A jövő internete, BMEVITMAV74

BME-VIK és DE-IK közös szabadon választható tárgya

Internet biztonság

Buttyán Levente

Budapesti Műszaki és Gazdaságtudományi Egyetem
Hálózati Rendszerek és Szolgáltatások Tanszék
CrySyS Adat- és Rendszerbiztonság Laboratórium

Budapest, 2015. tavasz

Internet (in)security

Levente Buttyán

CrySyS Lab, BME

www.crysys.hu

Contents

- what is security?
- threats
  - cybercrime
  - state sponsored targeted attacks
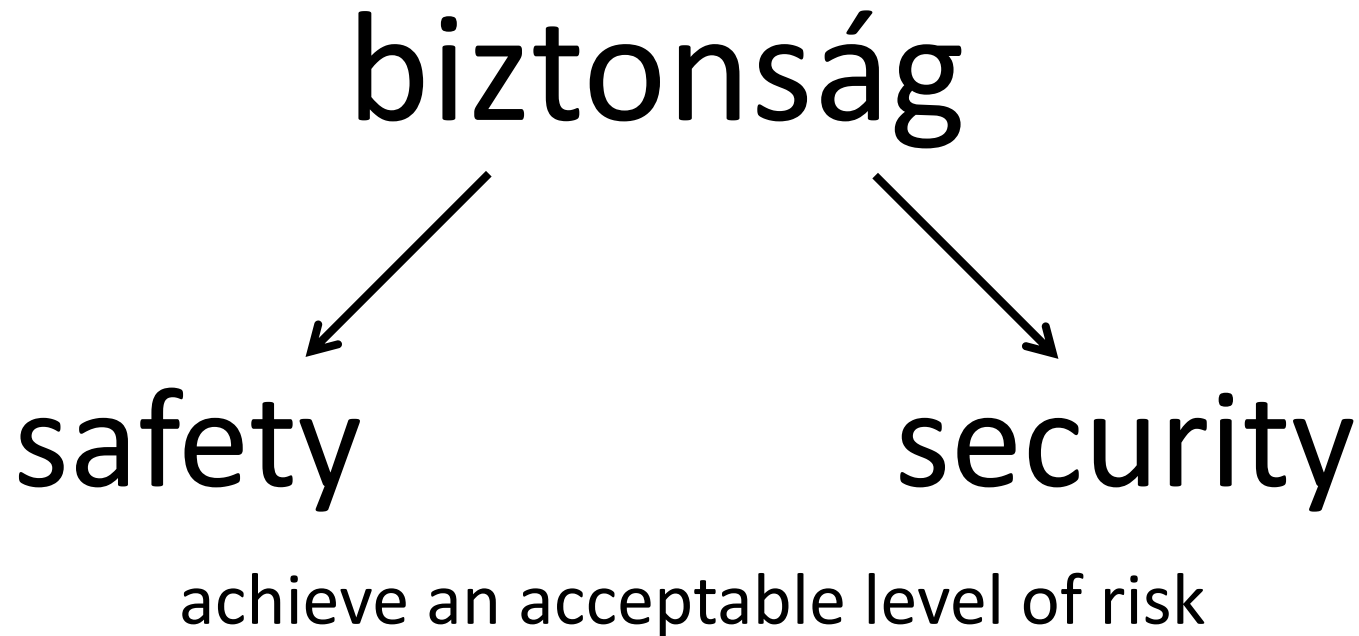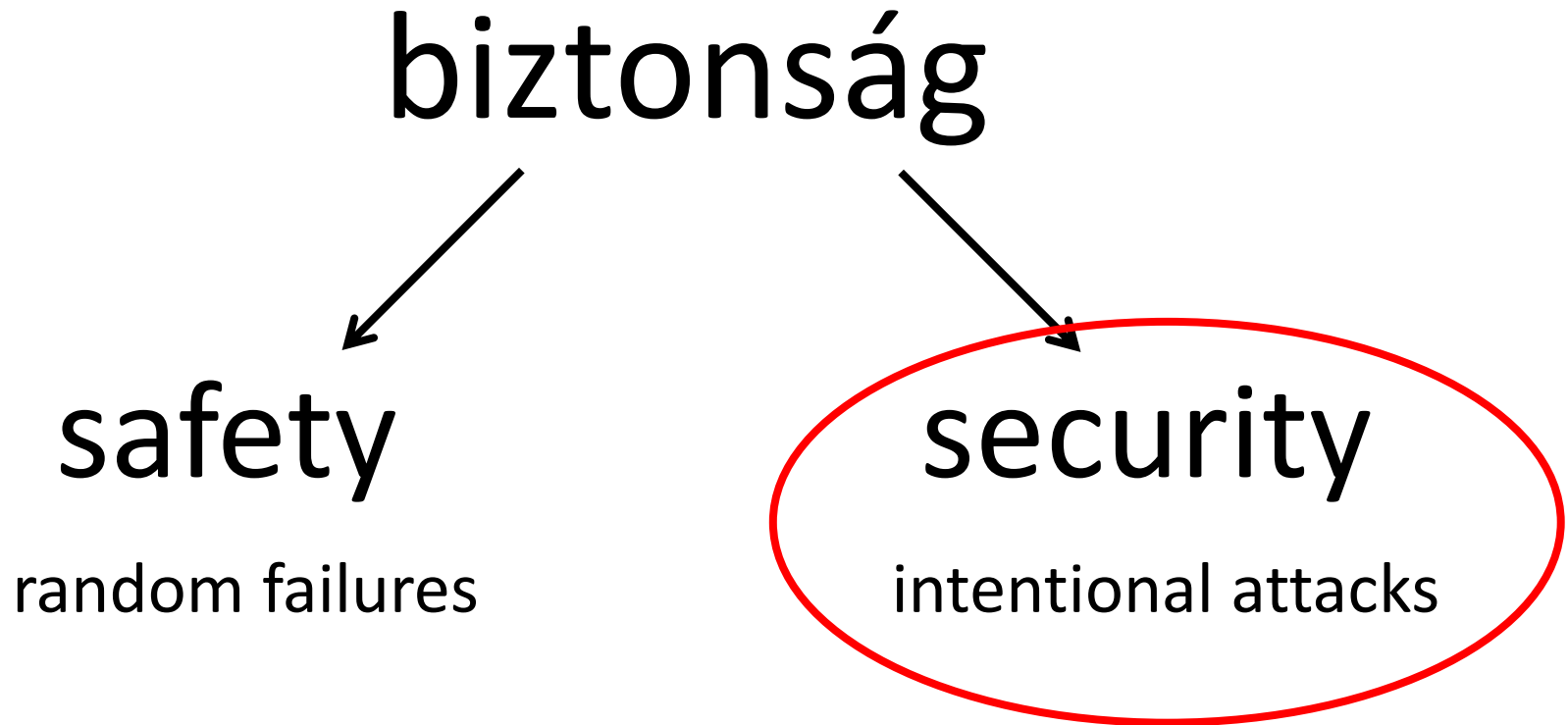- malware
- (in)security of the Internet of Things

WHAT IS SECURITY?

Security

- security = management of risk
- IT security is about the management of risk resulting from
  - the loss of confidentiality, integrity, or availability (CIA) of information that is processed, stored, and transferred by IT systems
  - the unauthorized access, corruption, or denial of services and resources that are provided by IT systems

IMPORTANT

completely preventing such incidents is not possible in general

→ the goal should be to optimize the risk of such incidents

biztonság

safety   security

achieve an acceptable level of risk

biztonság

safety

random failures

security

intentional attacks

Attackers

- attackers differ in their motivation and goals, technical background, information gathering capabilities, and available resources

- attacker (threat) models
  - script kiddy
  - disgruntled employee
  - competitor
  - hacktivist group
  - terrorist organization
  - cybercrime organization
  - state sponsored attacker

- one cannot really counter a threat → one should focus on addressing vulnerabilities

Vulnerabilities

- four different types:
  - **technical:** design flaws and implementation errors in systems, software, and protocols
  - **physical:** weaknesses allowing for physical access (e.g., unlocked door)
  - **operational:** weaknesses in the procedures used to operate the system
  - **personnel:** related to security awareness and trustworthiness of employees and contractors

- reasons for the existence of vulnerabilities
  - systems are designed, implemented, and operated by humans
    - » humans are imperfect and sometimes irrational
  - systems are increasingly complex
    - » easier to overlook flaws and mistakes
    - » harder to test and reason about
  - business constraints
    - » pressure on development time (reduce time-to-market)
    - » limited budget
    - » functionality vs. security trade-offs

Countermeasures

- four different types:
  - **technical:** computer and network security controls
    - » e.g., firewalls, anti-virus software, authentication tokens, security protocols, cryptographic algorithms, ...
  - **physical:** provide physical security
    - » e.g., locks, fences, security guards, tamper resistant hardware, ...
  - **operational:** policies and procedures related to the operation of the system and management of the personnel
    - » e.g., password changing policies, key management procedures, regular security testing, ...
    - » e.g., hiring and firing procedures, promotion procedures, vacation policies...
  - **personnel:** increase security awareness and trustworthiness of people
    - » e.g., security education, increasing employee satisfaction

FreakingNews.com

CYBERCRIME

The surface …

Breaches With More Than 10 Million
Identities Exposed

8

2013

**Total Identities
Exposed**

552 Million

2013

+493%

93 Million

2012

Top-Ten Types of Information Breached

01	**Real Names**
02	**Birth Dates**
03	**Government ID Numbers (Social Security)**
04	**Home Address**
05	**Medical Records**
06	**Phone Numbers**
07	**Financial Information**
08	**Email Addresses**
09	**User Names & Passwords**
10	**Insurance**

