BASIC CONCEPTS IN SOFTWARE SECURITY

Software Security

Pedro Adão 2022/23
(with Ana Matos & Miguel Pupo Correia)

TÉCNICO LISBOA

Book: Chapter1

3 main Security Attributes (CIA)

- Confidentiality – absence of disclosure of data by non-authorized parties

- Integrity – absence of invalid system or data modifications by non-authorized parties

- Availability – readiness of the system to provide its service

  – *non-authorized* requires a security policy, explicit or implicit

Vulnerabilities

- Vulnerability: a system (hw/sw) defect relevant security-wise
  - may be exploited by an attacker to subvert security policy

- They are defects but some people don't think so:

  "But some team leaders were not playing along. They were unwilling to relax schedules or use the productivity factor to offset the increased time needed to fix identified vulnerabilities [using static analysis tools]. They preferred to allocate time and budget to creating functionality rather than improving the vulnerability risk score of the their team's code. In effect, the team leaders conveniently assumed that security vulnerabilities were not defects and could be deferred for future enhancements or projects."

  - Jim Routh, *Beautiful Security*, pg 189, 2010

Attack + vulnerability

- Attack + Vulnerability → Intrusion

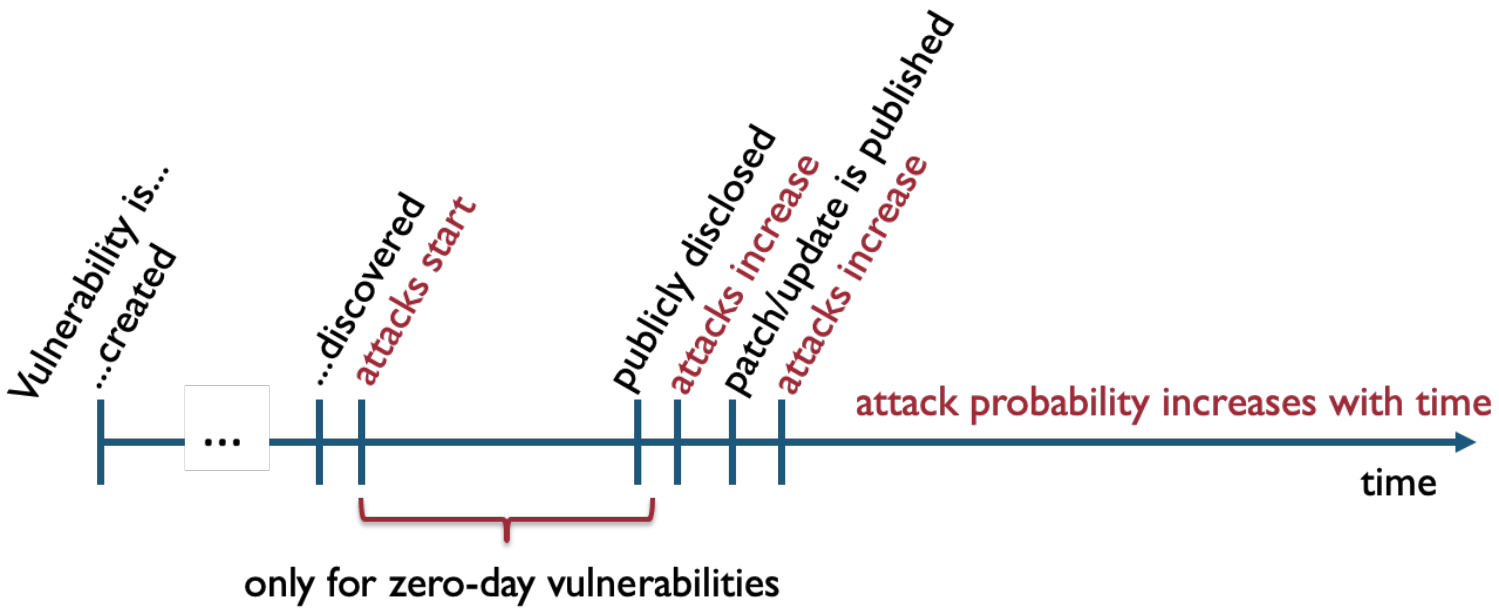
- 0-day vulnerability
  - A vulnerability not publicly known, only privately

> At least three zero-day exploits have been uncovered so far among the trove of data leaked by the attacker who breached Hacking Team. Hacking Team buys zero-day exploits in order to install its spyware, known as RCS, on

- Exploit
  - Piece of code that activates a vulnerability
  - Alternative meaning: to exploit = to run an attack

Hacking Team hack (!) 2015
http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/

Vulnerability lifecycle



Types of software vulnerabilities

a classification:

