Imperial College London

CO331 – Network and Web Security

4. Malware

Dr Sergio Maffeis
Department of Computing
Course web page: http://www.doc.ic.ac.uk/~maffeis/331

MALicious soft**WARE**

Imperial College London

- Examples
  - Virus: malicious code that copies itself into existing programs
  - Worm: self-replicating program that infects other machines over the network or removable devices
  - Trojan: malicious program that provides some useful service in order to pose as legitimate
  - Drive-by download: code executed by visiting a malicious website
  - Spoofed software: fake antivirus or fake software updates
  - Adware: displays intrusive advertisement
  - Spyware: steal sensitive documents
  - Ransomware: block access to machine or data until ransom is paid
  - Rootkit: modifies the OS to hide malicious activity of itself or other malware
  - Keylogger: log keystrokes to steal user credentials
  - Backdoor: opens a network connection for repeated access by the attacker
  - RAT: remotely control the machine in a targeted attack
  - Botnet: recruit the machine into a botnet

Malware dimensions

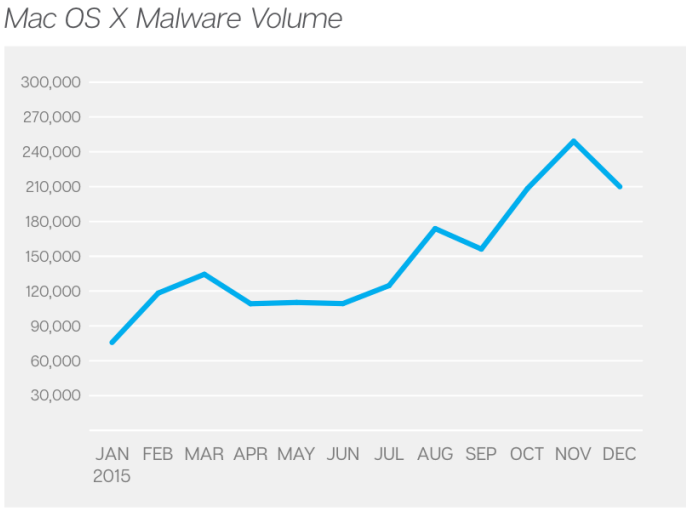
Imperial College London

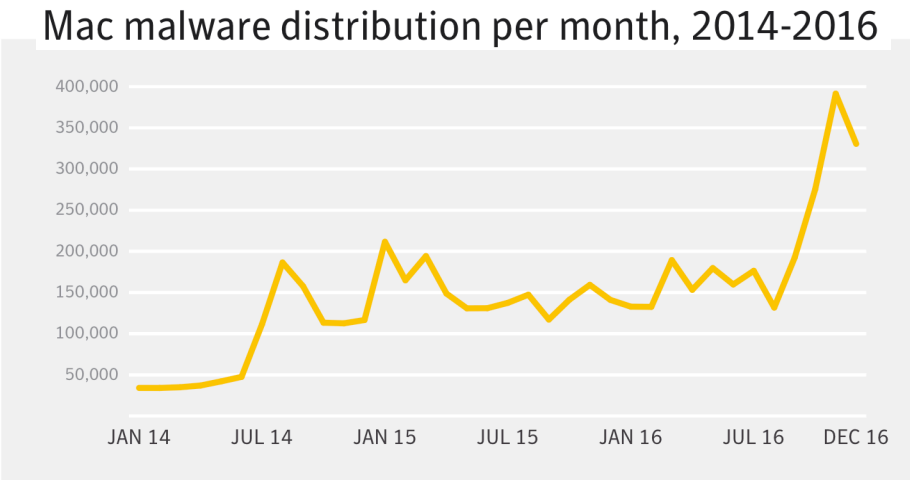
- Format
  - Injected code added to a legitimate program (virus)
  - DLL that is called by a legitimate program (fake software updates)
  - Script run by an application (macro virus)
  - Standalone executable that is run by the user or automatically by the system (trojan)
- Propagation
  - Installed by the attacker
    - Self-replication (worm)
    - Exploiting vulnerabilities (drive-by download)
  - Installed by the user
    - Social engineering (fake antivirus)
    - Compromised certificate (fake software updates)
- Privileges
  - Root: it *owns* the machine (rootkit)
  - User: can do limited damage (spyware), but can also attempt elevation of privilege to become root