Estimated Global Email Spam Volume / Day

2013 — **29** Billion

2012 — -3%

Number of Bots

2013 — **2.3** Million

2012 — **3.4** Million — **-33%**

The surface …

Email Virus Rate Smaller Number = Greater Risk

2013 **1** IN **196**

2012 1 IN 291

Email Phishing Rat

2013 **1** IN **392**

2012 1

New Unique Malicious Web Domains

2013 **56,158**

-24%

Websites Found With Malware

1 IN **532**
2012

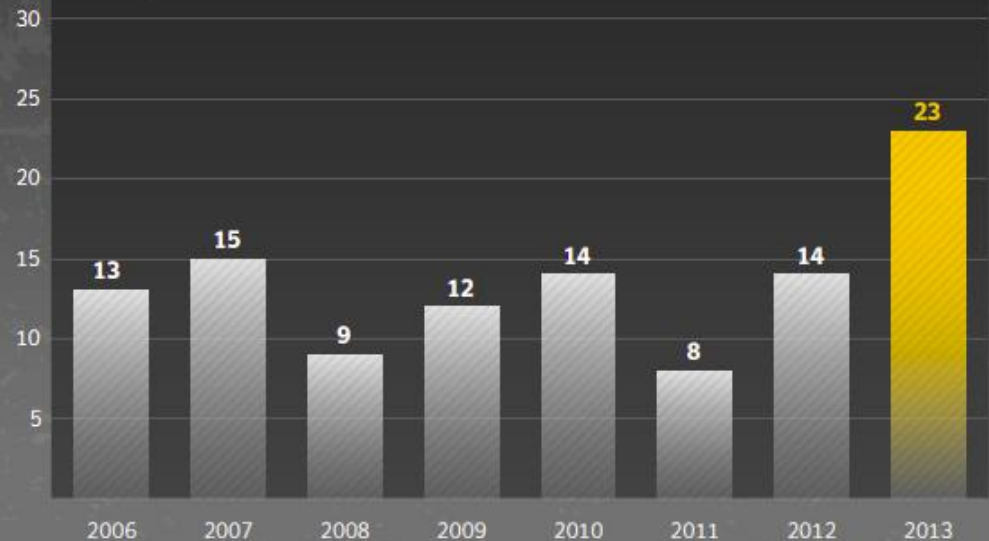**1** IN **566**
2013

New Vulnerabilities

2013 — 6,787 +28%

2012 — 5,

Zero-day Vulnerabilities, Annual Total, 2006 – 2013
Source: Symantec

DAY 0

2006: 13
2007: 15
2008: 9
2009: 12
2010: 14
2011: 8
2012: 14
2013: 23

Ransomware Over Time, 2013
Source: Symantec

Total Android Mobile Malware Variants

2013 — 3,262
2012 — 3,783
-14%

J	F	M	A	M	J	J	A	S	O	N	D
112	107	138	141	178	189	286	421	625	419	861	660

TREND
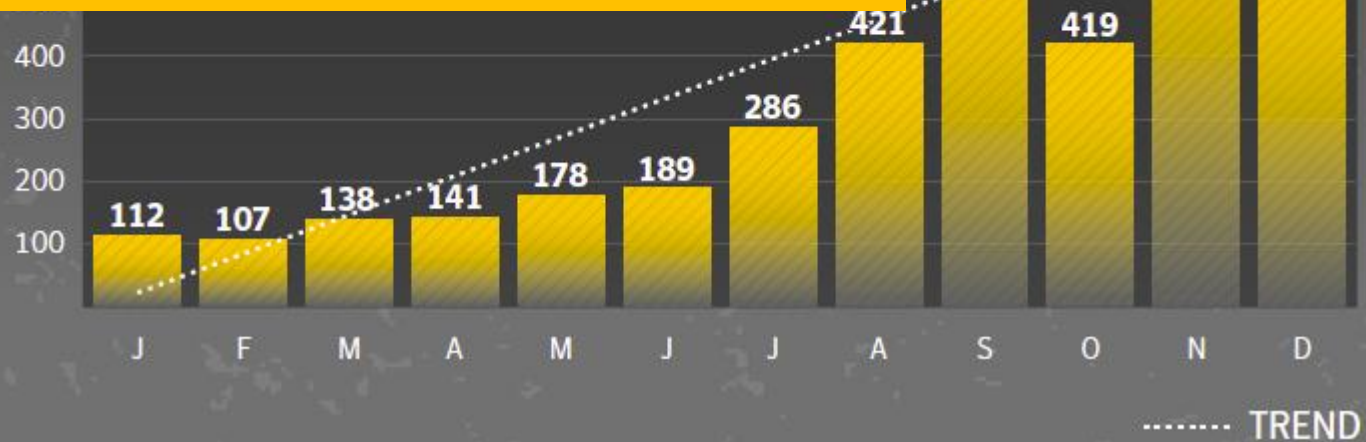
… and the back stage

- cybercrime has evolved into a complex, highly organized ecosystem involving leaders, engineers, infantry, and hired money mules

- products and services are sold and bought on underground markets

  – products

    » Trojans, exploits and exploit bundles, rootkits, crypters, traffic, fake documents, stolen credit card information and other credentials

  – services

    » dedicated server hosting, proxy servers, VPN services, pay-per-install services, DoS attacks, spamming, malware checking against security software, social engineering and account hacking

Underground market prices

Russian Cybercriminal Underground Market Product Offerings			
Product	**2011 Price**	**2012 Price**	**2013 Price**
Credit card credentials (per card): • American • Australian • Canadian • German • British	US$2.50 US$7 US$5 US$9 US$7	US$1 US$5 US$5 US$7 US$6–8	US$1 US$4 US$4 US$6 US$5
Scanned fake document: • European passport • Russian and other CIS passports	US$2.50 US$2–5	US$1 US$1–5	US$1 US$1–2

Trend Micro | Russian Underground Revisited

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Underground market prices

Russian Cybercriminal Underground Market Product Offerings

Product	2011 Price	2012 Price	2013 Price
Trojan:			
• Phoenix	US$500	US$150	US$0–35
• Adrenalin	US$790	No data	No data
• Limbo	US$350	No data	No data
• ZeuS (detected by Trend Micro as "ZBOT")	US$120	US$0	US$0
• SpyEye	US$500	US$0	US$0
Exploit kit:			
• Eleonore Browser Exploit Kit	US$700	No data	No data
• Phoenix Exploit Kit	US$600	US$250	US$0
• eCore Exploit Pack	US$1,000	No data	No data
Crypter:			
• Basic static	US$10–30	US$4–10	No data
• Static with stub and add-ons	US$30–80	US$15–25	US$10–30
• Polymorphic	US$100	US$80	US$65

Trend Micro | Russian Underground Revisited

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Underground market prices

Russian Cybercriminal Underground Service Offerings			
Service	**2011 Price**	**2012 Price**	**2013 Price**
Dedicated-/Bulletproof-server hosting • Low-end • High-end • Virtual private server (VPS)	US$160 US$450 US$70	US$100 US$160 US$40	US$50 US$190 US$12+
Proxy-server hosting (per day): • HTTP/S • SOCKS	US$2 US$2	US$1 US$2	US$1 US$2
Traffic-to-download conversion (PPI per 1,000 installations): • Australia traffic • U.K. traffic • U.S. traffic • Europe traffic • Mixed global traffic • Russia traffic	US$300–500 US$220–300 US$100–150 US$90–250 US$12–15 US$100–500	US$200–500 No data US$100–250 US$75–90 US$10–17 US$100–190	US$120–600 US$150–400 US$120–200 US$50–110 US$10–12 US$140–400

Trend Micro | Russian Underground Revisited
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Underground market prices

Russian Cybercriminal Underground Service Offerings			
Service	2011 Price	2012 Price	2013 Price
DDoS attack: • Lasts 1 hour • Lasts 24 hours	US$4–10 US$30–70	US$2–25 US$15–60	US$2–60 US$13–200
Spamming (per 10,000 messages): • Generic (uses a public database) • External-email-database-based • SMS • ICQ • Skype	US$13 US$17 US$600 US$55 No data	US$8 US$14 US$300 US$15 US$110	US$4–5 US$13 US$100 US4–9 US$86
Flooding: • Email (per 10,000 messages) • Landline phone • SMS (per 1,000 text messages)	US$30 US$32 US$15	US$3 US$23 US$10	US$2 US$25 US$8

Trend Micro | Russian Underground Revisited
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Underground market prices

Russian Cybercriminal Underground Service Offerings			
Service	**2011 Price**	**2012 Price**	**2013 Price**
Malware checking against security software: • Daily checking • Automatic reuploading in case a piece of malware is being detected by known anti-malware solutions • Checking against malicious URL blacklists	US$50 US$50 US$50	US$30 US$30 US$30	US$30 US$30 US$30
Hacking: • Facebook account • VK account • Odnoklassniki account • Twitter account • Gmail account • Mail.ru account • Yandex.ru account • Hotmail account	US$200 US$120–140 US$94 US$167 US$117 US$74 US$74 US$107	US$160 US$100 US$90 US$40 US$120 US$70 US$70 US$100	US$100 US$76 US$94 No data US$100 US$50 US$50 US$100

Trend Micro | Russian Underground Revisited
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Organizational structure

- executives
  - set up business models and infrastructure
  - make decisions and oversee operations
  - not involved with launching attacks directly
- middle managers
  - run affiliate programs (sort of sub-contracting)
  - recruited through "old boy" networks and/or underground forums
  - manage the ground-level forces (the infantry) that actually execute attacks
- infantry
  - the bottom of the chain of command
  - ground-level forces that actually carry out the attacks
  - recruited by recruiters from different communities (public or closed)

Organizational structure

■ recruiters

   – larger organizations use special recruiter services to recruit and manage the infantry

   – example recruitment ad:
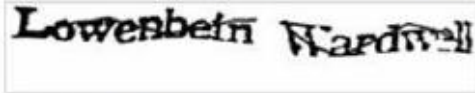
Organizational structure

- **R&D**
  - R&D organizations create custom-ordered attack tools
    - » private botnets, fake antivirus software, ransomware, exploit code

- **hosting providers**
  - offer locations on which to store the attack content
    - » exploit code, malware, and stolen data
  - may be official hosting providers or services posing as hosting providers
    - » the latter actually offer compromised systems for storage
  - typically offshore
    - » often found in safe havens (for attackers) such as Russia and China
    - » don't really care what people use their services for

- **money mules**
  - people who are knowingly or unknowingly used to launder money
    - » anonymously move money from one country or bank account to another
  - several mules, anonymous services and various bank accounts are used in order to make it harder for authorities to trace funds and to place legal responsibility on the mules themselves

Click Trajectories: End-to-End Analysis of the Spam Value Chain

Kirill Levchenko[*]   Andreas Pitsillidis[*]   Neha Chachra[*]   Brandon Enright[*]   Márk Félegyházi[‡]   Chris Grier[†]

Tristan Halvorson[*]   Chris Kanich[*]   Christian Kreibich[†◊]   He Liu[*]   Damon McCoy[*]

Nicholas Weaver[†◊]   Vern Paxson[†◊]   Geoffrey M. Voelker[*]   Stefan Savage[*]

[*]Department of Computer Science and Engineering
University of California, San Diego

[†]Computer Science Division
University of California, Berkeley

[◊]International Computer Science Institute
Berkeley, CA

[‡]Laboratory of Cryptography and System Security (CrySyS)
Budapest University of Technology and Economics

Abstract—Spam-based advertising is a business. While it has engendered both widespread antipathy and a multi-billion dollar anti-spam industry, it continues to exist because it fuels a profitable enterprise. We lack, however, a solid understanding of this enterprise's full structure, and thus most anti-spam interventions focus on only one facet of the overall spam value chain (e.g., spam filtering, URL blacklisting, site takedown). In this paper we present a holistic analysis that quantifies the full set of resources employed to monetize spam email—

it is these very relationships that capture the structural dependencies—and hence the potential *weaknesses*—within the spam ecosystem's business processes. Indeed, each distinct *path* through this chain—registrar, name server, hosting, affiliate program, payment processing, fulfillment—directly reflects an "entrepreneurial activity" by which the perpetrators muster capital investments and business relationships to create value. Today we lack insight into even

