SECURITY 2012

20. ročník konference o bezpečnosti v ICT

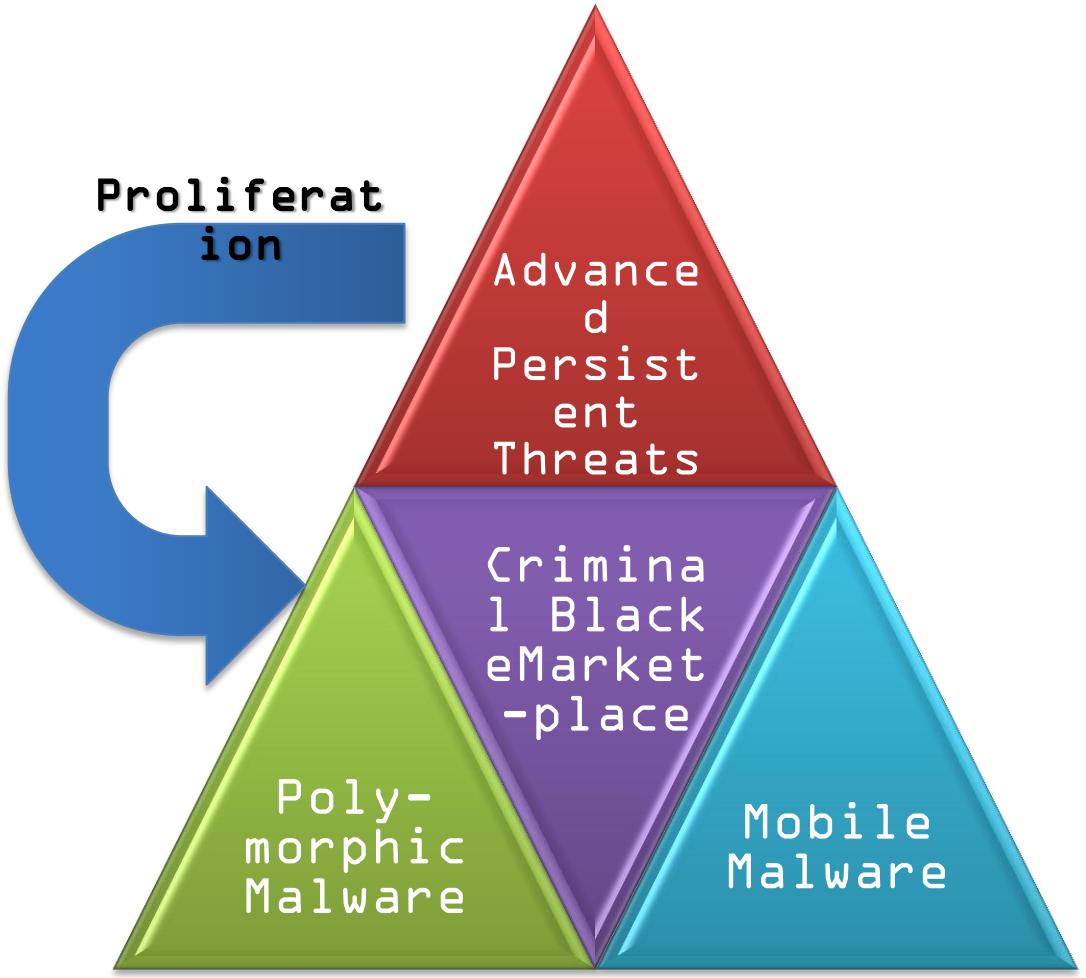
COSE
COGNITIVESECURITY

Modern Malware: Trends, Threats, Opportunities

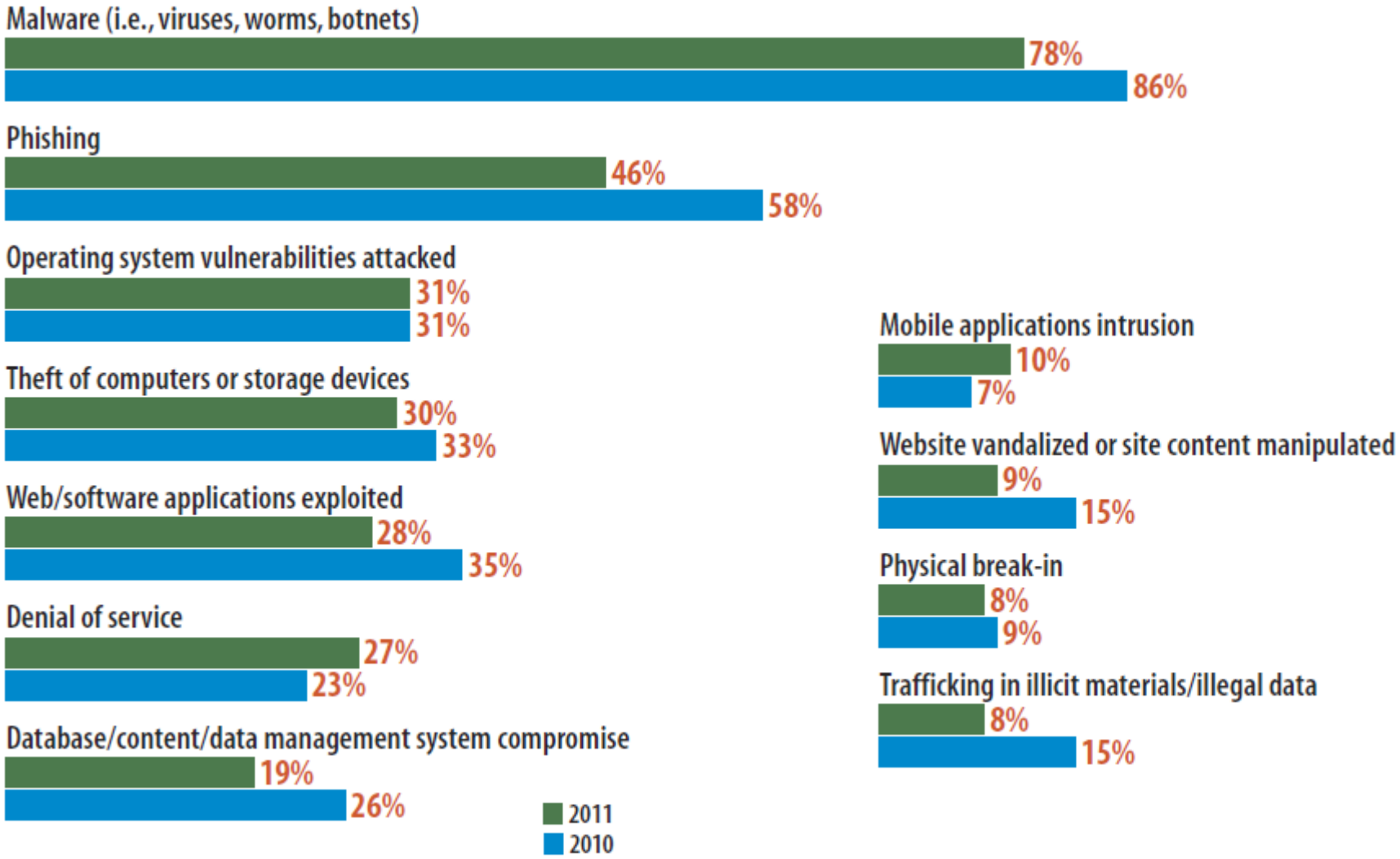
Martin Rehak, CEO
www.cognitive-security.com