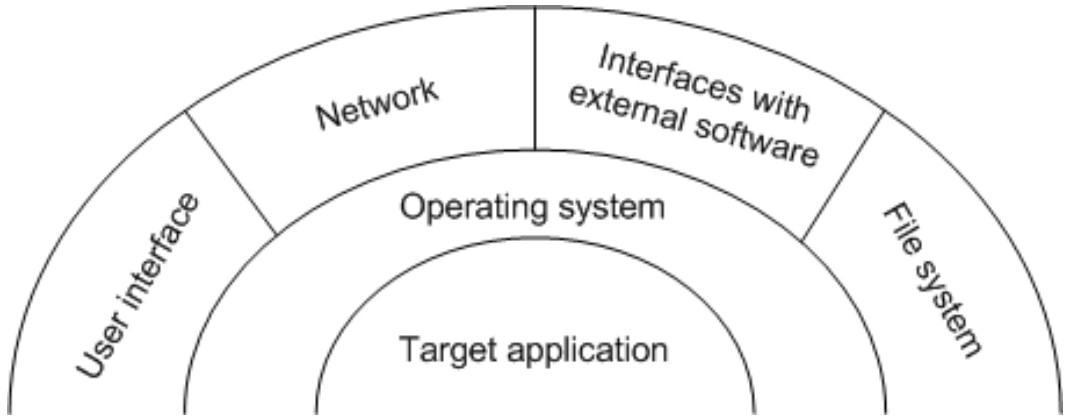
- Design vulnerability
  - inserted during the software design
- Coding vulnerability
  - introduced during programming (often a bug with security implications)
- Operational vulnerability
  - caused by the environment in which the software is executed or its configuration

Vulnerabilities (cont)

- Important sources about vulnerabilities:
- **Recent vulnerabilities (non-exhaustive)**: CERTs
  - http://www.cert.pt/ http://www.us-cert.gov/
- **Classification of vulnerabilities**: Common Weakness Enumeration
  - http://cwe.mitre.org/ http://cwe.mitre.org/data/
- **Catalog of vulnerabilities**: Common Vulnerabilities and Exposures http://cve.mitre.org/ - Example: CVE-2014-0160 (Heartbleed)
  - CVE's ids enable data exchange between security products
  - National Vulnerability Database: CWE + CVE +…
- **Recent vulnerabilities (not organized)**: Bugtraq
  - http://www.securityfocus.com/archive/1

Attack surface

- Attacks enter through interfaces – attack surface
  - what's the attack surface is the 1st question when speaking of an application security

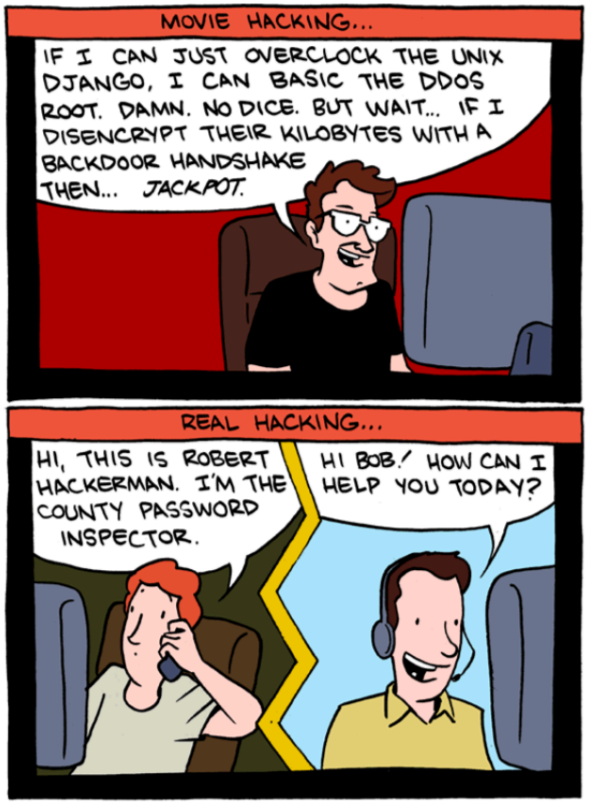


  - not trivial to understand in large software so there's much work on measuring it

Attacks

- Attack vector – several senses…
  - Type of vulnerability (BO, SQL injection,…)
  - Mode of attack (virus, worm,…)
- Can be technical vs. social engineering
- Can be directed or not directed
- Can be manual or automated

- **Classification of attacks**: *Common Attack Pattern Enumeration and Classification (CAPEC)* - https://capec.mitre.org