Case study: The spam value chain

- lot of attention focuses on the problem of spam delivery
  - spam filtering and blacklisting spamming hosts or domains

- this is only the visible portion of a large, multi-faceted business enterprise
  - spam is essentially an advertising medium
  - the revenue driven by spam campaigns seems to exceed their cost
  - spam is still a profitable business

- each click on a spam-advertised link is in fact just the start of a long and complex trajectory
  - spanning a range of both technical and business components that together provide the necessary infrastructure needed to monetize a customer's visit
  - including renting botnet services, registering domains, provisioning name servers, hosting web sites or proxies, payment processing, setting up merchant bank accounts, customer service, ...
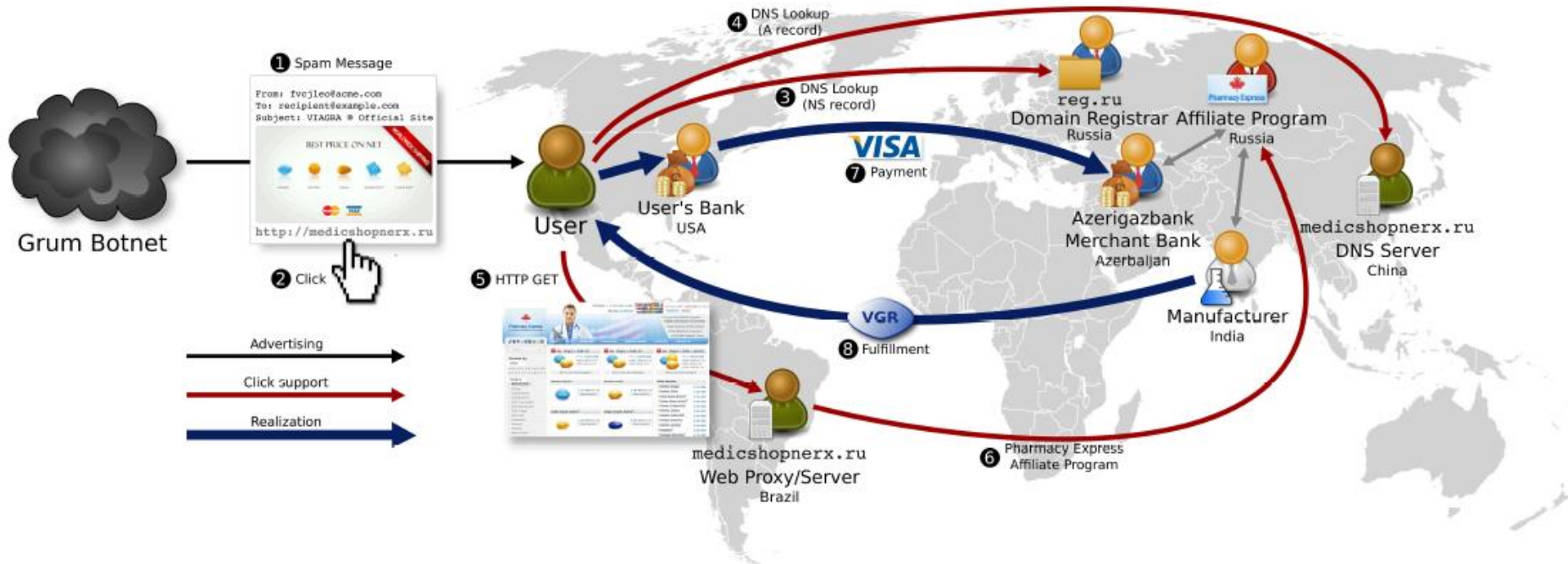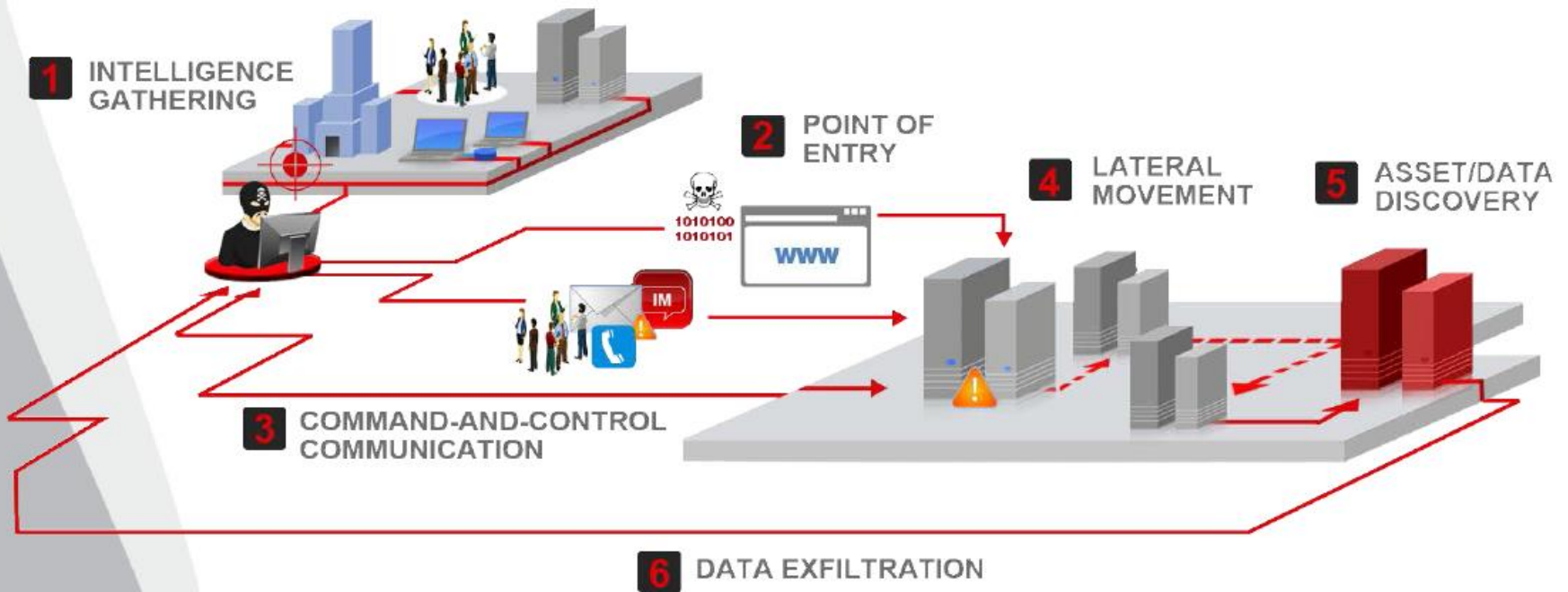
Targeted attacks use customized malware and refined targeted social engineering to gain unauthorized access to sensitive information. This is the next evolution of social engineering, where victims are researched in advance and specifically targeted.
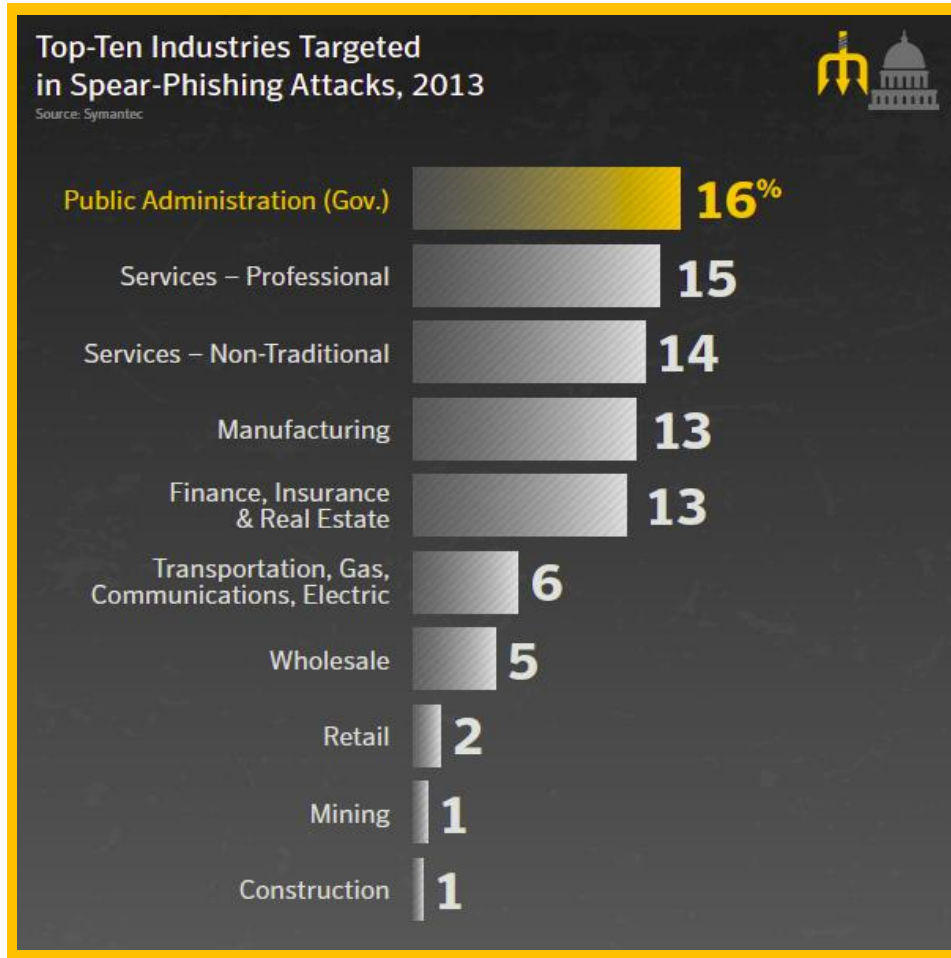
TARGETED ATTACKS

Features of targeted attacks

- highly customized tools and intrusion techniques
  - targeting a given organization or set of individuals
  - malware delivery by spear phishing and social engineering
  - multiple different exploits (often zero-day or very fresh)

- stealthy operation and persistence
  - average time of undetected compromise is ~1 year
  - careful design and intensive testing (QA)
    - to by-pass mainstream AV and security products without detection
    - to avoid causing anomalies on infected systems

- well-funded organizations behind
  - technical sophistication (e.g., advanced cryptography)
  - zero-day exploits, compromised signing keys, influence on security standards, ...