Top current trends in malware

1. Advanced Persistent Threats
2. Proliferation of advanced attacks
3. Professional black markets for higher malware efficiency
4. Polymorphic malware
5. Mobile malware

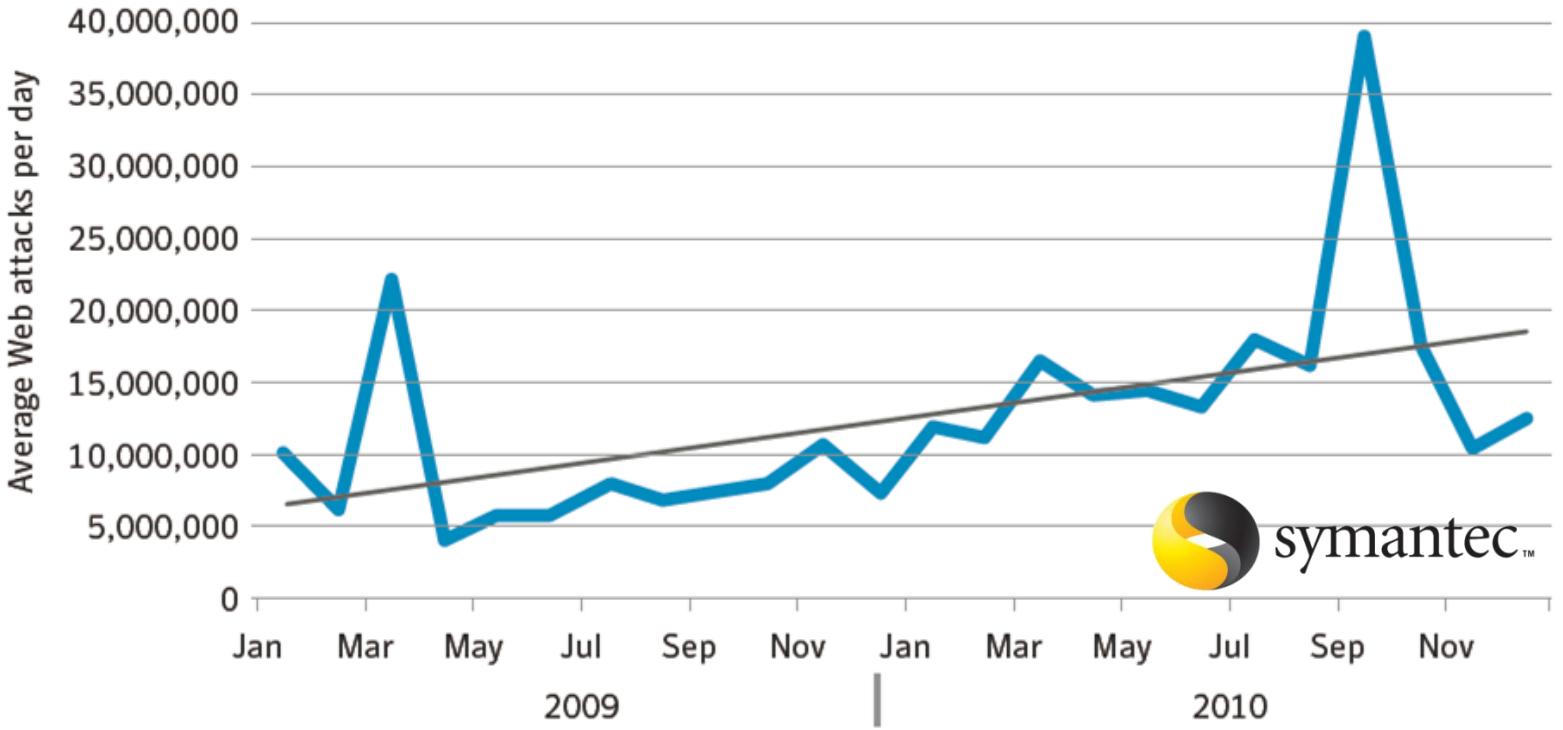


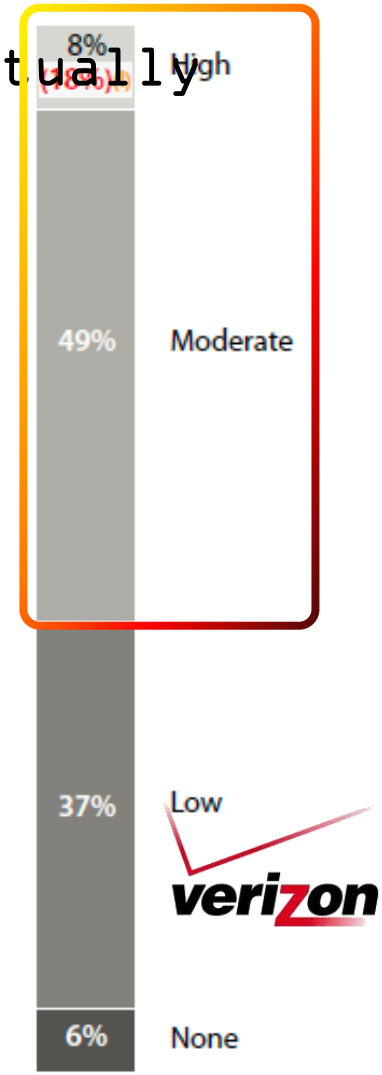
Top Security Breaches



Compromised Data Types & Difficulty

- "Given enough time… …criminals can breach virtually any single organization" - Verizon





Symantec - Internet Security Threat Report '11.Apr
*Verizon - '11 Data Breach Investigations

Advanced persistent threats

"In looking at computer systems of consequence – in government, Congress, at the Department of Defense, aerospace, companies with valuable trade secrets – we've not examined one yet that has not been infected by an advanced persistent threat."

Mike McConnell, (NY Times, Feb 11, 2012)

Target: Advanced Persistent Threats

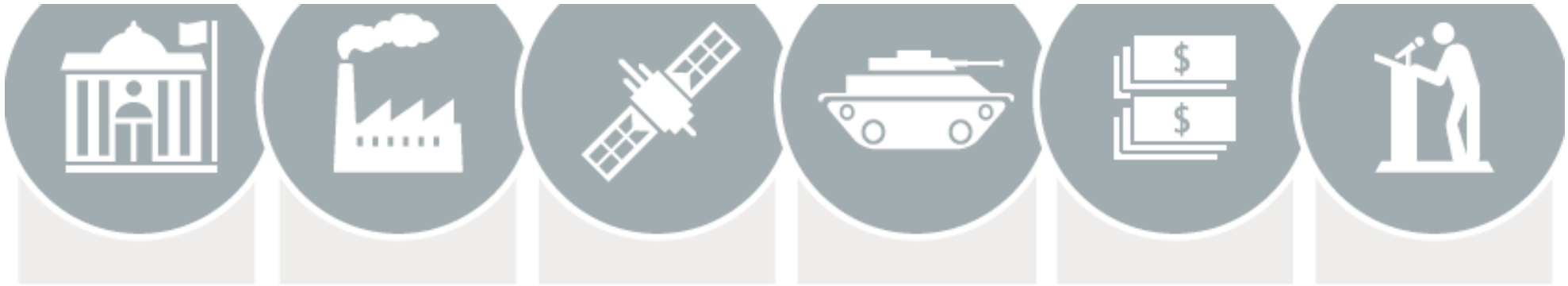
"The key to these intrusions is that the adversary is motivated by a massive hunger for secrets and intellectual property"