Malware campaigns

Imperial College London

- Generic attacks infect as many machines as possible
  - Deliver low-cost attacks with low chance of success
  - Value in numbers: build a botnet
- Targeted attacks aim to infect the machine of a particular high-value victim
  - May be personalised: company executive, nuclear power plant employee, politician, organization, high-net worth individual
  - Fewer targets: attack may be driven by human
  - Advanced Persistent Threats (APT): attackers stealthily exploit a system over time
- Malware targets different operating systems
  - Windows is still the most popular target
  - Android, OSX, Linux are now also popular

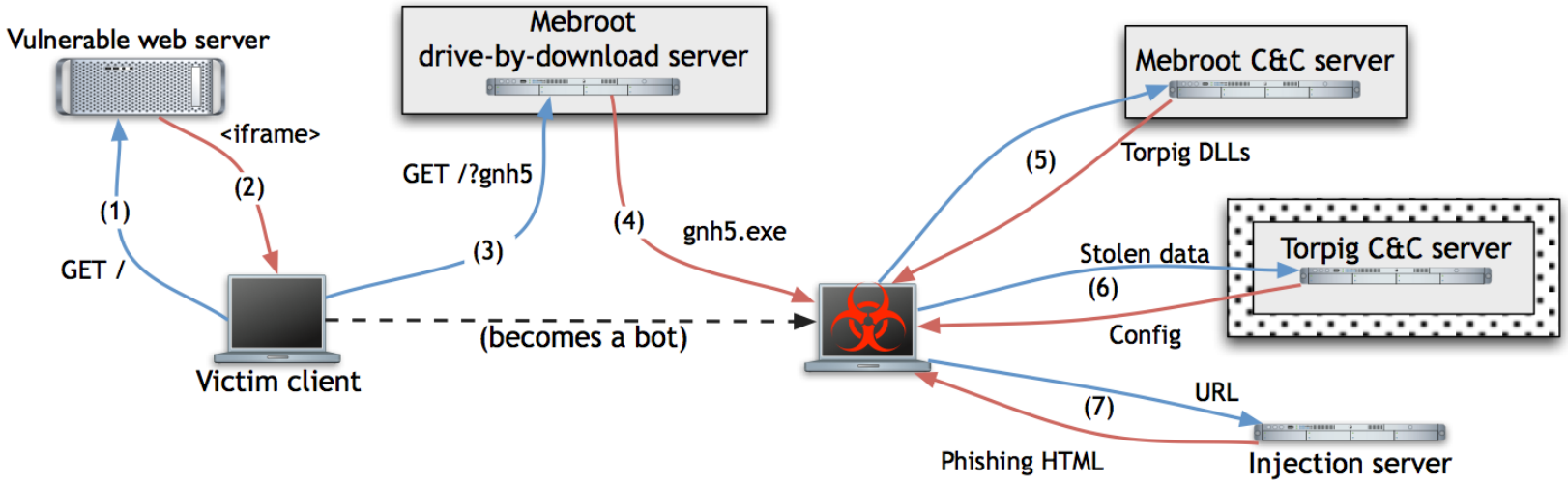




Botnets

Imperial College London

(Stone-Gross et al., CCS 2009)



- One attacker (the *botmaster*) can control hundred of thousands of infected machines
- Sophisticated *command-and-control* architectures
  - Peer-to-peer, hierarchical, star topology
  - Encrypted and stealthy communication of commands and results
  - Botmaster server may keep changing IP to avoid detection (fast flux/ domain flux)

