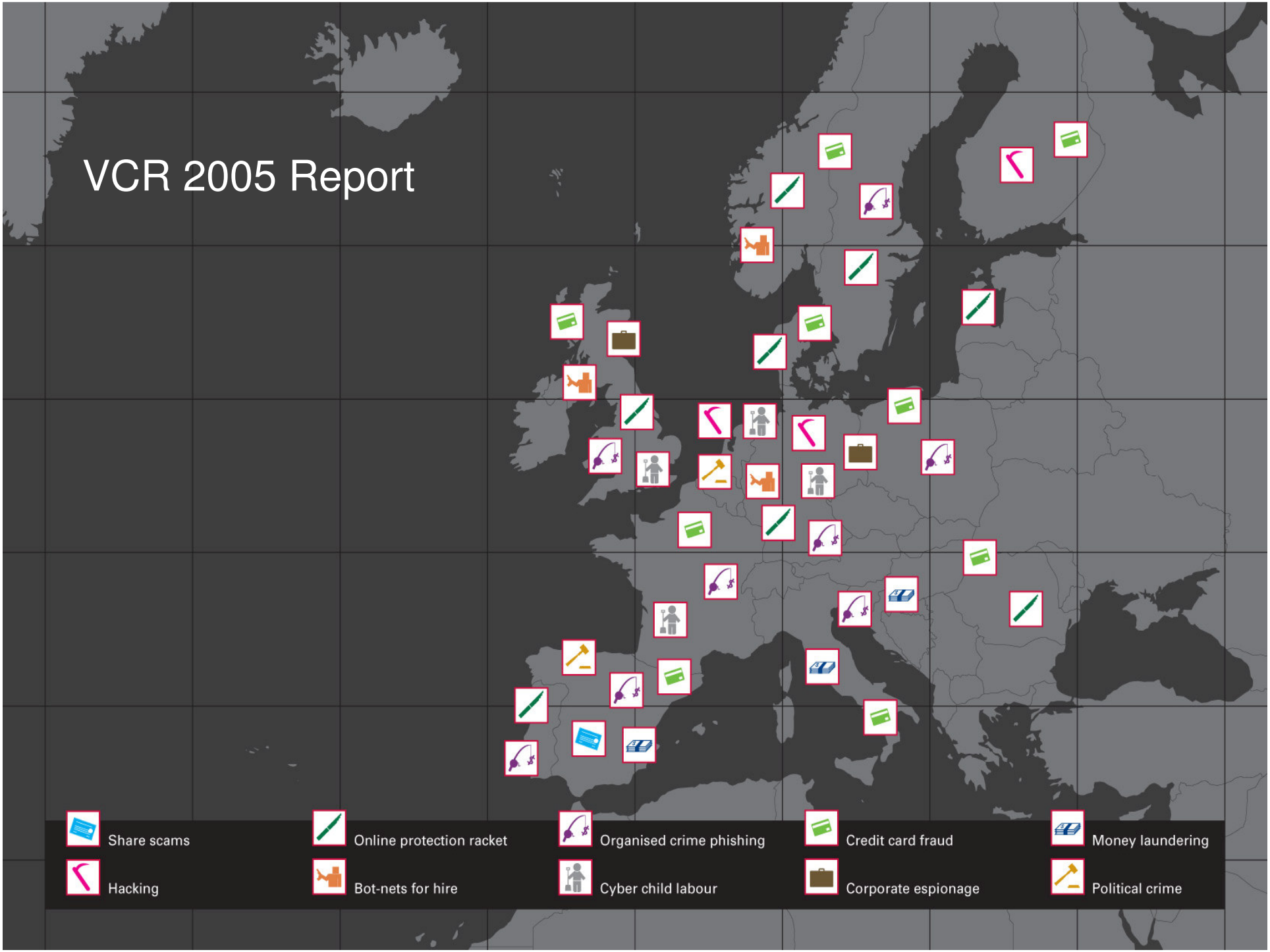
McAfee

Virtual Criminology & Threat Reports

Greg Day
EMEA Security Analyst
AVERT member


VCR 2005 Report
Share scams
Online protection racket
Organised crime phishing
Credit card fraud
Money laundering
Hacking
Bot-nets for hire
Cyber child labour
Corporate espionage
Political crime

