The Militarization of Cyberspace, [Version 1.0]

There is a new asymmetric threat rising from the darker spheres of the internet. Large, global networks of hijacked computers run by criminals can suddenly transmute into mercenary armies and attack the infrastructure of a country.The role of botnet warlords and their zombie armies in current military strategies and the implications on privacy.

Erich Moechel   Vienna PrivacyOS 2009 10 27

Evolution of the Botnets: 1999 - 2002

- After Melissa, ILOVEYOU etc. worms started transporting more and more trojans from 1999.
- CNN, Yahoo et al. downed by DDoS attack 2000
- Trojans and worms start dominating hitlists
- Phishing attacks on eBay, Paypal & Co 2001
- Sporadic DDoS-Attacks: Japan, Falun Gong et al. US accusing China on DoD network attacks
- 2002 “Identity Theft” on the rise in the US
- DDoS-Blackmail against gambling websites

Evolution of the Botnets: 2002 - 2005

- Black market: Botnet herders, spammers, phishers, fraudsters etc.
- Around 2003 first large phishing waves hit European banking systems
- More worms: Slammer, Mydoom, Netsky, Sober sporting new features
- Global zombie PC count 2005: one million. Phishing reaching a climax

Evolution of the Botnets 2005 -2007

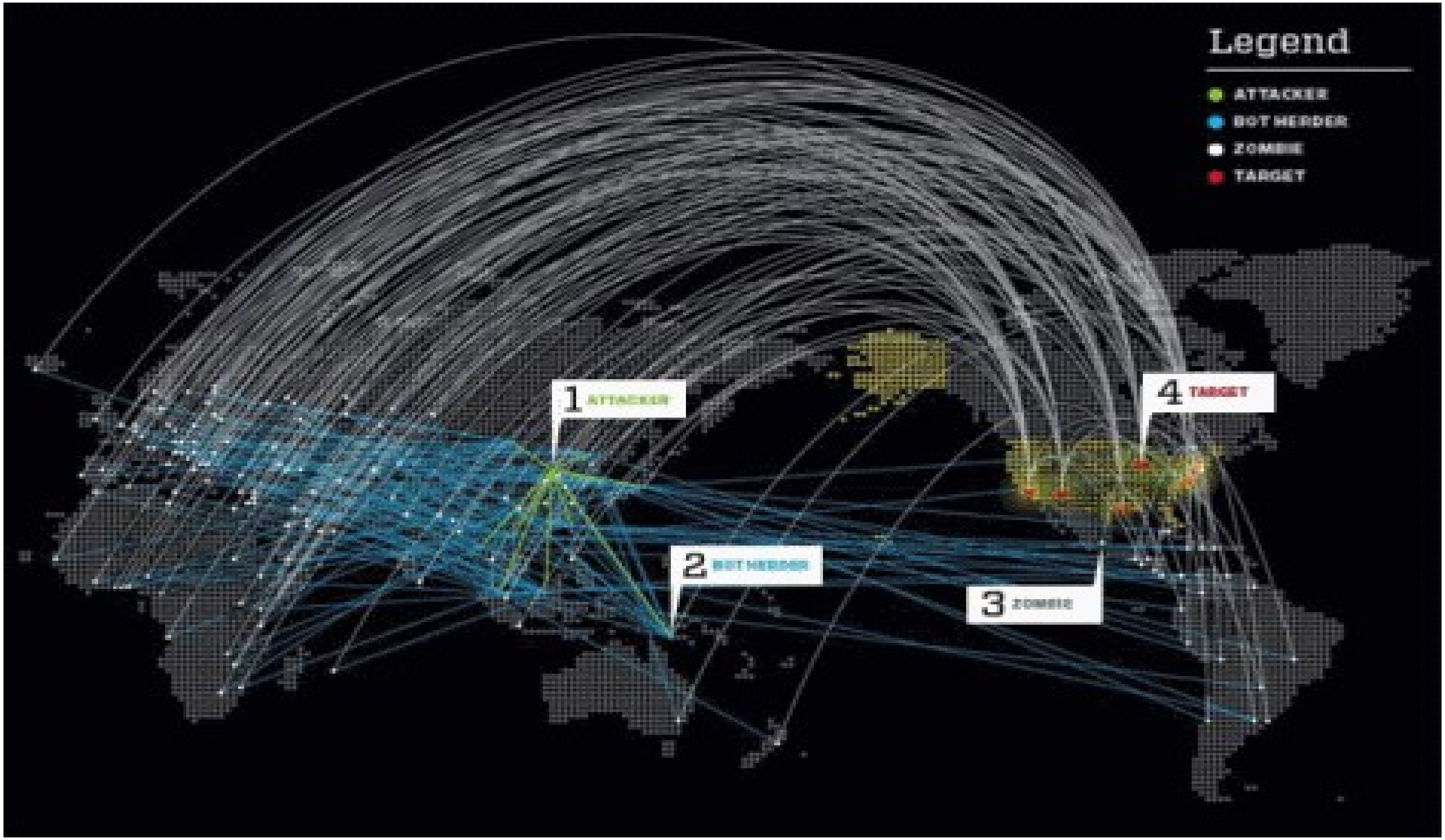
- 60 percent of new malware trojan type
- Targeted attacks using zero day exploits at Tibetan and Falun Gong dissenters
- Fully fledged malware suites hit the market
- Rise of the super botnets: RBN, Srizbi, Rustock, Storm.
- Estonia cut off by a massive DDoS-Attack

Evolution of the Botnets 2007 -2009

- Browser plug-ins become a primary source of infections
- Rent-a-botnet for DDoS on medium targets for less then 5K USD
- Malware distribution shifting from e-mail to multiple channels. “Drive by“ infections.
- Differentiation in botnet types