Cyber espionage workflow

source: TrendMicro Security Intelligence Blog

Targets of targeted attacks

Top-Ten Industries Targeted in Spear-Phishing Attacks, 2013
Source: Symantec

Industry	Percentage
Public Administration (Gov.)	16%
Services – Professional	15
Services – Non-Traditional	14
Manufacturing	13
Finance, Insurance & Real Estate	13
Transportation, Gas, Communications, Electric	6
Wholesale	5
Retail	2
Mining	1
Construction	1

more likely to target organizations of strategic importance, such as government agencies, defense contractors, high profile manufacturers, critical infrastructure operators and their partner ecosystem

– more than half focus on the defense and aerospace sector, sometimes attacking the same company in different countries at the same time

small organizations in the supply-chain of large ones are often used as stepping stones
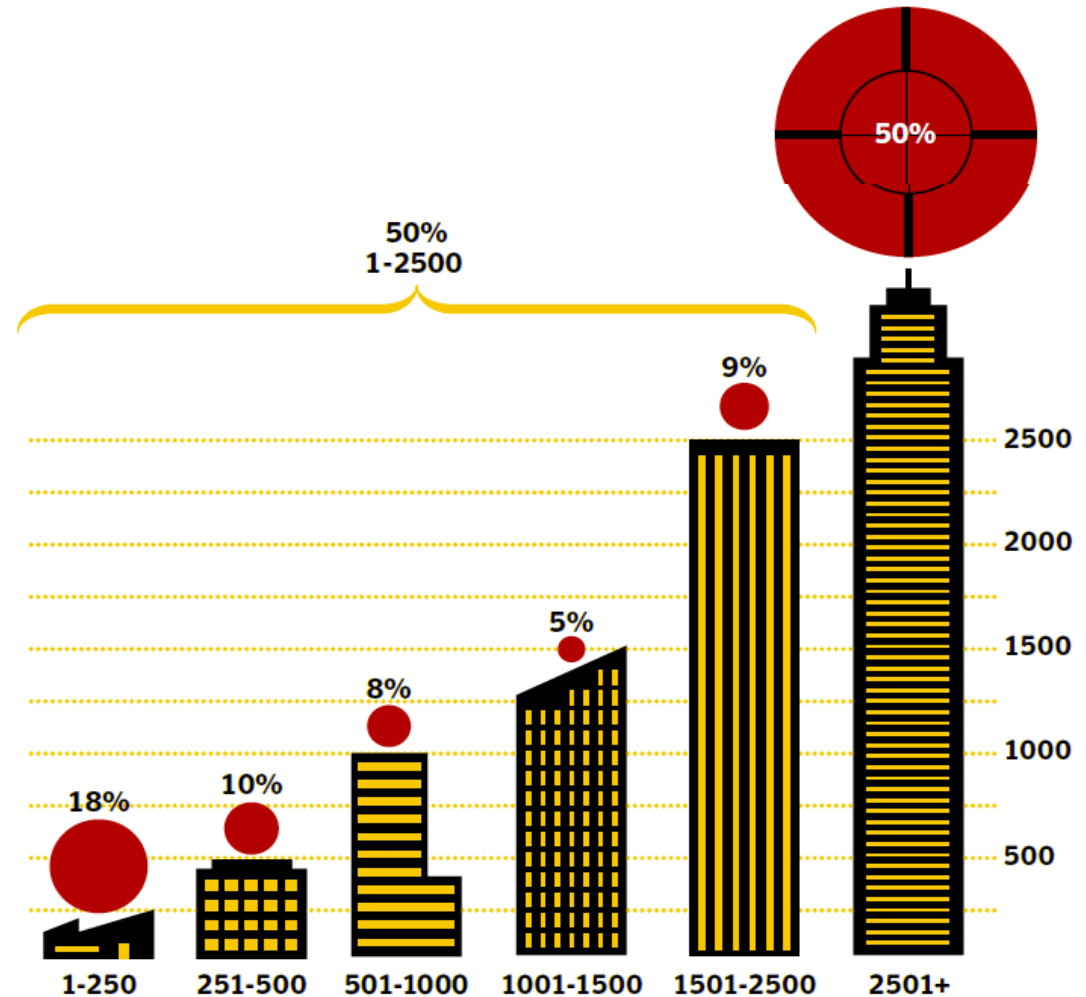
RSA Under "Extremely Sophisticated" Attack; Yes, That Includes Those Tokens

Lockheed Martin

Comodo: Web attack

Comodohacker returns in DigiNotar incident

Claiming credit for the cyberattack against Dutch certificate company DigiNotar, Comodohacker is threatening to release other fake certificates.

by **Lance Whitney** | September 6, 2011 8:35 AM PDT

Some recent examples

Sep 18 EvilGrab Malware Family Used In Targeted Attacks In Asia

6:05 pm (UTC-7) | by Jayronn Christian Bucu (Senior Research Engineer)

Recen
It is ca
detect

Chemical Attack in Syria Used as Enticement in Targeted Attack

Symantec Security Response | 06 Sep 2013 22:12:35 GMT

Targeted attacks are a daily occurrence and attackers are fast to employ the latest news stories in their social engineering themes. In a recent targeted attack, delivering a payload of Backdoor.Korplug and caught by our Symantec.cloud services, we observed an attacker taking advantage of a recently published article by the Washington Post in relation to chemical attacks in Syria. The attacker took the full text of the article and used it in

Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets

September 21, 2013 | By Ned Moran and Nart Villeneuve | Advanced Malware, Exploits, Targeted Attack, Technical, Threat Intelligence | Comments 0

FireEye has discovered a campaign leveraging the recently announced zero-day CVE-2013-3893. This campaign, which we have labeled 'Operation DeputyDog', began as early as August 19, 2013 and appears to have targeted organizations in Japan. FireEye Labs has been continuously monitoring the activities of the threat actor responsible for this campaign. Analysis based on our Dynamic Threat Intelligence cluster shows that this current campaign leveraged command and control infrastructure that is related to the infrastructure used in the attack on Bit9.
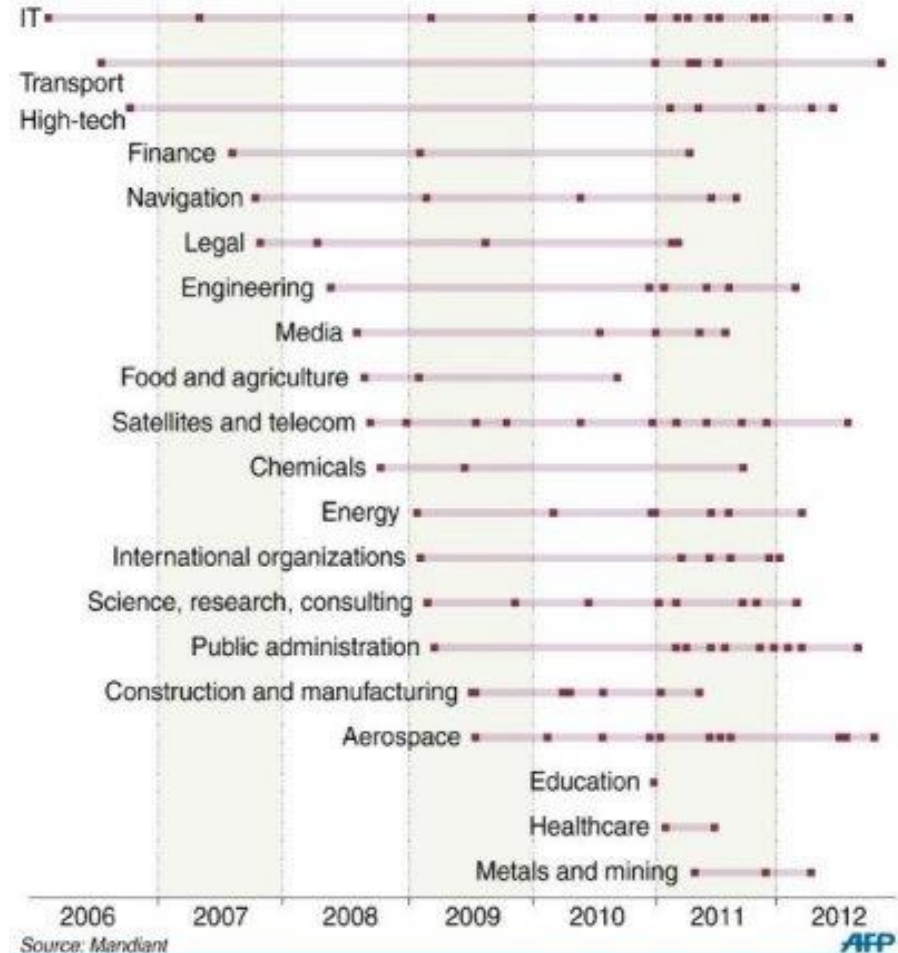
Advanced Persistent Threats

- APT1 (PLA Unit 61398)
  - nearly 150 victims over 7 years
  - maintained access to victim networks for an average of 356 days
  - size of its infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators

Unit 61398 on Datong Road in Shanghai

Source: Mandiant, Google

Hacked by APT1

Industries that have been targeted by the China-based espionage group APT1, according to US security firm Mandiant

Timeline by sector

IT
Transport
High-tech
Finance
Navigation
Legal
Engineering
Media
Food and agriculture
Satellites and telecom
Chemicals
Energy
International organizations
Science, research, consulting
Public administration
Construction and manufacturing
Aerospace
Education
Healthcare
Metals and mining

2006 2007 2008 2009 2010 2011 2012

Source: Mandiant

AFP

Advanced Persistent Threats

- Office of Tailored Access Operations (TAO)
    - cyber-warfare intelligence-gathering unit of the NSA
    - identifies, monitors, infiltrates, and gathers intelligence on computer systems being used by entities foreign to the United States (computer network exploitation)
    - has tools for breaking into commonly used hardware, including routers, switches, and firewalls from multiple product vendor lines (QUANTUM attack suite)

Examples for suppliers

GAMMAGROUP

Home · Company Profile · Contact Us

FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

COMPANY   CUSTOMERS   PRODUCTS AND SERVICES   NEWS   CONTACT

Products and Services

Intrusion Tools

Innovative cyber tools to target the suspect's devices and extract valuable intelligence:

» Passwords
» Files
» Device information

Remote Monitoring and Deployment Solutions

Easy-to-use turnkey solutions help governmental customers to
» Track suspects
» Monitor their online and offline activities
» Realize other specific requirements

Training and After-Sales Services

» Practical and operational training
» Specialist consulting
» Transfer of know how into governmental operations
» Ongoing support
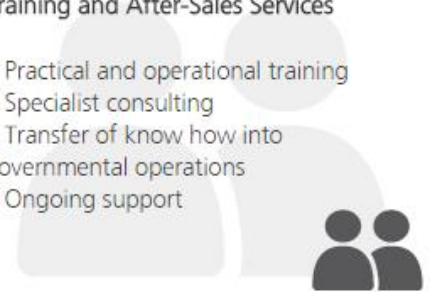
Examples for suppliers

]Hacking**Team**[About us   The Solution   Customer Policy   Careers   Contacts

Deploy
A SECRET
agent.

Total control over your targets.
Log **everything you need**. Always.
Anywhere they are.