McAfee

"[If] you're not seeing APT attacks in your organization, it is probably not that they are not occurring or that you're safe. It's more likely that you may need to rethink your detection capabilities."

cisco

All Industry Sectors at Risk



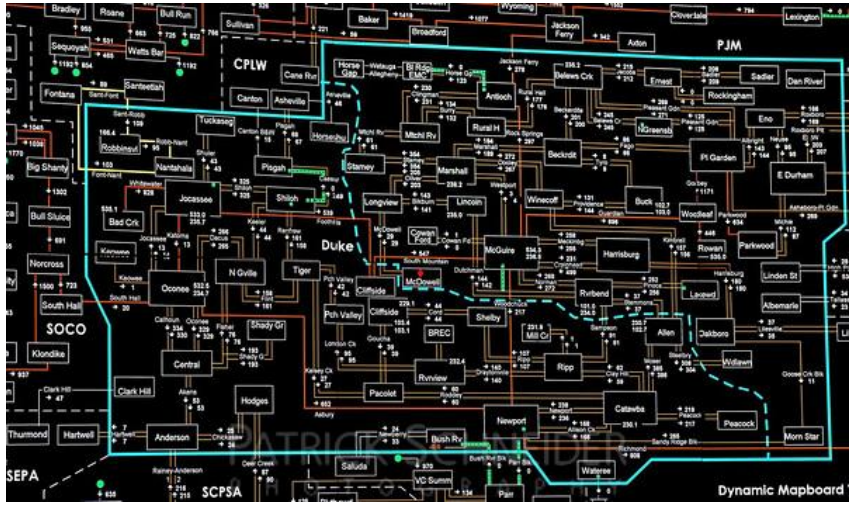
U.S. Federal Government	6	Construction/ Heavy Industry	3	Electronics Industry	3	Defense Contractor	13	Real Estate	2	International Sports	5
U.S. State Government	5	Steel Industry	1	Computer Security	2			Accounting Industry	2	Economics/ Trade	2
U.S. County Government	3	Energy	1	Information Technology	2			Agriculture	1	Think Tanks	2
Canadian Government	2	Solar Power	1	Satellite Communica-tions	1			Insurance	1	International Government/ Economics/ Trade	1
South Korean Government	1	U.S. Government Contractor	1	News Media	1					Political Non-profit	1
Vietnam Government	1	United Nations	1	Information Services	1					U.S. National Security Non-profit	1
Taiwan Government	1	Indian Government	1	Communica-tions	1						

"…every company in every conceivable industry with significant size & valuable intellectual property & trade secrets has been compromised (or will be shortly)…" – McAfee

Advanced Persistent Threats

Strategically motivated

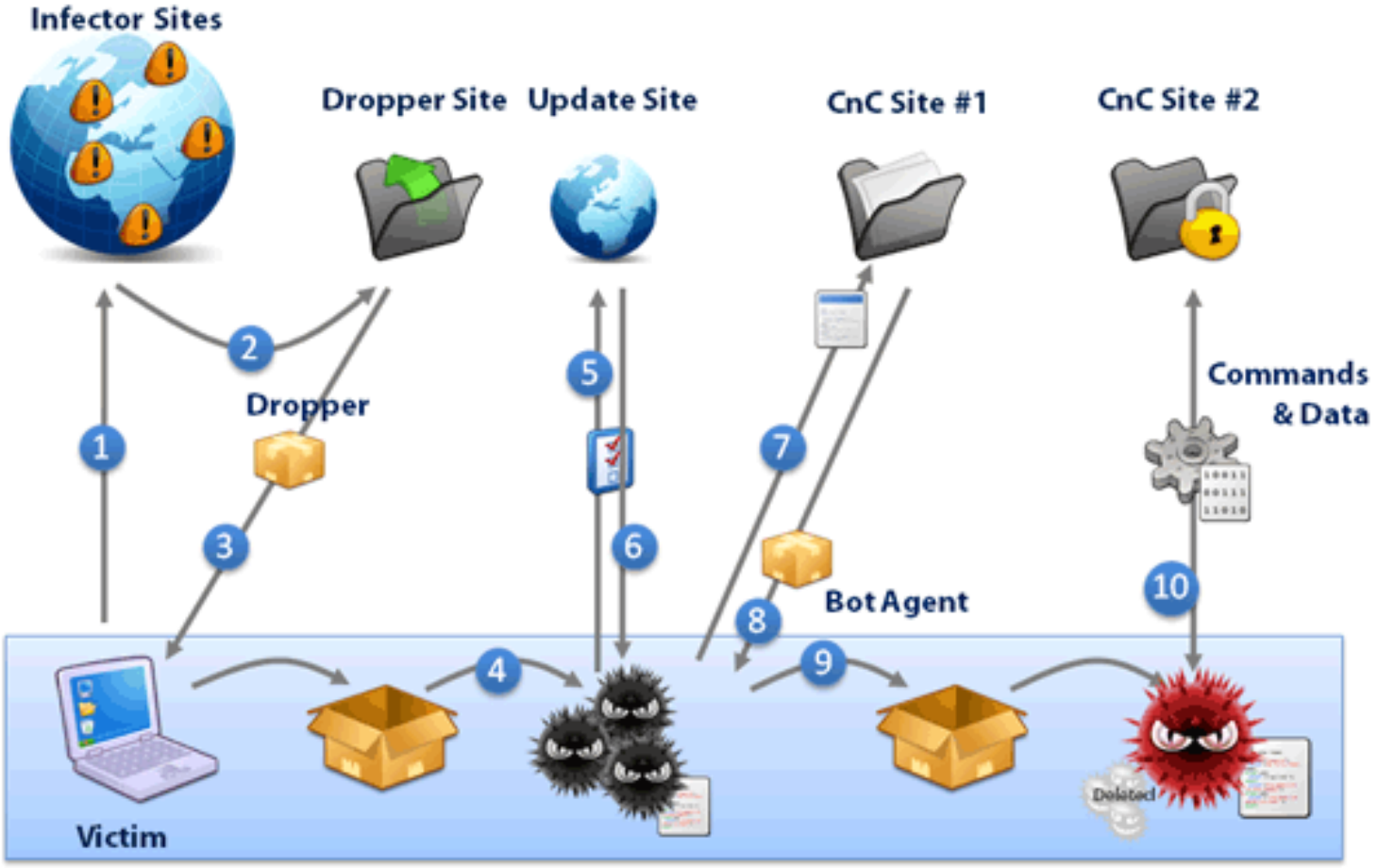
- Compromise of specific info & processes
- Confidentiality - Intellectual Property (IPR) compromise
- Integrity
  - Industry processes
  - Trading systems



Targeted

- Single/few targets
- Original malware/exploit/attack techniques
- Unique proxy/com. channels
- Professional infiltration (social engineering, web, email, business partners)
- Defined information scope

Modern malware operation



Source: Damballa

APT Impact: JSF

"…Before the intrusions were discovered nearly three years ago, Chinese hackers actually sat in on what were supposed to have been secure, online program-progress conferences, the officials say…"

"Defense analysts note that the JSF's information system was not designed with cyberespionage, now called advanced persistent threat, in mind. Lockheed Martin officials now admit that subcontractors (6-8 in 2009 alone, according to company officials) were hacked and "totally compromised." In fact, the stealth fighter program probably has the biggest "attack surface" or points that can be attacked owing to the vast number of international subcontractors."