Botnet goals

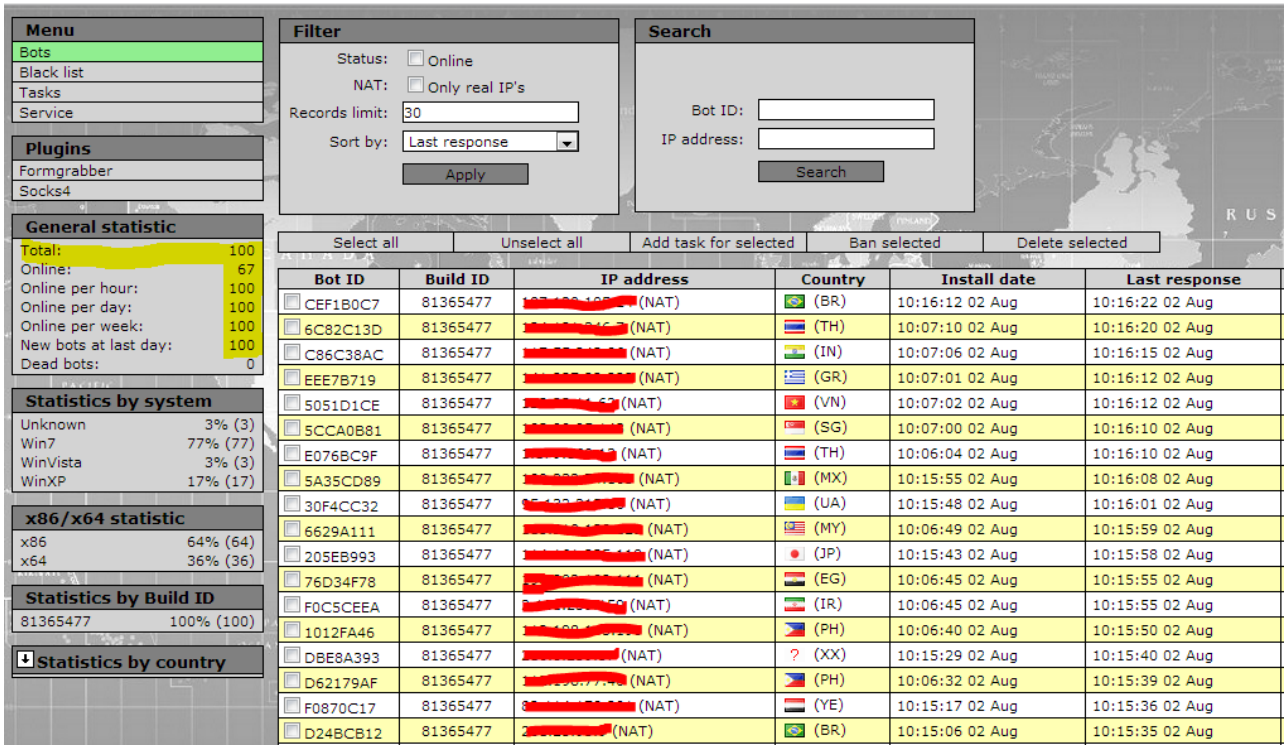
Imperial College London

- Steal user credentials
  - Credit card numbers
  - Gmail or Facebook passwords
  - Gaming passwords
- Spam: deliver unrequested email
  - Advertising illegal, counterfeit goods
  - Spread malicious attachments
  - Fraud, deception: romance scams, phishing
- Click fraud: generate advertising revenue from bogus user clicks
  - Startup from Imperial students, bought by Google: http://www.spider.io
- Distributed denial of service (DDOS): flood web servers with requests
  - Take down servers or slow them down significantly
  - Blackmail companies under attack
  - Disrupt communications on the target network