DDos attack at US targets

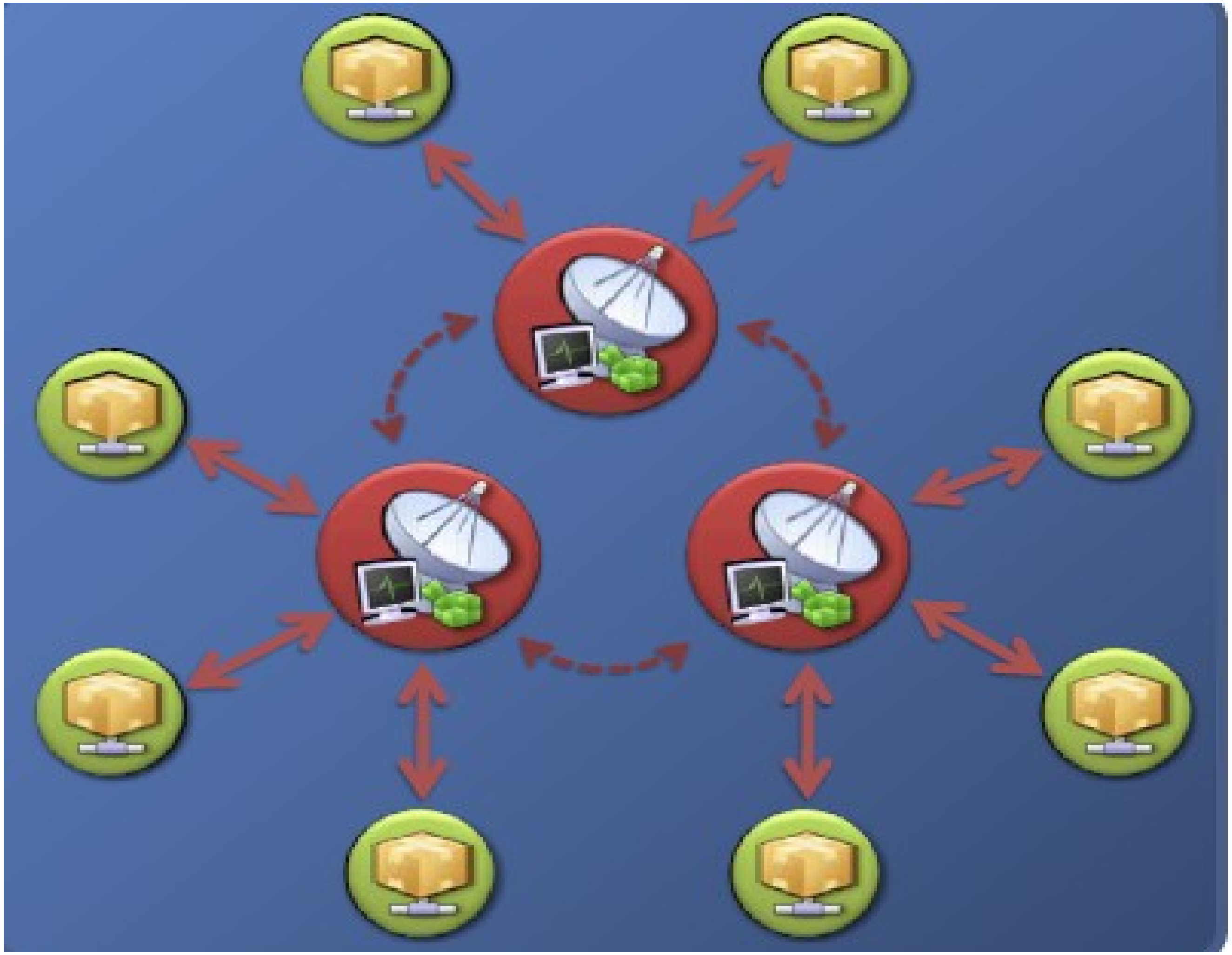
[image creator unknown]



„Independence Day“: The DDoS Attacks on South Korea, July 2009

- Three major waves around July 4 2009
- Banking sector hit, Online banking halted for days
- Sophisticated „fast flux“ programming
- Fire and forget: Fully automated, rotating command/control
- No supersize but „upper middleclass“ botnet. Estimated 50. – 150.000 PCs

Type of botnet most likely used in South Korea [graph courtesy damballa.com]



The lessons of „Independence Day“

- The better the defender's IT infrastructure the more firepower has an attacking DDoS force.
- This topples a strategic axiom valid since antiquity: Infrastructure and topography always counted on the defending side.
- Much more impact with improved timing of attacks and/or use of a supersize botnet
- Attack first mistaken as a „symbolic“ event, very late initial reaction by the Korean government

Recent numbers form the darker spheres of the internet

- 14 million newly infected PCs in Q2 2009, or 150K per day.
- Rustock and Cutwail botnets currently sporting up to two million zombie PCs each
- Spam capacity 1-3 billion e-mails per hour
- Price drop in botnet rentals below 1K USD for mid scale DDoS attacks.

The botnet dilemma from a military perspective

- Massive cyber attacks hard to detect early, harder to assess, impossible to counter
- Mindless mercenaries attack from around the globe and inside a beleaguered country
- No visible enemy to engage – no retaliation
- A dozen specialists, half a year and 200K USD cash are enough to constitute a zombie PC army big enough to take down the USA

Contact, coordinates

For more information and contact data:
http://moechel.com
email:
firstname@lastname.com

key id: **0x007DB429**
fingerprint
9F49 57E7 8824 26C8 78B5 F3B6 F416 7AFB 007D B429