[video]

MALWARE

Malware

- malware = **mal**icious soft**ware**
  - a.k.a. malicious code or malcode
- any code that can be added to a software system in order to intentionally cause harm or subvert the intended function of the system
- generic term that encompasses viruses, worms, Trojans, and other intrusive code

Basic types of malware

- virus
- worm
- Trojan horse

note: categorization has become increasingly difficult, because recent malware often combine the characteristics of multiple basic types

Basic types of malware

- virus
  - when executed, replicates itself by inserting its own copies (possibly modified) into other computer programs, data files, or the boot sector of hard drives (or other bootable storage media)
    - » affected program/file/medium is said to be *infected* and it serves as the *host* for the virus
  - in order to function, viruses require their hosts
    - » virus code is executed when host program/file/medium is executed/opened
    - » the virus spreads from one system to another by moving the infected host programs/files/media to other systems
  - besides replicating, the virus may perform some harmful activity
    - » e.g., steal information, delete files, or display unwanted messages
- worm
- Trojan horse

Basic types of malware

- virus

- worm
  - standalone computer program that replicates itself in order to spread to other computers
    - » unlike a virus, it does not need to attach itself to a host program/file/medium
  - often, it uses a computer network for spreading, relying on exploitable security vulnerabilities on the target computer to infect it
  - besides replicating, the worm may perform some harmful activity
    - » e.g., steal information, delete files, or display unwanted messages
    - » extensive bandwidth usage by the spreading of the worm may itself cause harm

- Trojan horse

Basic types of malware

- virus

- worm

- Trojan horse
  - standalone computer program that appears to perform some useful function, but it (also) performs some harmful activity
    - » e.g., steal information, provide a *backdoor* (Remote Access Trojan – RAT)
    - » may function as a *time bomb* (harmful activity is triggered at a specific time or by a specific event)
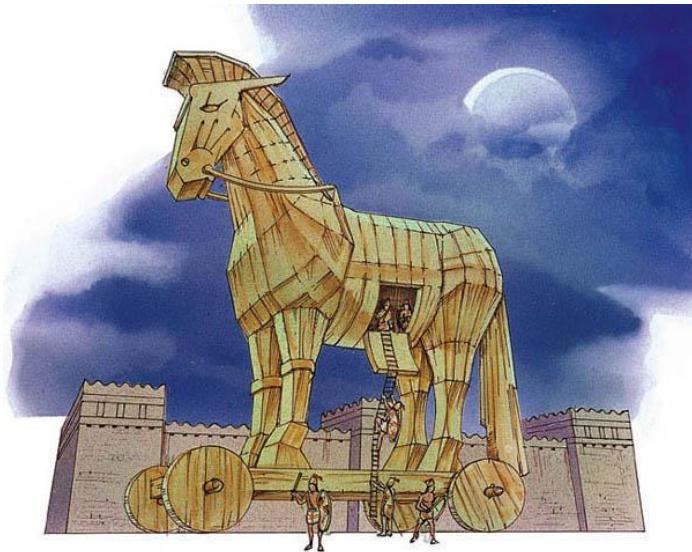
Recent trends in malware development

- mass malware development is driven by cybercrime

- malware for smart devices proliferate

- malware is extensively used in state sponsored targeted attacks (cyberwar?)

Mass malware and cybercrime

- malware infected computers represent value for criminals
  - theft of personal information and account credentials (e.g., passwords)
    » stolen information can be used directly or sold on underground markets
  - man-in-the-middle attacks
    » e.g., compromised browser may alter e-banking transactions (ZeuS)
    » e.g., compromised smart phone may intercept and redirect SMS messages containing one-time transaction authorization tokens
  - use of computing resources
    » infected computers can be organized into botnets and used for spam, DDoS, and click fraud
    » infected computers can be used for bitcoin mining
  - ransom
    » hard disk of infected computer can be encrypted and decryption key can be revealed only after some payment

- malware itself can be monetized
  - malware can be sold on underground markets

Example – ZeuS web page injection

- ZeuS injects additional HTML into legitimate pages that causes the user to input credential information not actually required by the financial Web site

- example:
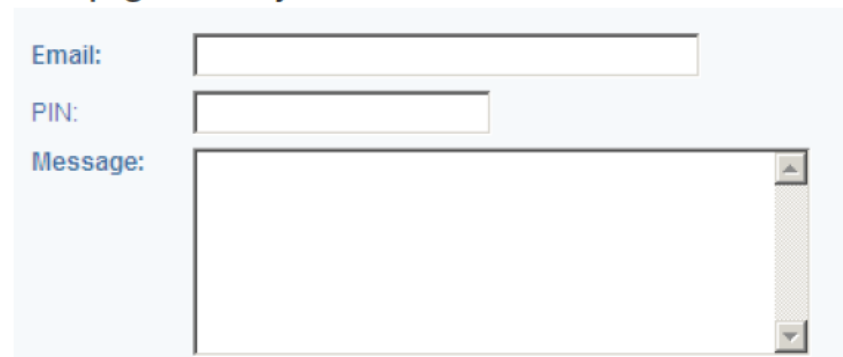
```
set _ url http://www.[REMOVED].com/contact.php GP
data _ before
name='email'*</tr>
data _ end
data _ inject
<tr><td>PIN:</td><td><input type="text" name="pinnumber" id="pinnumber" /></td></tr>
data _ end
```

Web page before injection

| Email: | |
| Message: | |

Web page after injection

Email:	
PIN:	
Message:	

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf

Example – ZeuS web page injection

- when the form is sent, ZeuS will intercept the content of the form including the PIN number and send this information to the command and control server

Intercepted form sent to command and control server

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf
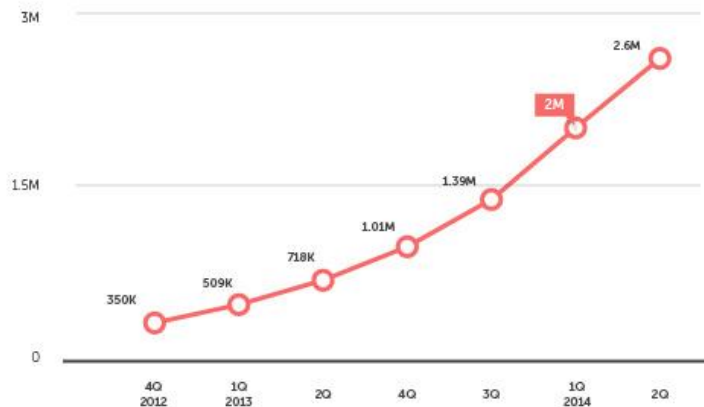
Malware for smart devices

- for criminals, there's not much difference between a PC and a smart phone as a potential target
  - smart phones have considerable computing power
  - they are always on and connected to the network
  - they run all sorts of applications originating from different sources
    - » users use them for sensitive tasks too
    - » new (potentially malicious) applications can be installed on them
  - they store or have access to large amount of personal information
  - number of smart phones is large enough → it is worth attacking them
- → compromising smart phones represents new revenue sources for attackers
- → consequently, number of malware for smart phones has been increasing exponentially in the last few years
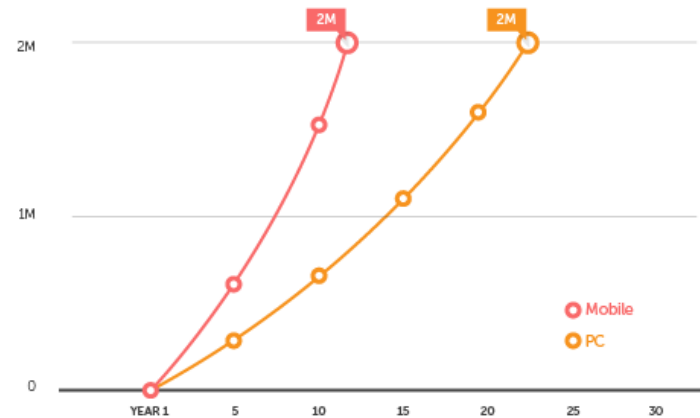
Mobile malware history and growth rate

2004
Cabir
First worm affecting Symbian Series 60 phones. Spreads from phone to phone by using Bluetooth OBEX push protocol.

2009
Ikee and Duh
Worms affecting jailbroken iPhones using Cydia app distribution system due to a hardcoded password in sshd.

2010
FakePlayer
First malware for Android makes money by sending SMS messages to premium line numbers in Russia.

2011
DroidDream
First large attack to Google Play market. Over 50 apps containing a root exploit published to Android Market.

2012
Zitmo
Popular Windows bot and banking malware Zeus improved with its Android component designed to steal banking mTANs.

2013
1000 new Android malware samples discovered every day

Masterkey
A vulnerability in Android discovered exploiting certificate validation in Android which allows malware to disguise as a legitimate app.

2014
2000 new Android malware samples discovered every day

DownAPK
Windows based malware uses Android debugging bridge to install fake banking app to Android devices connected to the infected PC.

http://www.sophos.com/en-us/threat-center/mobile-security-threat-report.aspx

Mobile Malware and High-Risk App Total Count

350K (4Q 2012), 509K (1Q 2013), 718K (2Q), 1.01M (4Q), 1.39M (3Q), 2M (1Q 2014), 2.6M (2Q)

PC and Mobile Malware Growth Rate

○ Mobile
○ PC

http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/the-mobile-landscape-roundup-1h-2014

Android vs. iOS

- Apple has a more rigorous app review process
- iOS apps are signed, developer certificate are issued only after obtaining a verified Apple credential
- Google relies more on platform protection mechanisms (permissions and sandboxing)
- Android apps are signed, but developer certificate can be self-signed
- **Android apps are also distributed via alternative app markets**
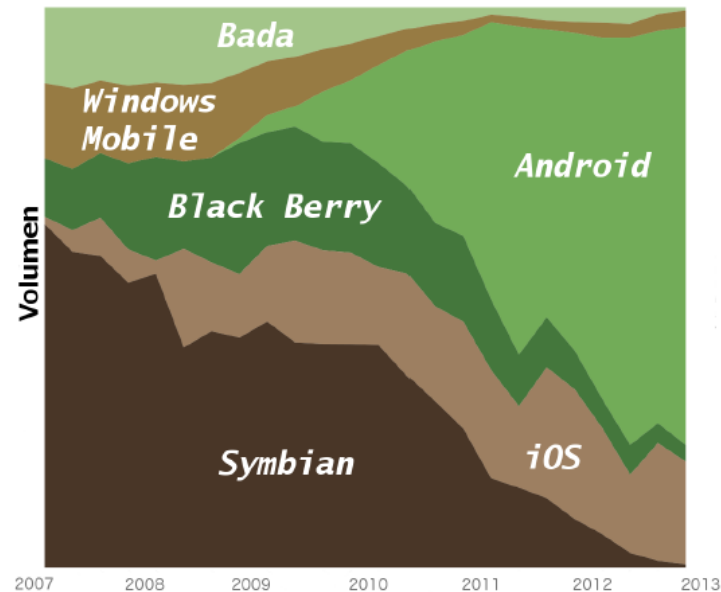
Malware and Market Share Correlation
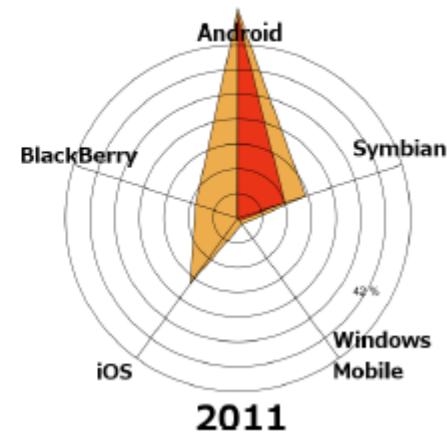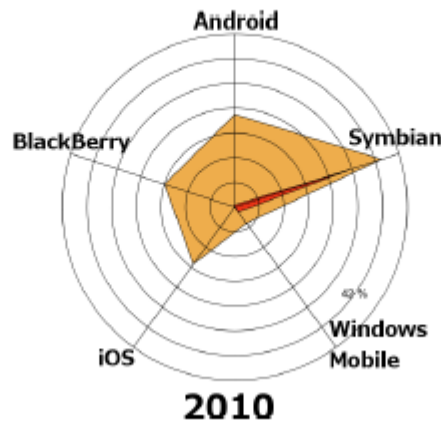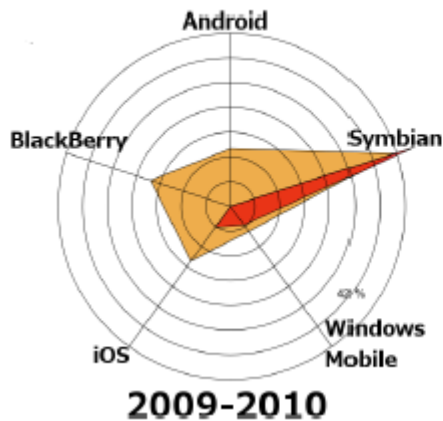
- Malware
- Market Share