Aviation Week, via. Defense.org

Getting there: RSA Case Study

March '11: RSA Compromise

- *"Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products…", "…this information could potentially be **used to reduce the effectiveness** of a current two-factor authentication implementation as part of a broader attack."* RSA/EMC SEC filing

April: L3 compromise discovered:

- *"L-3 Communications has been actively targeted with*

Lockheed Martin:

- *"Unknown hackers have broken into the security networks of Lockheed Martin Corp & several other U.S. military contractors"*
- *"They breached security systems designed to keep out intruders by creating duplicates to "SecurID" electronic keys from EMC Corp's (EMC.N)* (Reuters, May 27)

Raytheon/Boeing:

- *…immediate companywide actions in March … "As a result of these actions, we prevented a widespread disruption of our network," he said.*
- *Boeing […] had a "wide range" of systems in place*

RSA: Conclusion

Together, the attacks suggest the RSA intruders obtained crucial information — possibly the encryption seeds for SecurID tokens — that they're using in targeted intelligence-gathering missions against sensitive U.S. targets.

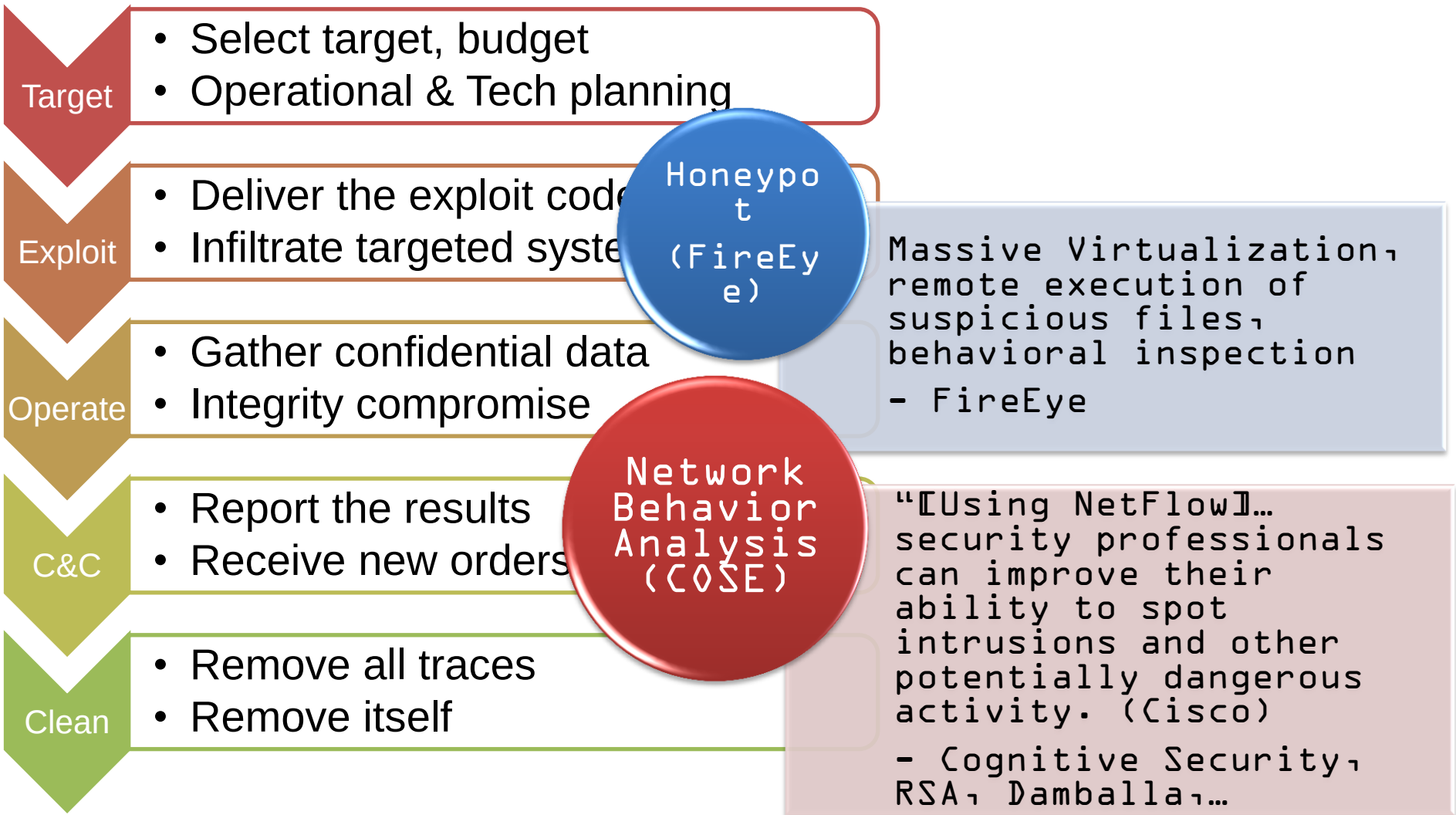
Wired, May 2011

US Chamber of Commerce

"…But the scope of the problem is illustrated by an incident at the United States Chamber of Commerce in 2010.

*The chamber did not learn that it — and its member organizations — were the victims of a cybertheft that had lasted for months until the Federal Bureau of Investigation told the group that servers in China were stealing information from four of its Asia policy experts, who frequent China. By the time the chamber secured its network, hackers had pilfered at least **six weeks worth of e-mails** with its member organizations, which include most of the nation's largest corporations. Later still, the chamber discovered that its **office printer** and even a **thermostat** in one of its corporate apartments were still communicating with an Internet address in*

APT Detection and Containment



APT Prevention: Historical Perspective

Line X

- Line X - targeted technology "transfer" program managed by KGB to steal western technology
- Closing approx. 10 years gap in application of research results
- Analogous to current Asian-country originated threats

Farwell program

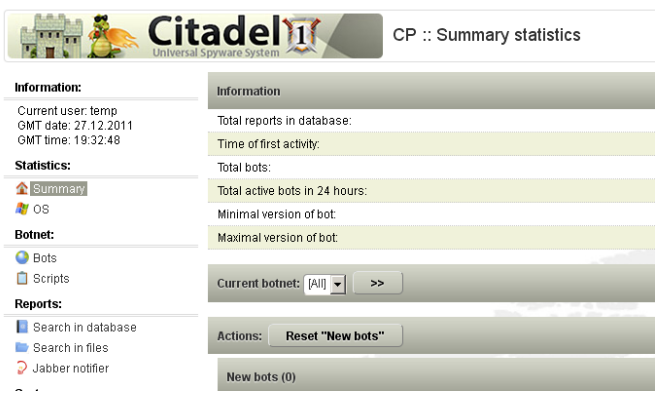
- CIA/NATO activity countering 1980's APT
- Targeted disinformation and deception
- Biggest-ever non-nuclear explosion credited to program