McAfee Virtual Criminology 2005

- Rejuvenation of traditional crimes
  - Extortion (business & consumer)
    - Mafiaboy (2000)
      - DDoS tool, utilized >70 computers
      - $1.7bil in damages by slowing DoS websites (inc CNN, Yahoo, Amazon & eBay
    - Ransomware (2006)
      - Helen Barrows (CryZiP), 40yr old Nurse from Rochdale
  - Theft (information & money)
    - Michael Haephrati + wife (PWS-Hotworld trojan)
      - 10-11Gb of data inc marketing plans, business plans, & details of new products from their systems
    - Gozi Trojan collects data from over 5000 consumer and 300 companies
      - Steals SSL session data through IE exploit, Data sent to a server in St. Petersburg
      - sold on a subscription basis, black market street value of US$2million
  - Financial fraud
    - Keyloggers
      - London offices of the Japanese bank Sumitomo Mitsui
        - Keyloggers Foiled In Attempted $423 Million Bank Heist
    - Phishing
    - Nigeria scams (Online dating)
    - Identity Theft/Password stealers
      - Haxdoor
      - Nordea bank ($11m) & over 600 other financial institutions targeted

VCR 2006 Report

McAfee

FROM PURISTS TO PROFITEERS: THE CYBERCRIME FOOD CHAIN

Perpetrators of cybercrime today range from the amateurs with limited programming skills who rely on pre-packaged scripts to execute their attacks, right through to the well-trained professional criminals who are armed with all the latest resources.

THE INNOVATORS

Who? Focused individuals who devote their time to finding security holes in systems or exploring new environments to see if they are suitable for malicious code

Why? The Challenge

How? Embrace the challenge of overcoming existing protection measures and seek to break in through the back door

Danger Rating: Low

These purists, the 'elite threat authors', only make up 2% of the hacking and malware author population

THE AMATEUR FAME SEEKERS

Who? Novices of the game with limited computing capabilities and programming skills

Why? Hungry mainly for media attention

How? Use ready-made tools and tricks

Danger Rating: Moderate

Threat lies in the unleashing of attacks without really understanding how they work

THE COPY-CATTERS

Who? Would-be hackers and malware authors

Why? The celebrity status of the cybercrime community has prompted an upsurge of those desperate to replicate their formulae for fame

How? Less focused on developing something new and more interested in recreating simple attacks

Danger Rating: Moderate

THE INSIDERS

Who? Disgruntled or ex-employees, contractors and consultants

Why? Revenge or petty theft

How? Take advantage of inadequate security, aided by the privileges given to their positions within the workplace

Danger Rating: High

This group is a growing and serious security problem

THE ORGANISED CYBER-GANGSTERS

Who? Highly motivated, highly organised, real-world cyber-crooks
Limited in number but limitless in power

Why? Intent on breaching vulnerable computers to reap the rewards

How? Like in most communities of successful criminals, at the centre is a

tight core of masterminds who concentrate on profiteering by whichever means possible – but surrounding themselves with the human and computer resources to make that happen

Danger Rating: High

McAfee Virtual Criminology 2006

The Cyber Gang & recruiting techniques

- 68 of 77 Students admitted to engaging in activity that could be classified as deviant (Purdue university 2006 – Computer science students).
- “If you have people reading in the media that other people are making a lot of money from cybercrime – and if they have the criminal intent – then they are definitely also going to take that path” – Dave Thomas Section Chief FBI, Cyber division
- Virtuality of the crime – VCR report
- “If you can find a young person, perhaps a student, before his options have fully matured, then make him truly believe in your cause, he will server you for many years”. (Former KGB Maj. Gen. Oleg Kalugin).
- Thrill is a drug like addiction – e.g. Shiva Brent Sharma
- Average hacker age 14 – 19 Robert Schifren
- “Cybercriminals see the internet as a job opportunity” – Dave Thomas, FBI