2009-2010

2010

2011

Example – ZeuS-in-the-mobile (Zitmo)

- to defeat online banking attacks, banks introduced one-time authorization codes sent in an SMS message to the client (also referred to as two-factor authentication)

- attackers' response was Zitmo
  - designed to steal one-time codes without the users noticing
  - works in close collaboration with regular ZeuS
  - ZeuS running on the PC modifies the e-banking authentication page such that it also asks the user to enter data about their mobile device (make, model, and phone number), which are sent to the criminals
  - later, the user receives an SMS message on her phone asking to install a new „security certificate", which is in fact Zitmo
  - once installed, Zitmo intercepts and forwards SMS messages containing one-time codes to the criminals

Malware for targeted attacks

- malware can be used in attacks targeting a given organization or set of individuals with the objective of
  - espionage
    - » compromise of intellectual property (industrial espionage)
    - » intelligence gathering relevant for politics and military
  - sabotage
    - » disrupting critical computing and communication infrastructures
    - » destruction of physical infrastructures (e.g., blowing up gas pipelines, bringing down electricity grids, forcing the shut-down of nuclear power plants, ...)

- often, infecting the computers of the target by some malware is the easiest or cheapest way to reach the above objectives
  - e.g., strong encryption on communication links makes wiretapping hard → malware can obtain and exfiltrate the information from a compromised device (computer, router, or mobile phone) before it is encrypted
  - e.g., critical infrastructures rely on industrial control equipment (embedded computers) that have exploitable security vulnerabilities, just like PCs or smart phones → malware can compromise the operation of those equipment, which may lead to disruption of services or physical damage

- attackers behind such attacks are
  - military or state intelligence organizations (a.k.a. Advanced Persistent Threats)
 - large companies (in case of industrial espionage)

Example – Stuxnet

- a computer worm first discovered in July 2010

- designed to physically destroy uranium centrifuges in the Natanz enrichment facility in Iran

- infected computers running Windows and spread by
  - infecting removable drives
  - copying itself over the network using a variety of means
  - copying itself to Step 7 projects (runs automatically when project is opened)

- if not in the target environment, it did nothing

- once inside the target environment, it reprogramed PLCs controlling the rotation speed of the uranium centrifuges

- manipulation of the rotation speed led to physical damage
  - hundreds of centrifuges were destroyed

Stuxnet – Special features

- very specific target (nuclear facility)
- objective was physical destruction by logical means (sabotage)
- worm-like spreading → thousands of infected machines
- yet, remained uncovered for months (years?)
  - time was enough to reach its target
  - careful testing during development to avoid anomalies on infected machines
- used multiple zero-day exploits and a digitally signed driver
  - signature was created with the possibly compromised key of a Taiwanese hardware manufacturer
- used advanced privilege escalation, code injection, and rootkit techniques, as well as a peer-to-peer update mechanism
- first known malware that contained also a PLC rootkit
- required a testbed similar to the target environment
  - who has a testbed with uranium centrifuges?
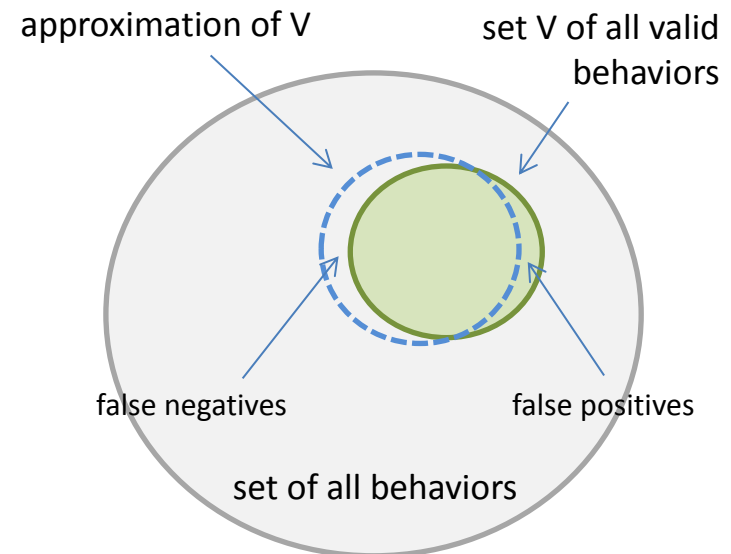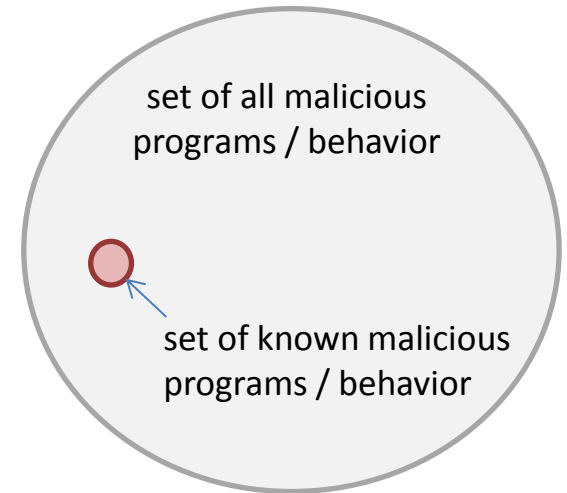- state sponsored attackers behind

Stuxnet – PLC attack

- PLC devices are loaded with blocks of code and data by a programming device (engineering workstation running a PLC management software on Windows)

- PLC block exchange between the programming device and the PLC is handled by a DLL (s7otbxdx.dll)

- Stuxnet replaces this DLL with its own copy
  - can monitor PLC blocks being written to and read from the PLC
  - can infect a PLC by inserting its own blocks and replacing or infecting existing blocks
  - can mask the fact that a PLC is infected
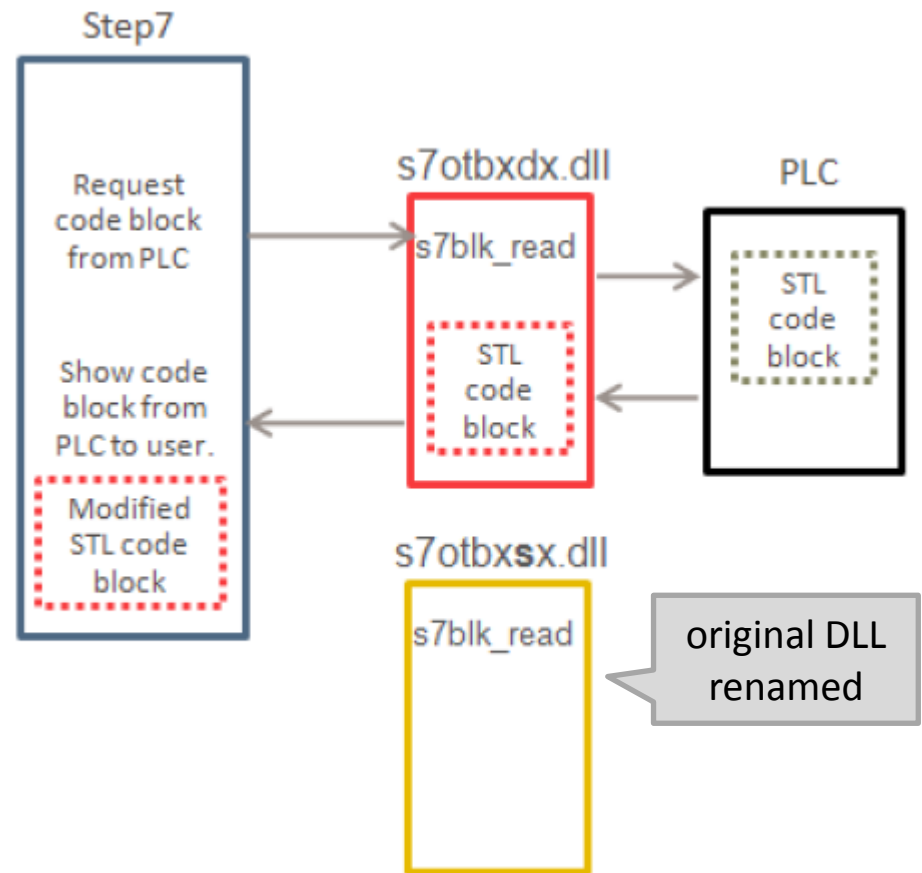
Malware detection

- signature based detection
    - uses its characterization of what is known to be malicious to decide the maliciousness of a program under inspection

- anomaly based detection
    - uses its knowledge of what constitutes normal to decide the maliciousness of a program under inspection

+ both approaches can be applied to the program code or to the program behavior
    - the signature based approach is often used for both code and behavior
    - the anomaly based approach is mostly applied for behavior features

set of all malicious programs / behavior

set of known malicious programs / behavior

approximation of V

set V of all valid behaviors

false negatives

false positives

set of all behaviors

New approaches to malware detection

- traditional anti-virus products seem to be ineffective in detecting new malware

- a range of new solutions, specifically designed to detect APT attacks, have appeared on the market
  - Cisco's SourceFire, Checkpoint, Damballa, Fidelis XPS, FireEye, Fortinet, LastLine, Palo Alto's WildFire, Trend Micro's Deep Discovery and Websense

- how good they are ???

