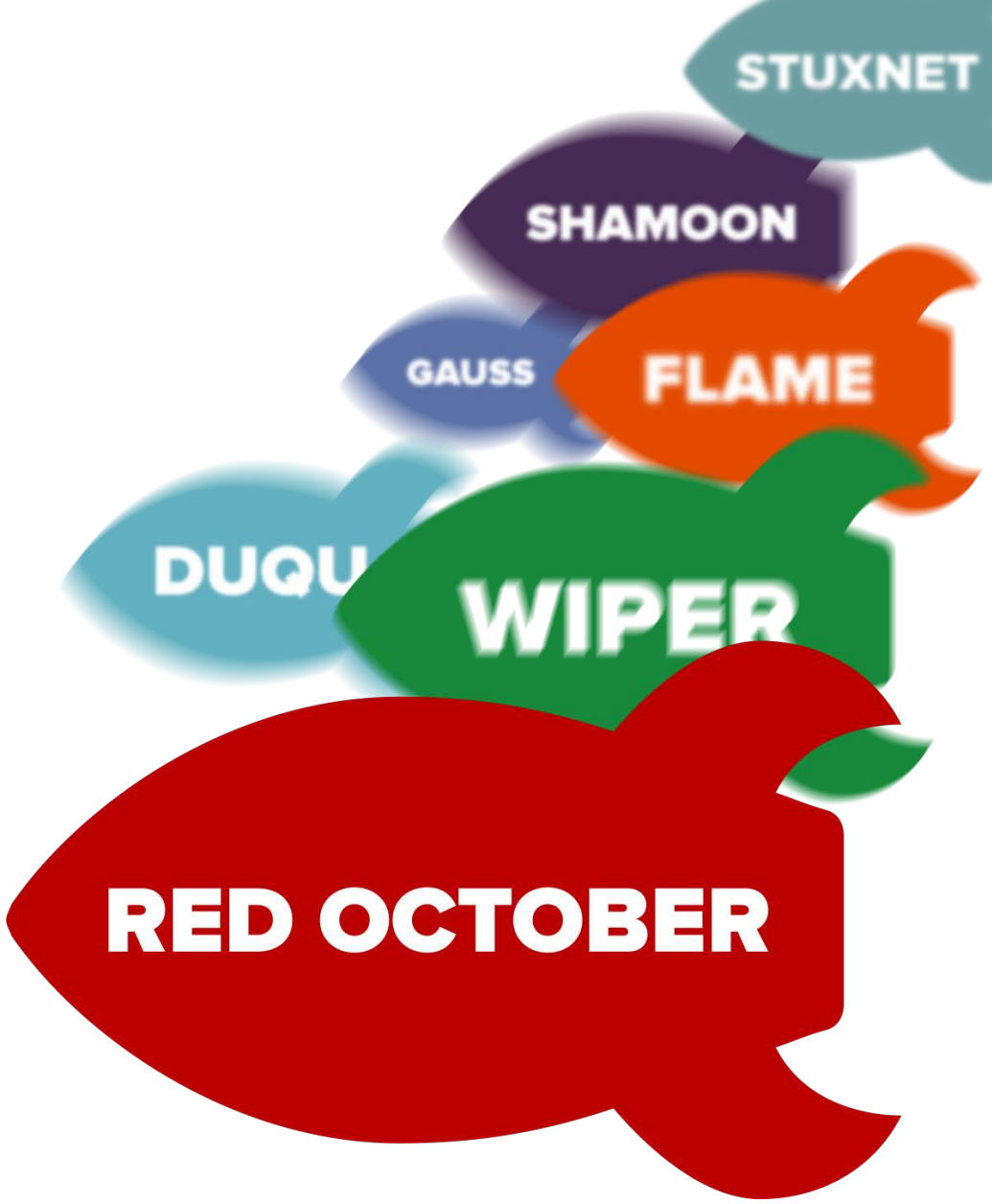
- Cybecriminals
- Hacktivists
- Government agencies
- Terrorists

MOTIVATION

- Financial
- Reputation damage
- Political
- Military
- Sabotage / scare tactics

CYBERTOOLS

- Espionage
- Sabotage
- Terrorism



THE ABCs OF CYBERWEAPONS

A – Attribution almost impossible

B – Boomerang effect

C – Collateral damage

D – Defense much harder than offense

E – Ease of development

CRITICAL TARGETS

Industrial systems

- Stuxnet – Iran, 2010

Critical IT infrastructure

- Shamoon – Saudi Aramco, 2012

Telecommunications

- DDoS – Estonia, 2007

ANATOMY OF HIGH PROFILE ATTACKS

:loop

- Gathering data on the target network
- Detailed analysis of the data
- Attack vector selected
- Malware tested
- Delivery method chosen
- Implementation

go to loop

PROTECTION AGAINST TARGETED ATTACKS

- Strict admin policies & education
- Technologies
- Government regulation & international cooperation

SECURE OPERATING SYSTEM

- Microkernel
- Network security scenarios + filters

THE RULES OF THE GAME ARE CHANGING

- **25+ years ago:**
  - Script kiddies
  - Antivirus
- **10+ years ago:**
  - Criminals; later – hacktivists
  - Internet Security suites / Endpoint Security
- **Now:**
  - Sophisticated attackers, including government agencies
  - Solution?...

IT SECURITY INDUSTRY CHALLENGES

- Detecting mass malware infections
- Detecting pinpointed cyberwarfare strikes
- Detecting **all** threats – regardless of origin or purpose

Thank you!