AVERT 2007 predictions

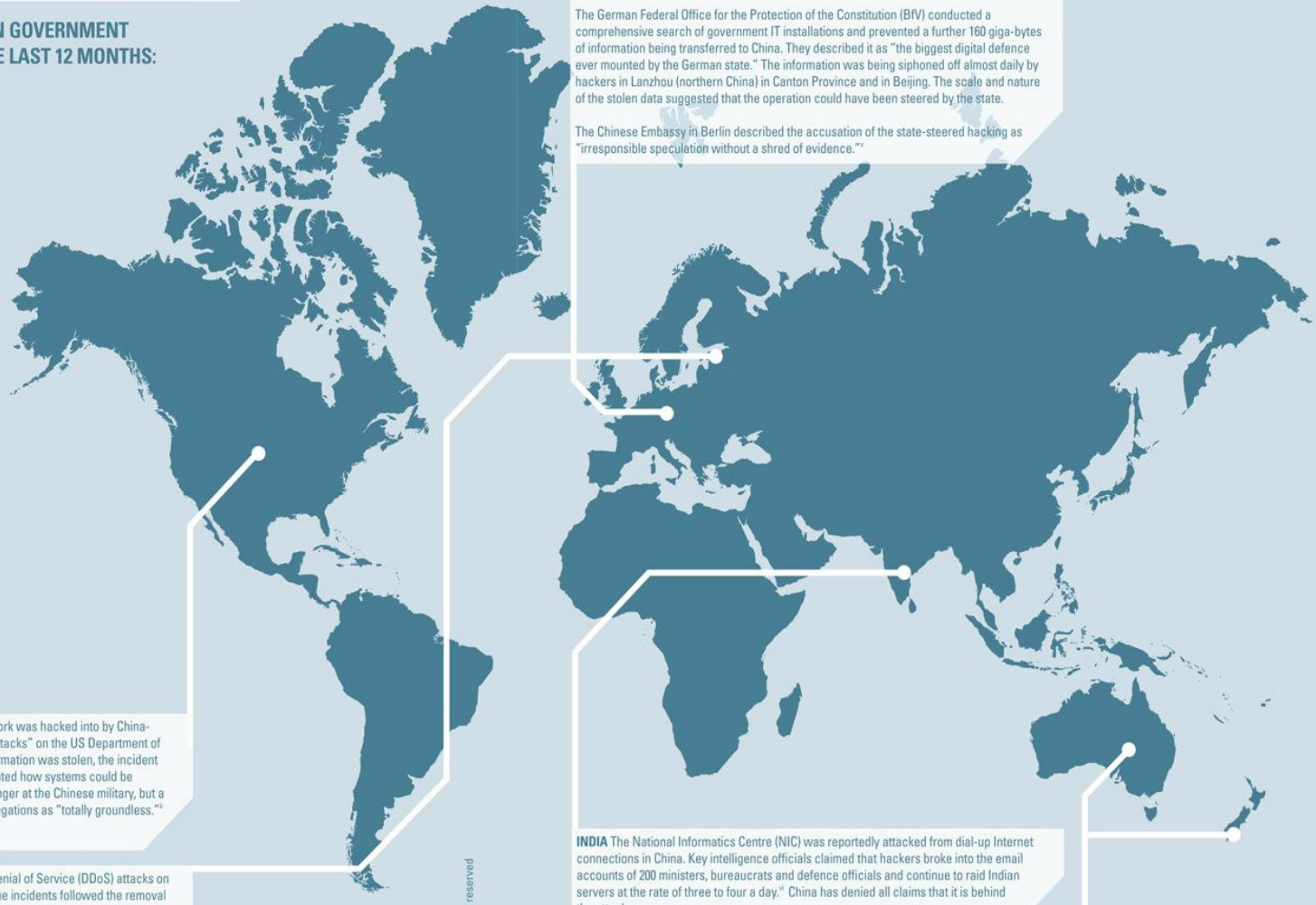
1. Password stealing sites
   - 1400% increase according to APACs, not just banks though!
2. Spam Increase
   - Images move from 1% to 40% in a year
3. Video sharing increase (along with Web2)
   - Myspace, Utube, etc.
4. Mobile device attacks
   - SMS'ing, cross platform (PC, to device)
5. Adware continues to go mainstream (commercially)
6. Identity Theft (data loss)
7. BOTs continue as favourite automatic tool
8. Parasitic malware on the comeback
   - 10% today, 80% packaged encrypted already
9. Rootkits (32-bit) growth
   - 700% growth in 2006
10. Vulnerabilities continue, fuelled by underground markets