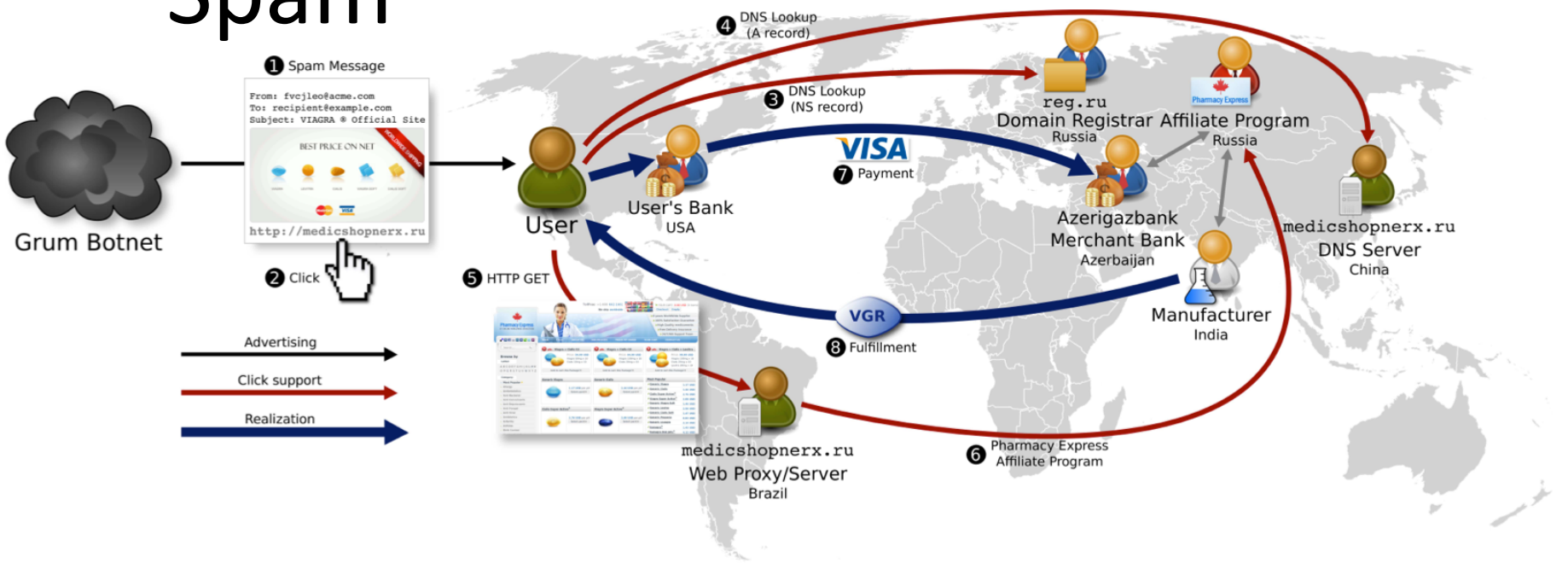
The botnet economy

Imperial College London

- Botnets have their own sophisticated economy
  - Botmaster can rent spare capacity to other criminals on the market
    - $1 = 10 machines in the US, 100 machines in Asia
  - Very organized: 24/7 technical support, training, complaints department..



Spam



- 18 billion spam emails per year are just the beginning
- The spam value chain includes
  - Botnets, domain registration, name servers, hosting services
  - Payment processing, bank accounts, customer service, products and delivery
- Spammers are the marketers for Affiliate programs that support online stores with the back-office functions
- Researchers tried to buy pharmaceuticals, replica watches and software from spam
  - 120 attempts, 56 payments succeeded, 49 products delivered
  - They did not try the meds, replicas were crude and disappointing, but software had no malware!
  - For details, see recommended reading

(Levchenko et al., 2011)