- controversial test results published by NSS Labs in 2013
  - FireEye withdrew from the test, because:

  „the NSS sample set doesn't include Unknowns, Complex Malware (Encoded/Encrypted Exploit Code & Payload), and APTs"

Out test of anti-APT tools

- the team
  - MRG Effitas has strong experience in anti-virus testing
  - CrySyS Lab has strong experience in analysing APT attacks

- objective
  - to implement some ideas we had for bypassing cutting-edge APT attack detection tools without actually being detected
  - to test if our ideas really work in practice
  - did not aim for determining exact detection rate

Contributions

- we developed 4 custom samples in 2 weeks without access to any APT attack detection tools
  - all 4 test samples implemented RAT functionality
    - » remote interactive code execution
    - » file download and upload
  - remote communication via back-connect C&C communication
    - » polling request interval was less than 1 minute
  - no lateral movement

- we tested 5 APT attack detection solutions in Q3 2014
  - all 5 tested products are well-established in the market
  - we cannot mention vendor names

Results

- one of our 4 custom samples bypassed all 5 products

- another sample bypassed 3 products

- only the two simplest samples have been detected by the tested products
  - even those triggered alarms with low severity in some cases.

| Sample\Product	Product 1	Product 2	Product 3	Product 4	Product 5
Test sample 1	detected	detected	detected	detected	detected
Test sample 2	detected	detected	detected	detected	detected
Test sample 3	detected	bypassed	bypassed	detected	bypassed
Test 4 - BAB0	bypassed	bypassed	bypassed	bypassed	bypassed

BAB0

technology
review
Published by MIT

The Internet Is Broken

The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app

By David Talbot on February 15, 2006
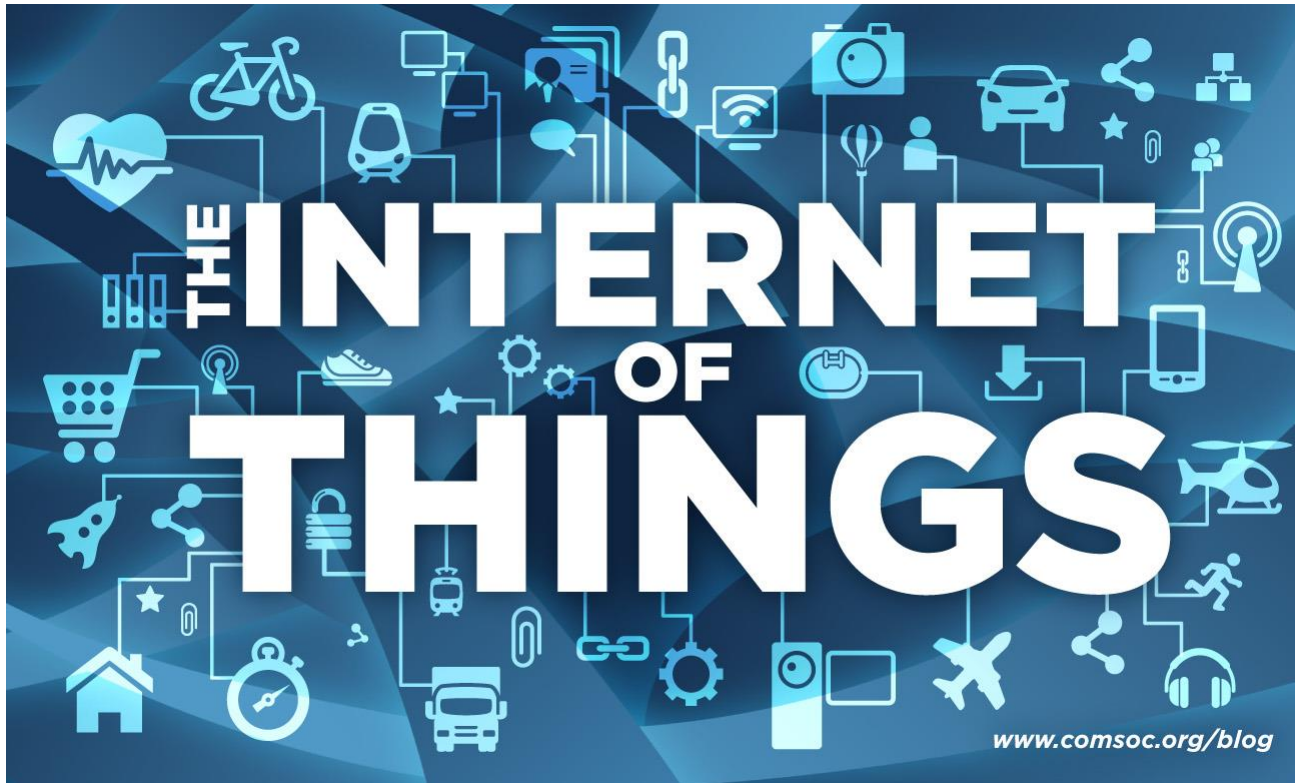
OUTLOOK TO THE FUTURE

2020

4 BILLION	$4 TRILLION	25+ MILLION	25+ BILLION	50 TRILLION
Connected People	Revenue Opportunity	Apps	Embedded and Intelligent Systems	GBs of Data