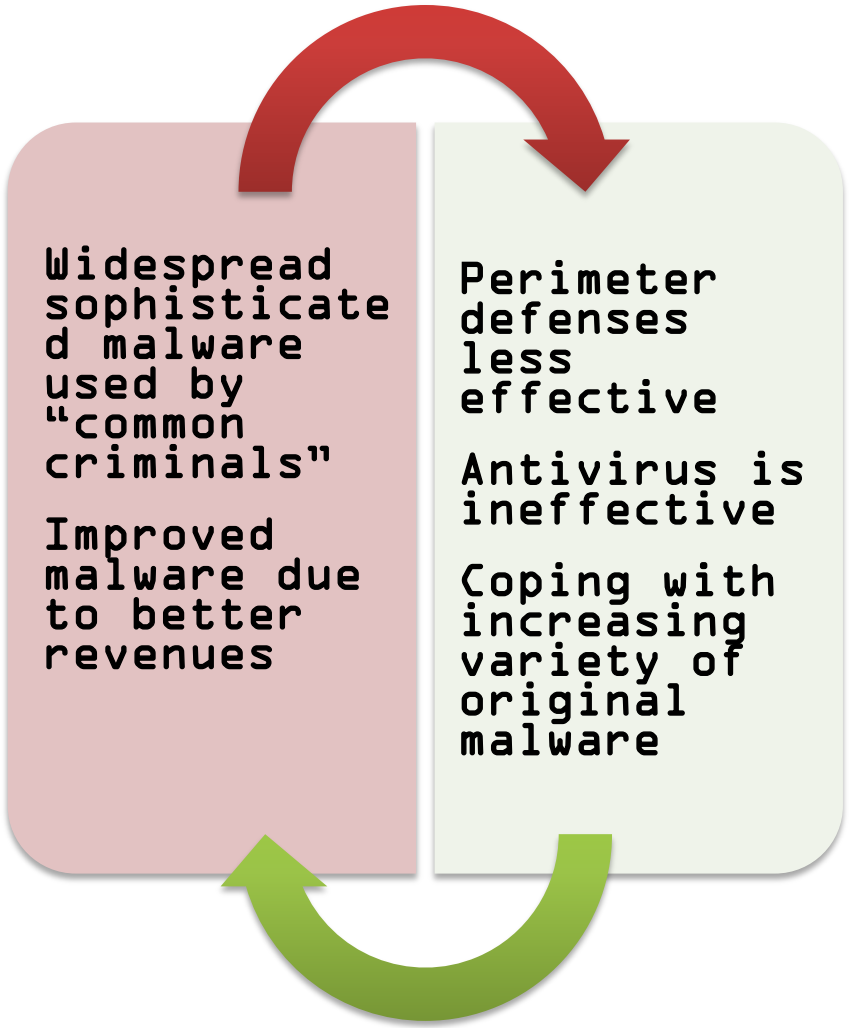
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm

Proliferation of APT-Grade technology

Trend:

- Increasing size of network warfare units in non-NATO militaries
- Results in mass of trained professionals on

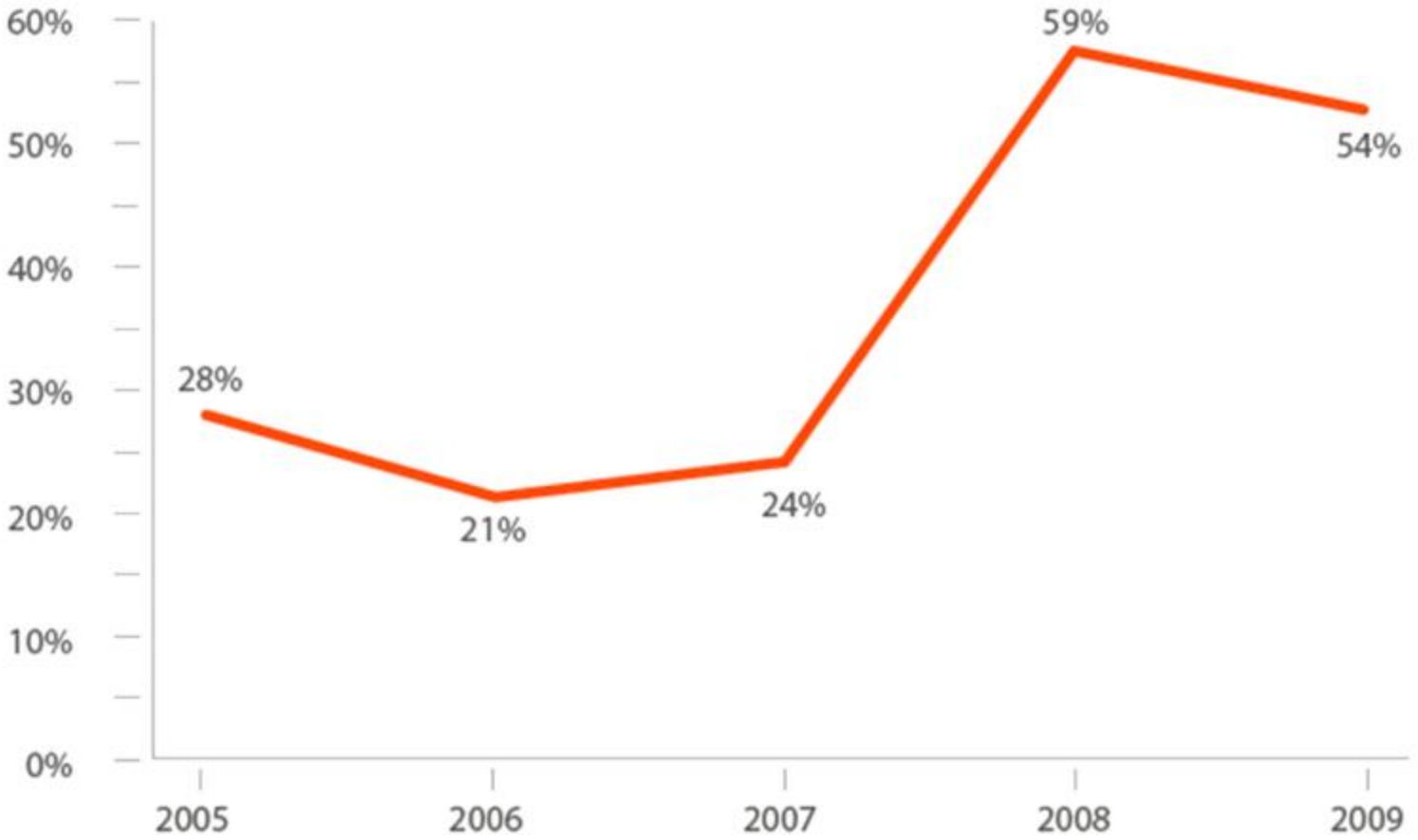




Malware frameworks:

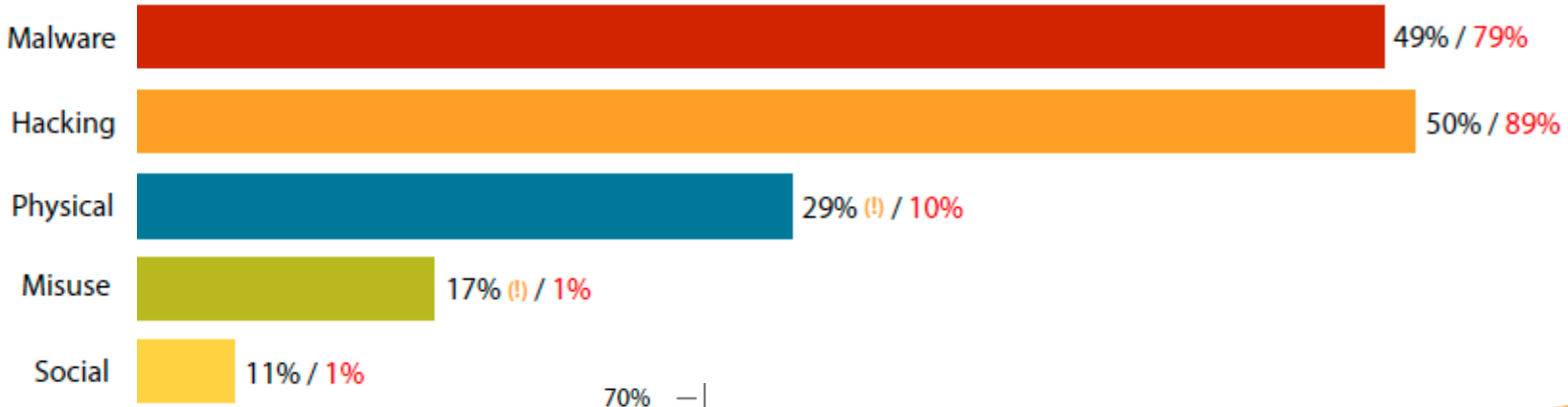
- From code libraries to malware-as-a-service model
- Support, ticketing, charge-back, …

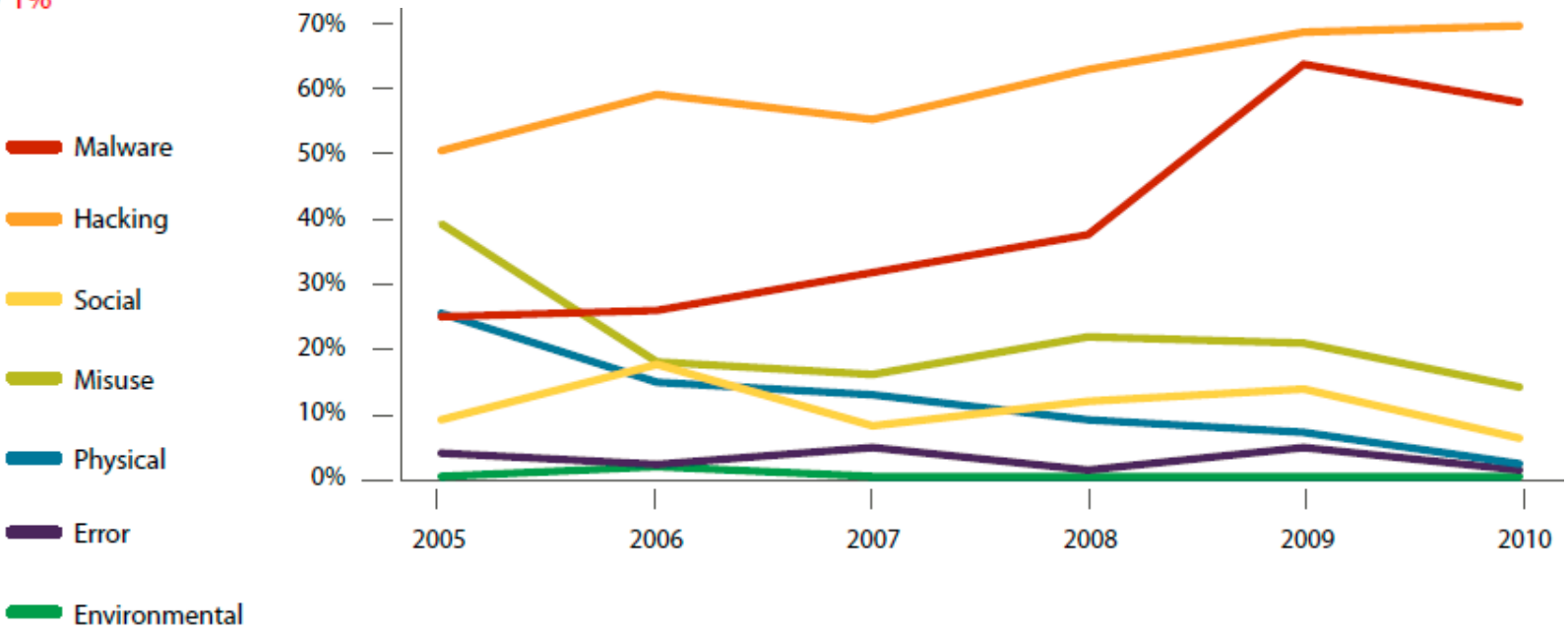
Malware Customization Over Time



*Verizon - '10 Data Breach Investigations Report

Top Attacks





% breaches / % records
*Verizon - '11 Data Breach Investigations Report

Efficient Black Markets

Global technology base

- Exploits, malware, software frameworks and resources are developed and shared globally
- High technical quality, functional specialization, global competition

Local targeting & exploitation

- Botnet operation, information harvesting from exploited PC's, information dissemination is performed locally