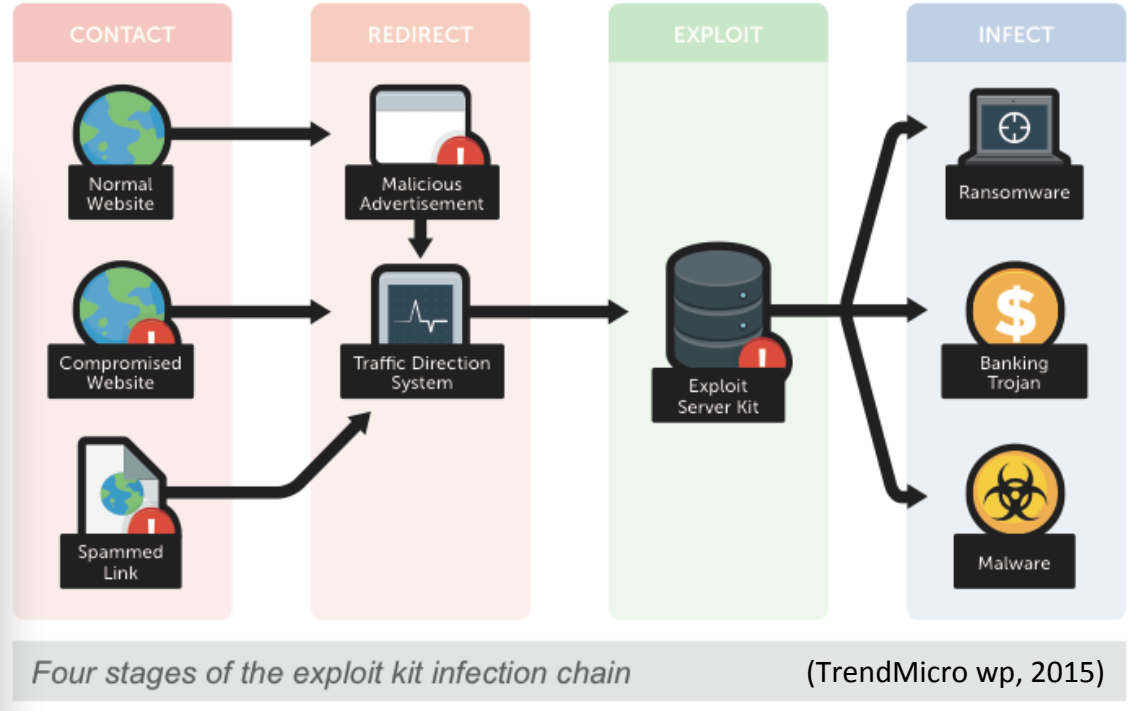
Weaponised malware

Imperial College London

- Malware can be turned into a weapon
  - Designed to affect specific targets
  - Achieve objectives that would otherwise require espionage or the use of force
- Worms
  - Can spread very quickly: parallel replication
  - Can reach air-gapped systems
  - Can cause physical damage
- Botnets
  - Can contain a large number of machines
  - Can coordinate attacks to deplete target resources
  - Can disrupt communications in a whole country
- Examples
  - 2007 DDOS on Estonia, attributed to Russia, several days of internet disruption
  - 2010 Stuxnet attack on Iranian nuclear centrifuges, attributed to US and Israel
  - 2012 Shamoon virus wipes clean 35,000 Saudi ARAMCO computers, attributed to Iran as retaliation to Stuxnet
  - 2014 US State Department and White House network infiltration, attributed to Russia
  - 2017 NoPetya cyberweapon masked as “ransomware”, damaging Ukranian assets

Commoditised malware

Imperial College London



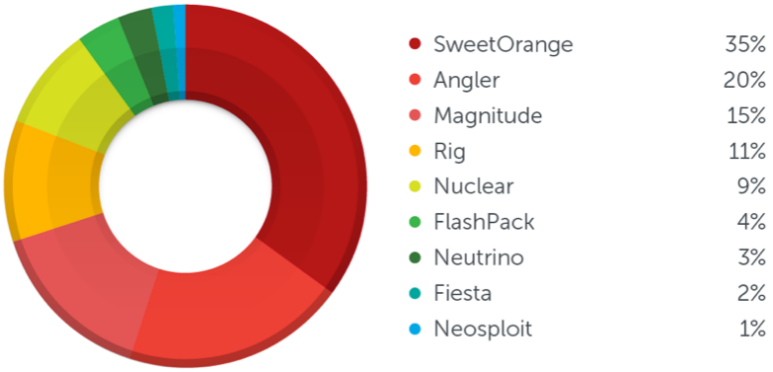
Four stages of the exploit kit infection chain (TrendMicro wp, 2015)