VCR 2007 report

CHAPTER ONE: THE INCREASING CYBERTHREAT TO NATIONAL SECURITY

How the Internet has become a weapon for political, military and economic espionage

THE FOLLOWING CYBERATTACKS ON GOVERNMENT TARGETS HAVE TAKEN PLACE IN THE LAST 12 MONTHS:



GERMANY Germany's respected weekly, Der Spiegel, reported that China was thought to have hacked into the computer systems of Germany's Chancellery as well as systems at three ministries, infecting the networks with spy programs. The alleged attacks occurred just before Chancellor Angela Merkel visited Beijing. Computers in the Chancellery and the Foreign, Economics and Research ministries were targeted.

The German Federal Office for the Protection of the Constitution (BfV) conducted a comprehensive search of government IT installations and prevented a further 160 giga-bytes of information being transferred to China. They described it as "the biggest digital defence ever mounted by the German state." The information was being siphoned off almost daily by hackers in Lanzhou (northern China) in Canton Province and in Beijing. The scale and nature of the stolen data suggested that the operation could have been steered by the state.

The Chinese Embassy in Berlin described the accusation of the state-steered hacking as "irresponsible speculation without a shred of evidence."[v]

UNITED STATES In June 2007, a Pentagon computer network was hacked into by China-based perpetrators in "one of the most successful cyberattacks" on the US Department of Defense. While it is questionable how much sensitive information was stolen, the incident succeeded in raising concerns to a new level as it highlighted how systems could be disrupted at critical times. Many were quick to point the finger at the Chinese military, but a Chinese Foreign Ministry spokeswoman dismissed the allegations as "totally groundless."[i]

ESTONIA In April 2007, Estonia experienced Distributed Denial of Service (DDoS) attacks on government, news and bank servers for several weeks. The incidents followed the removal of a Soviet statue from a central Tallinn Square to the outskirts of the city. At the height of these attacks, 20,000 networks of compromised computers were linked, and analysis of the malicious traffic showed that computers from the United States, Canada, Brazil, Vietnam and others were involved. "It was a political campaign induced by the Russians; a political campaign designed to destroy our security and destroy our society. The attacks had hierarchy and co-ordination," said Mikhel Tammet, director of the Estonian communication and information technology department.[iv] It was a probing attack from which attackers and defenders both learned a great deal.

Russian officials deny that claim. Kremlin spokesman Dmitri Peskov called it "out of the question" that the Russian government were involved in the attacks.[iv]

INDIA The National Informatics Centre (NIC) was reportedly attacked from dial-up Internet connections in China. Key intelligence officials claimed that hackers broke into the email accounts of 200 ministers, bureaucrats and defence officials and continue to raid Indian servers at the rate of three to four a day.[vi] China has denied all claims that it is behind the attacks.