Monetization through hands-off markets

- Risk minimization for key

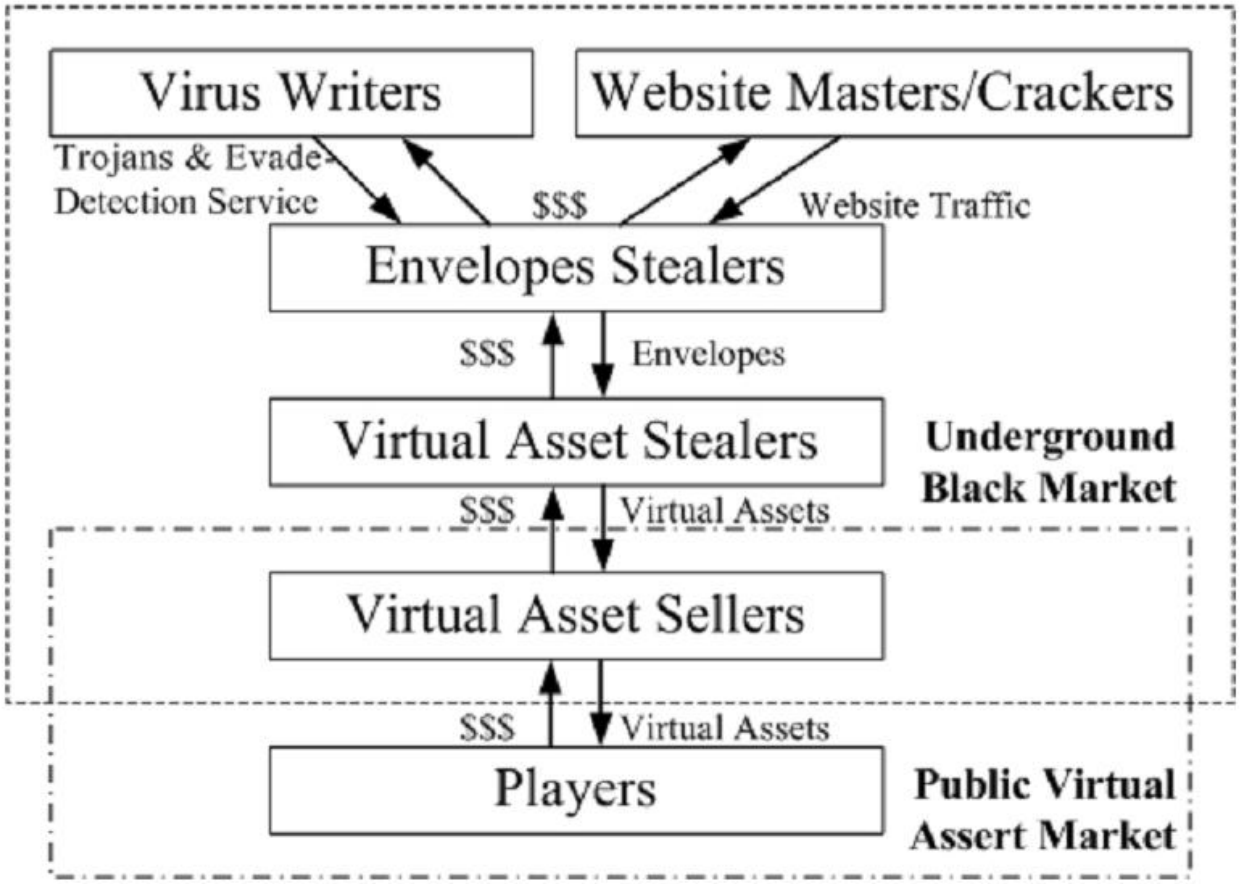
Impact

1. Increasing technology level defined by global competition

2. Specialized, local command & control structures for specific exploits

3. Increasing competition between the attackers: botnets attacking each other, lawsuits…,

Black market example



Polymorphic malware

Polymorphism: self-modification of malware during lifetime

Syntactic polymorphism

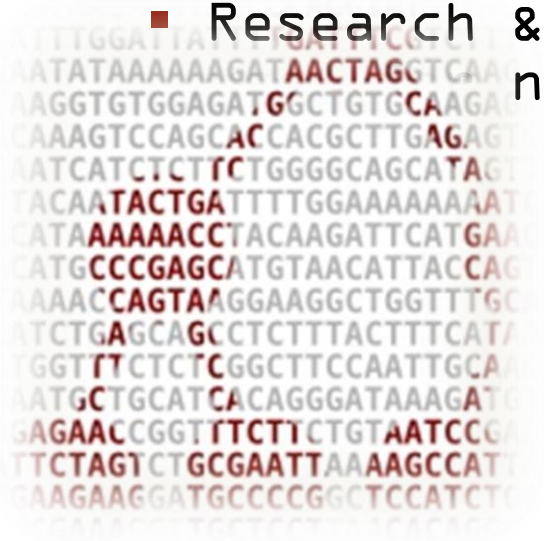
- Packers, obfuscation: hiding from detection by IDS/IPS and AV

Semantic

- Modification of the malware behavior at runtime
- Managed by C2, upgrades
- Result of environmental conditions and local decision
  - Stuxnet

Use of genetic programming/algorithms to:

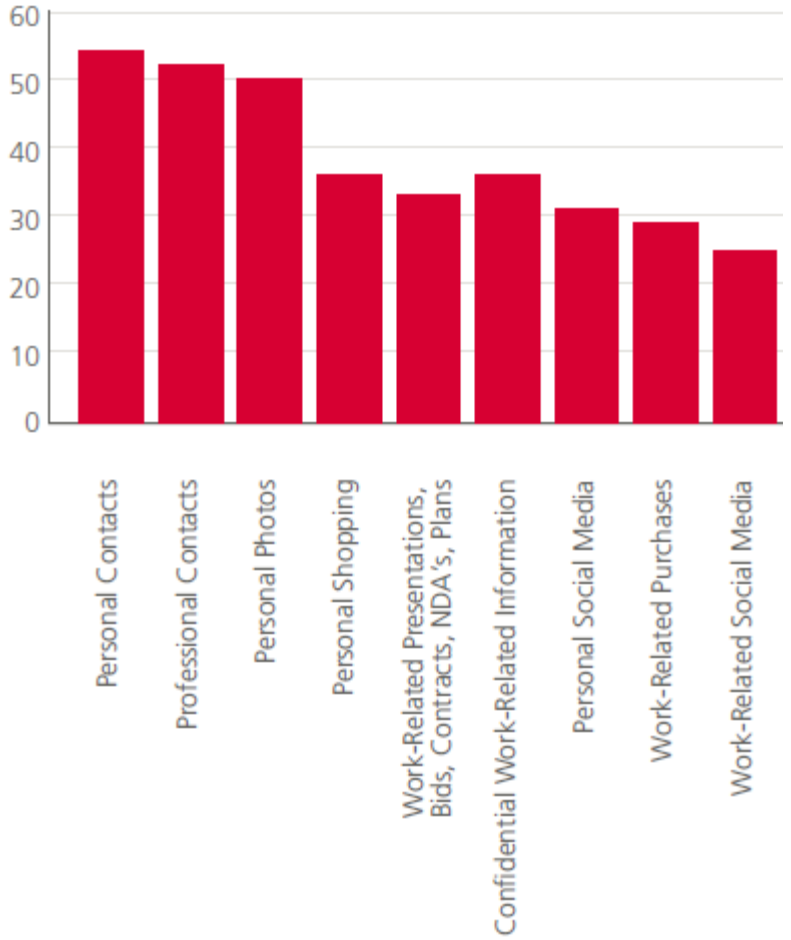
- Learn the evasion techniques from individual IDS instances
- Identify novel exploits by fuzzy testing-like approaches
- Research & government now



Mobile Security - Current & Future Threats

Mobile devices hold a rich set of personal information:

- Location details
- browsing & call history
- contact lists & phone numbers
- SMS, email & Facebook
- Calendar details
- Stored Passwords in clear text
- Premium-rate calling