- Exploit kits: "commercial" malware toolkits sold or rented out to criminals
  - Capabilities: automated vulnerability analysis, exploitation and post-exploitation
  - Include Anti-Virus evasion techniques
    - Exploiting CVE-2013-7331 to find files in the system: kl1.sys => Kaspersky AV installed
  - Operator needs to subscribe to traffic from spam and malicious ads
  - Comes with administration console fine tune parameters, select victims
    - Users with a certain demographic, from a certain geographical area

Exploit kits and vulnerabilities

Imperial College London

- From: *Evolution of exploit kits,* TrendMicro working paper, 2015
- Currently 70 exploit kits available, using more than a hundred vulnerabilities



Distribution of exploit kit attacks

	Nuclear	SweetOrange	FlashPack
Internet Explorer	*CVE-2013-2551*	*CVE-2013-2551* *CVE-2014-0322* *CVE-2014-6332*	*CVE-2013-2551* *CVE-2013-3918* *CVE-2014-0322*
Microsoft Silverlight	*CVE-2013-0074*		
Adobe Flash Player	*CVE-2014-0515* *CVE-2014-0569* *CVE-2014-8439* *CVE-2015-0311*	*CVE-2014-0515* *CVE-2014-0569*	*CVE-2013-0634* *CVE-2014-0497* *CVE-2014-0515* *CVE-2014-0569*
Adobe Acrobat/ Reader	*CVE-2010-0188*		
Oracle Java	*CVE-2012-0507*		*CVE-2013-2460* *CVE-2013-2471*
XMLDOM ActiveX	*CVE-2013-7331*		

Malware detection

Imperial College London

- Detect malware just before or after infection (Antivirus)
  - Theorem: impossible to have a perfect antivirus (similar to halting problem)
  - Main approach: scan programs for *signatures* (sequences of instructions typical of the malware)
  - Metamorphic malware
    - Code is obfuscated until it does not contain known signatures
    - The new malware code has a new signature that needs to be added to the antivirus
  - Moral hazard: collecting thousands of signatures is good for Antivirus marketing
- Blacklist web pages hosting phishing and malware
  - For example, Google Safe Browsing, Facebook Threat Exchange
  - Based on human reports or crawling pages to detect malware
- Either way, the attacker always gets a window of opportunity before detection

Malware analysis

Imperial College London

- Malware samples are captured
  - Cleaning up after an infection
  - Running *honeypots*: intentionally vulnerable machines that attract attacks
    - Networks of honeypots used for worm detection
- Observe malware execution in a VM sandbox
  - Look for effects on storage, system settings, network traffic
  - Problems
    - Malware can try and kill logging processes and IDSs in the guest OS
    - Approx 16% of malware detects virtualization and behaves differently
- Dynamic analysis
  - Extract a signature based on malware behaviour, not code
  - Typically patterns of system calls made by malware
    - Read file, open network connection, send data, …
  - Malware may evade detection by mixing malicious behaviour with legitimate-looking behaviour
  - Further challenge: how to elicit malware behaviour
- Guest lecture 23/2
  - *Malware analysis - An overview and some key challenges*

Malware prevention

Imperial College London

- Most common infection vectors are vulnerabilities and social engineering
  - Educate humans to avoid direct installs
  - Update and patch software in response to vulnerability disclosures
    - Most malware uses known vulnerabilities from CVE database
    - Although "serious" malware can contain zero-days (Stuxnet had 5!)
  - Firewalls and Intrusion Detection Systems help prevent network infections
- **Certified secure systems**
  - Vision*: hardware and software should come with proof of correctness and/or security*
  - Ongoing research in academia and industry, all over the world
    - Harvard, Upenn, MIT, INRIA, NICTA, Microsoft Research, etc.
    - Imperial's contribution: JSCert, RIAPAV/RIVESST