NEW ZEALAND & AUSTRALIA Asia Pacific News reported that Chinese hackers had allegedly tried to hack into highly classified government computer networks in Australia and New Zealand as part of a broader international operation to glean military secrets from Western nations. According to news.com.au, Canberra refused to either confirm or deny that its agencies, including the Defence Department, had been subject to cyberattack. New Zealand Prime Minister Helen Clark confirmed that foreign intelligence agencies had tried to hack into government computer networks but had not compromised top-secret data banks. The Chinese Government has denied any involvement.

AVERT 2008 predictions

1. Bull's-eye on Web 2.0
2. Botnets - Follow the Storm
3. IM = Instant Malware
4. Target: Online Gaming
5. Vista joins the party
6. Adware in decline
7. Phishers cast a wider net
8. Parasitic crimeware takes root
9. Virtualization transforms information security
10. VoIP - Prelude to a worm?

The changing target & methods

- No more great train Robberies - Sumitomo bank!
- Target resource attacks
  - 200,000 web pages in 48 hours
- BOT armies grow – focus on attack longevity
  - Time = Money
  - Use the public
- Target the consumer and the SMB
- Commercial Malware tools – Pinch II & MPACK
- Vulnerability black market & online auction
- Code recycling & version control
- Open source model adoption – FURookit, DoomJuice

Storm worm a.k.a Nuwar

W32/Nuwar@MM

Type	Virus
SubType	Email
Discovery Date	11/02/2006
Length	Varies
Minimum DAT	4887 (11/02/2006)
Updated DAT	5149 (10/25/2007)
Minimum Engine	5.1.00
Description Added	11/02/2006
Description Modified	08/27/2007 9:11 PM (PT)

Generations of subject trickery

EXE file	New Years celebrations	(Dec 06)
	War/Missle strike	(Apr 07)
GIF in Zip file	Virus/worm/trojan detected!	(Apr 07)
EXE file link	eCard "You've received a greetind card…"	(June – July 07)
	eCard multiple subject lines	(July – Aug 07)
	Information phishing subject lines	(Aug 07)
	Beta testing/help required subject lines	(Aug 07)
	Cool video subject lines	(Aug 07)
	Labour day greetings subject lines	(Sept 07)
Privacy tool link (exe)	Privacy invasion warnings subject lines	(Sept 07)
Web site, links to Trojan	NFL (new season starts) subject lines	(Sept 07)
Web site, links to Trojan & JS vulns to execute	Gaming	(Sept 07)
Web site, fake shockwave to (exe)	Psycho Cat	(Oct 07)
Web site, scripts (expoits & infection) or click download File names & packer changed	Krackin p2p sharing tool	(Oct 07)
	Merry Christmas	(Dec 07)
	New Year greeting ecard	(Dec 07)
	With Love (Valentines)	(Jan 08)

Storm worm, what does it do?

- SMTP threat replication
- P2P communication using eDonkey/Overnet protocol
  - Second stage infection URLS
  - Command & control
  - Updates URLs
- DDoS functionality
  - SYN flood
  - ICMP pings
- Obviscation
  - Uses Packers (may be double packed)
  - Kernel Rookit (into services.exe)
  - Bypasses Windows firewall (allowed process)
  - Moving backend servers (DNS, FFlux, multiple servers, etc).
  - Pesudo-polymorphic script on websites

- Terminates apps, inc text
  - mcafee
  - hijack
  - lockdown
  - firewall
  - avg
  - zonea
  - nod32
  - rav
  - avp
  - viru
  - Registry Editor
  - taskmgr
  - f-pro
  - msconfig
  - blackice
  - vsmon
  - spybot
  - reged
  - nav
  - troja
  - anti
- SMTP spam tool
- Backdoor trojan
- Used for punp'n'dump stock spam scams

McAfee

Protect what you value.

Thank You

01010100011010000011000010110111001101011001000000111100101101111011101010000110100001010

Greg_Day@McAfee.com

01000111011100100110010101100111010111110100010001100100101111001010000000100110101100011010000001011001100110010100101011100110001101101111011011011