Internet Access remains a large vulnerability hole

Up-In-Coming Threats

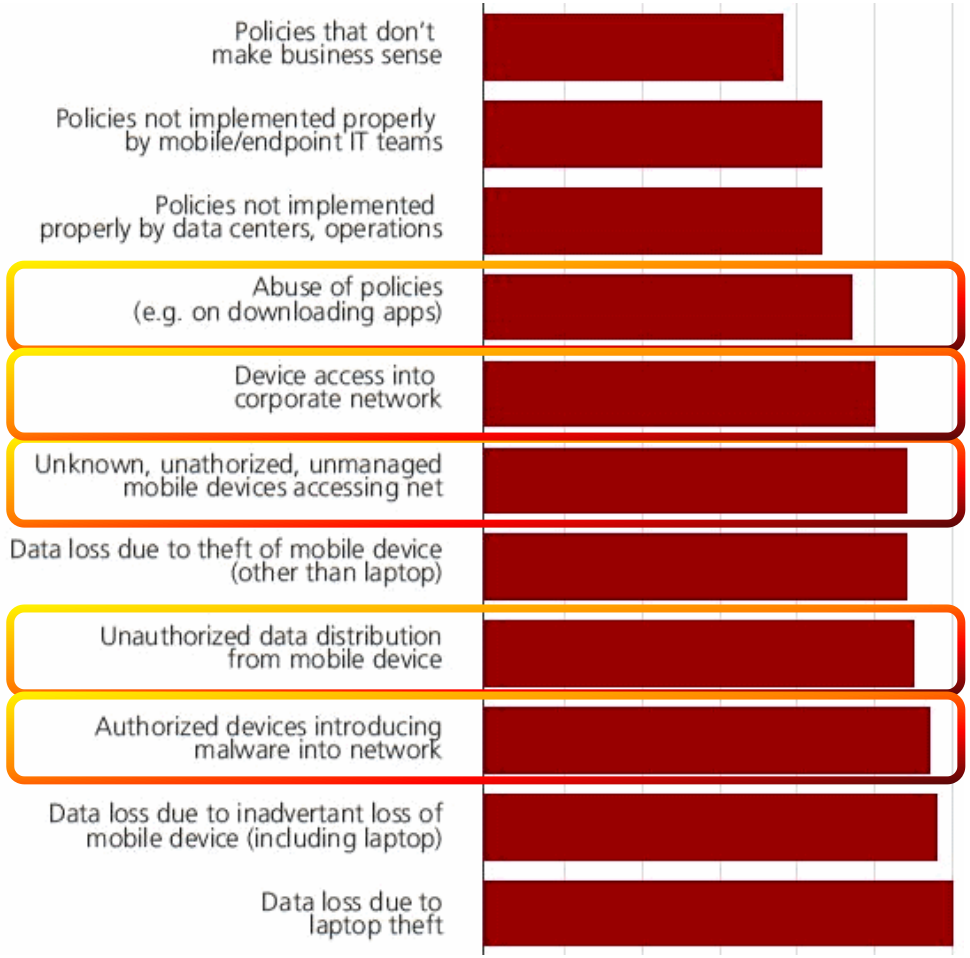
- Micro-payment vulnerabilities

McAfee - Mobility and Security Dazzling Opportunities, Profound Challenges (11.May)
LookOut - Mobile Threat Report (11.Aug)

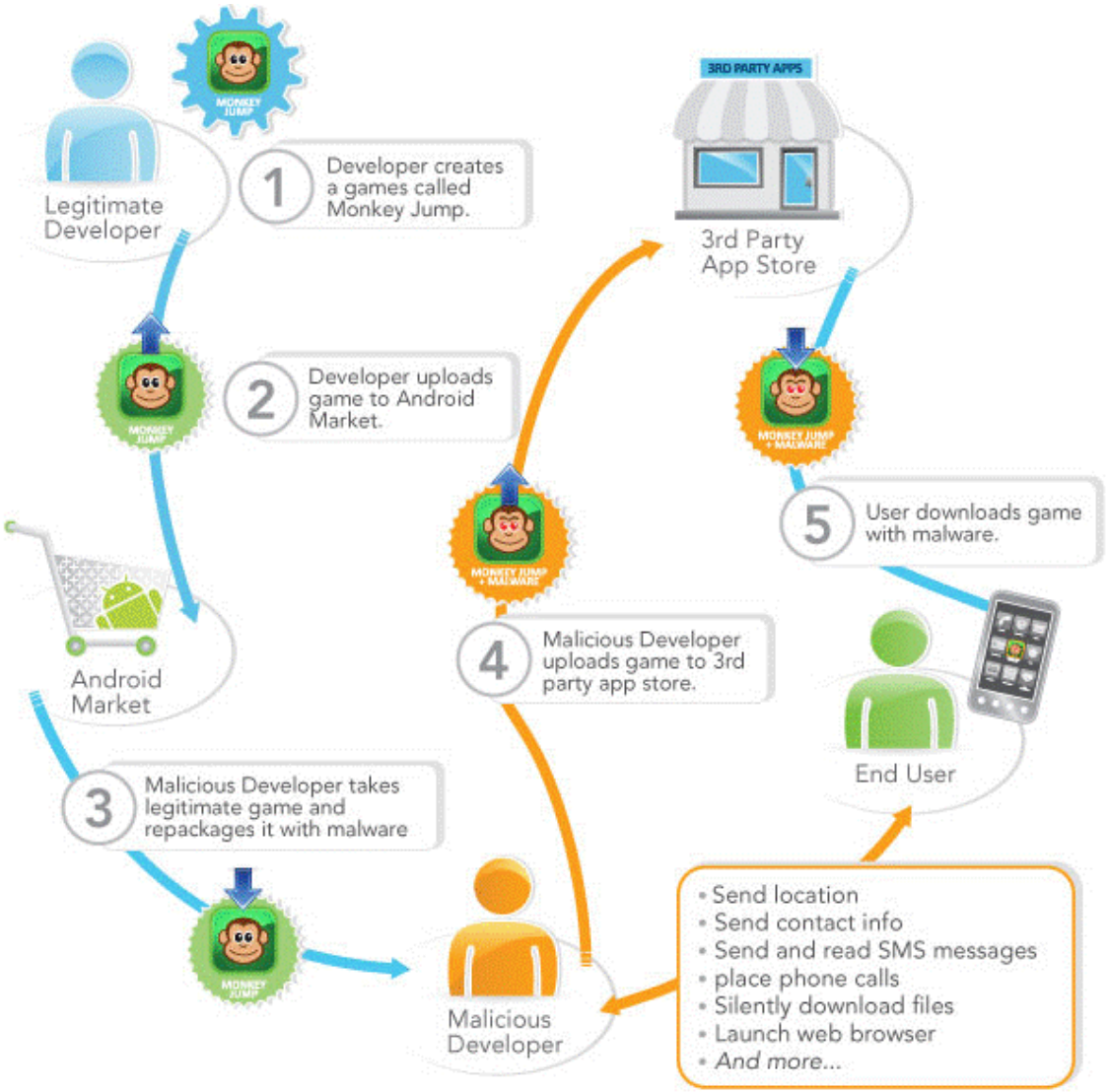
Mobile Security - Market Challenges

Recent Issues…

- iPhone "Root-kitting"
  - Bypassing device security
- Theft of smartphones, & tablets
  - sensitive records compromised
- Spoofed ActiveSync policy apps
  - Reporting higher security than what is actually available
- "Co-mingling"
  - Mixing private & corporate data
- Malware
  - Stealing data & bandwidth
  - Uncertified apps with malware
  - Capturing info & forwarding



Malware Threat Example - Repackaging



APT and Mobile Security

"If a company has significant intellectual property that the Chinese and Russians are interested in, and you go over there with mobile devices, your devices will get penetrated," said Joel F. Brenner, formerly the top counterintelligence official in the office of the director of national intelligence.

NY Times, 11.2.2012

Conclusions

Modern threats are immune to reactive defense posture:

- AV, IDS, anti-malware, D

Security teams need to adopt to a more proactive, forward looking approach to cy

Protecting company's business operations instead of the network

Based on initiative and business relevance