Source: Mario Morales, IDC

Camera

Infrared Sensor

Visual Control

Magnetic Door Sensor

Smoke Sensor

Gas Sensor

Automatic Doors And Windows

Automatic Curtain

Automatic Air Conditioning Switch

ET8511 IP FAM
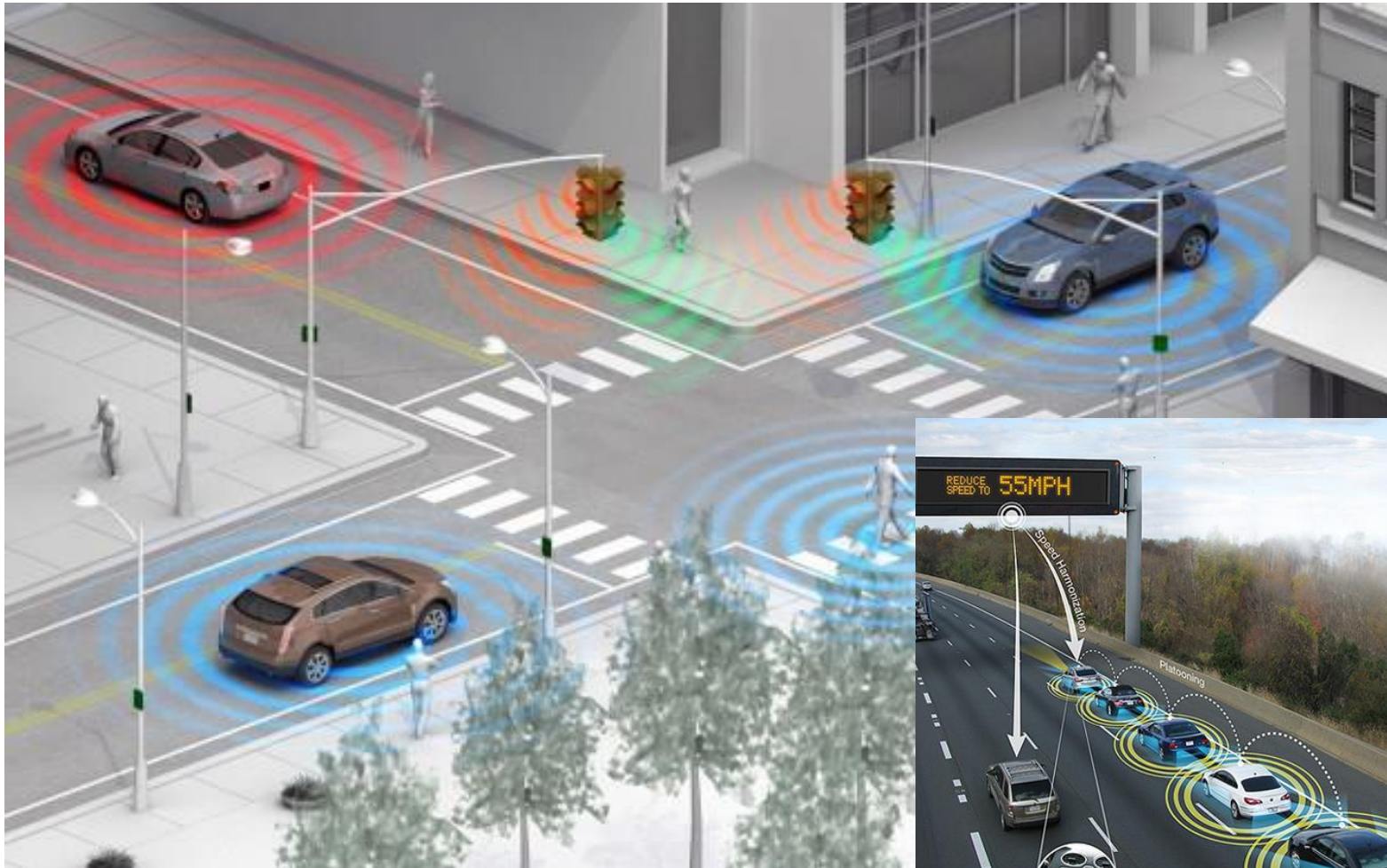
Intelligent Switch

Remote Monitoring
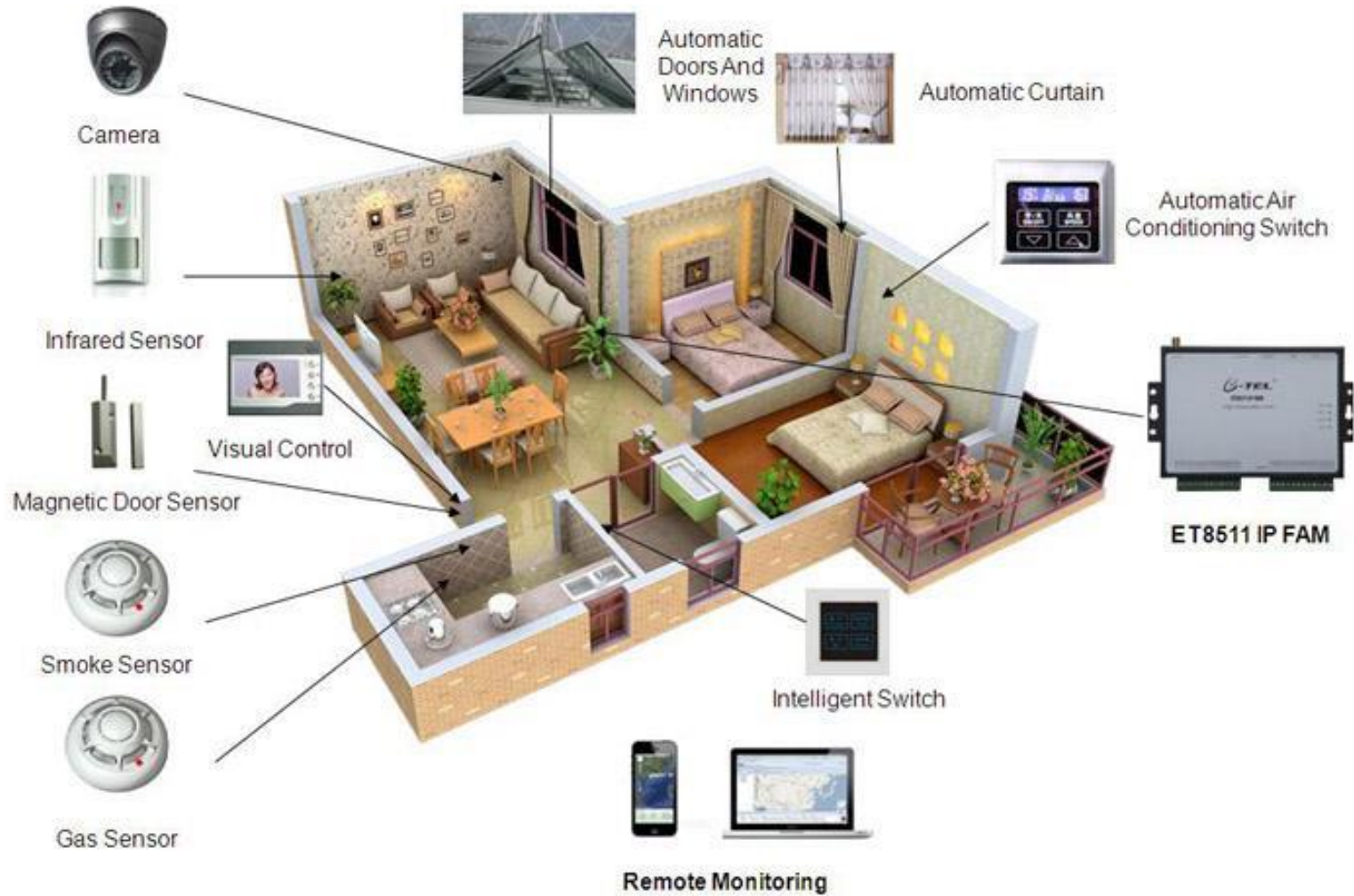
Smart vehicles
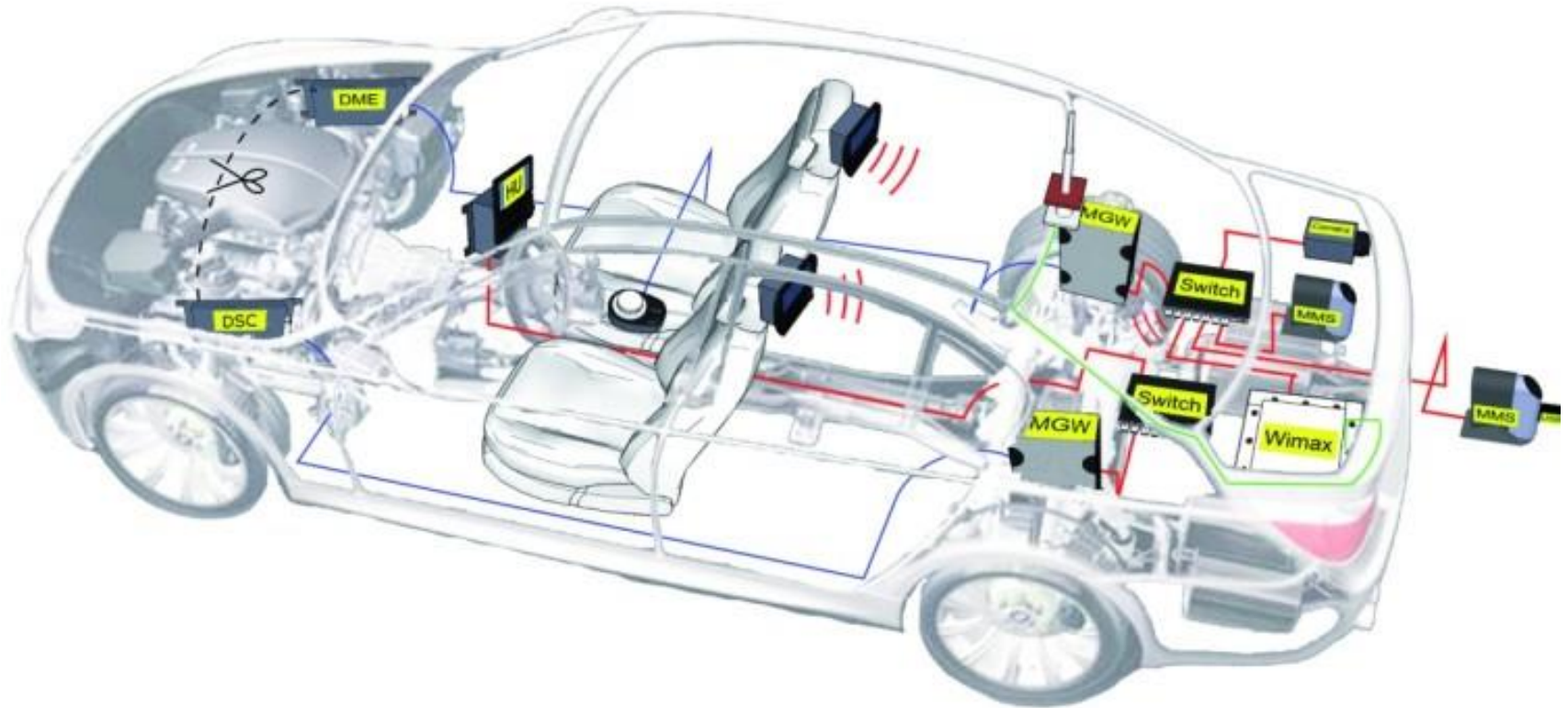
Intelligent transport systems

Photo Source: USDOT
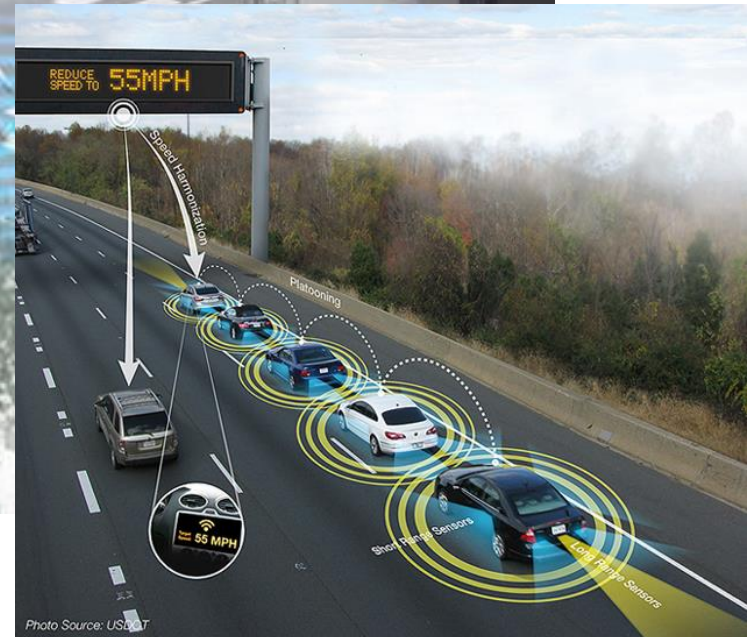
Smart parking
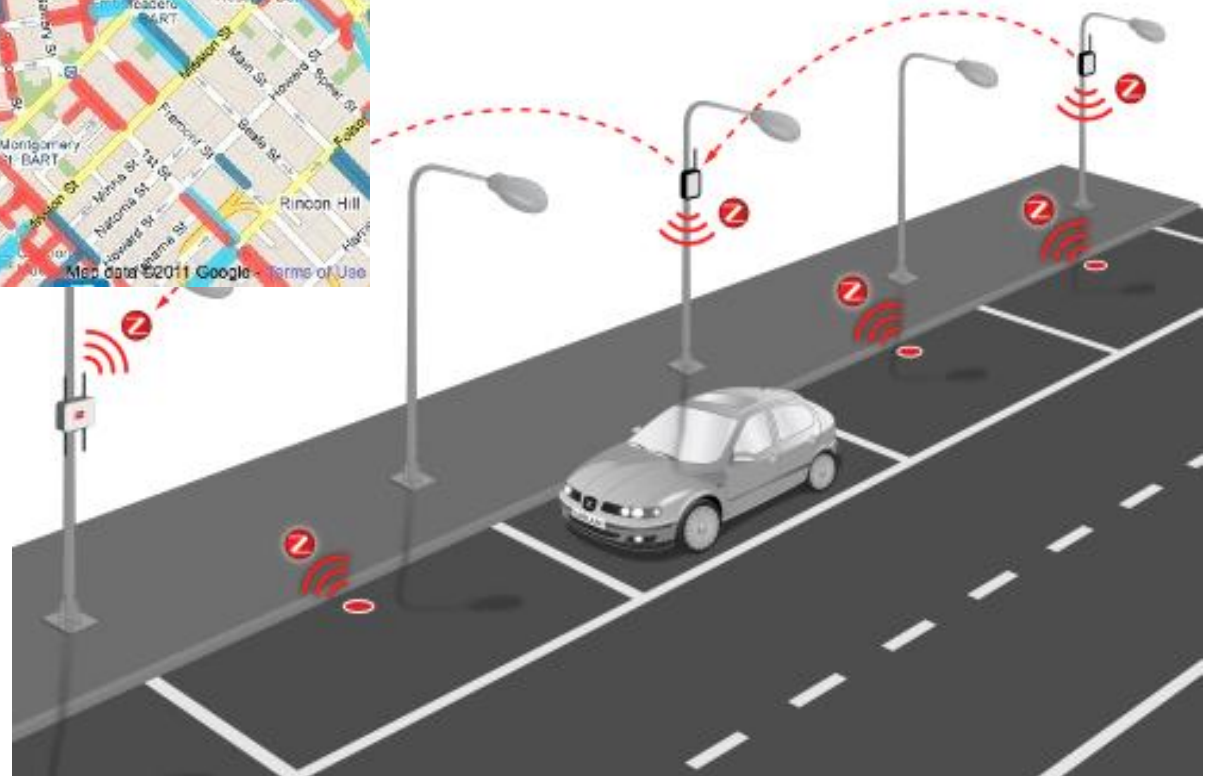
How about security?

No surprise, IoT devices are insecure

By

— Hacking a living room: Kaspersky Lab researcher finds

ENTREPRENEURS 8/03/2013 @ 8:08PM | 15,132 views

Hacking Insulin Pumps And Other Medical Devices From Black Hat

+ Comment Now + Follow Comments

H
in

Repo

Firr

David Shep

by S

(Photo: Detroit News, file)

PODCASTS

:king

Traffic Monitoring Tech Vulnerable To Hacking

POSTED BY: PAUL   MAY 1, 2014 11:36   COMMENTS OFF

Connected cars aren't the only transportation innovation that's coming down the pike (pun intended). As we've noted before: smart roads and smart infrastructure promise even more transformative changes than – say – having Siri read your text messages to you through your stereo system.

?