Manual attack

- Footprinting
  - Initial information gathering about potential targets (e.g. IP addresses, protocols, systems connected to the internet) with DNS, databases, WHOIS
- Scanning
  - Looking for reachable systems, open ports (port scanning w/*nmap*)
  - Fingerprinting – discovering software versions used
- Enumeration
  - More intrusive; info about network resources/shares, users/groups, software
- Discover vulnerability(ies)
  - Manually or with scanning tools (Nessus, OpenVAS, Havij for SQLI)
- Attack itself, running the exploit → intrusion
- Privilege escalation (by exploiting another vulnerability(ies))
- Installing rootkit / backdoor / ...
- Covering tracks

Automated attack 1: Worm

Components of a worm:

- Target selector
- Scanning motor

Equivalent to footprinting, scanning, enumeration

- Warhead – exploit code
- Load – what is carried by the worm (e.g. bot/rootkit code)
- Propagation motor – moves the worm

next several automated attacks

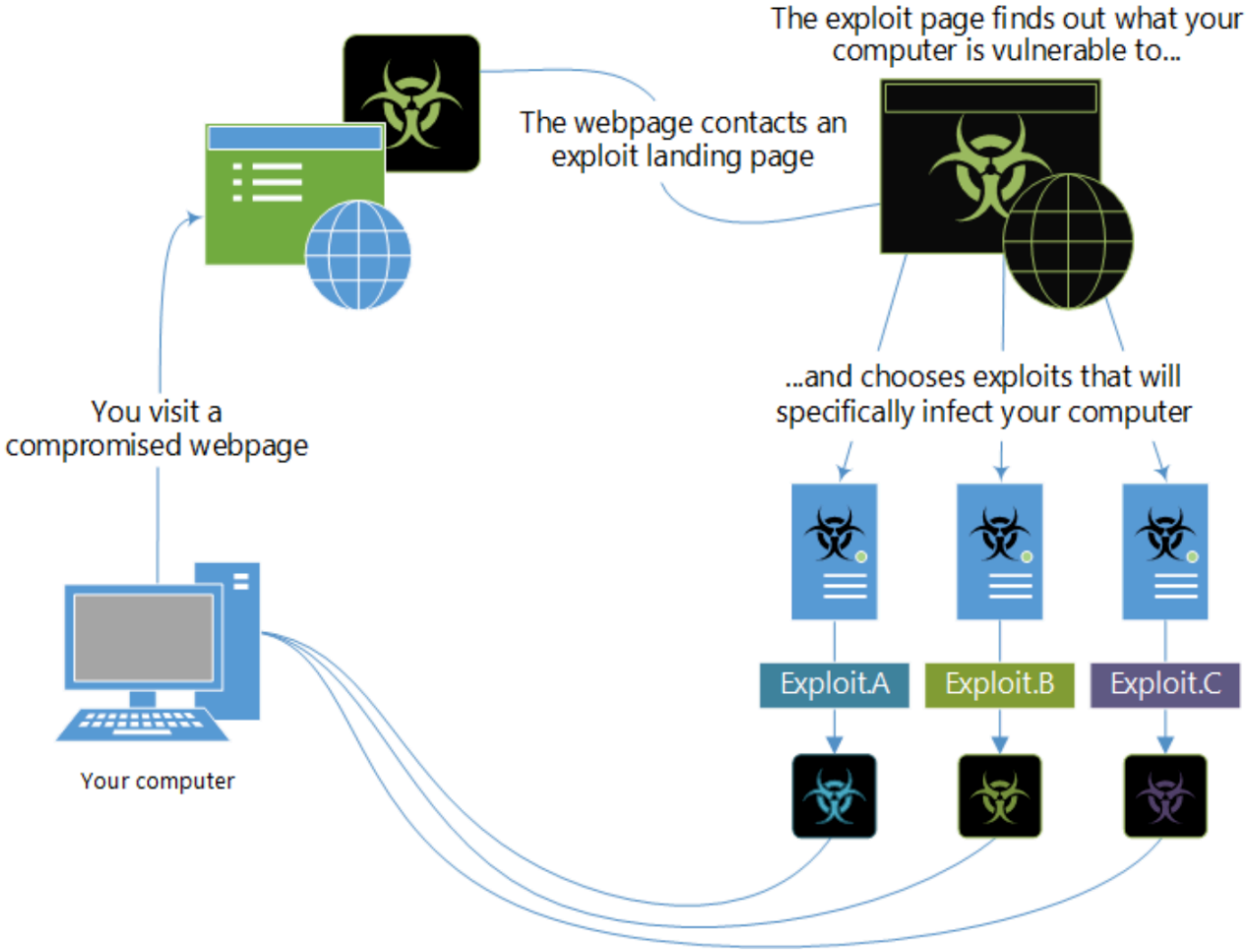
Drive-by download

- Web pages with malware
- When user accesses one with a vulnerable browser, the malware exploits the vulnerability
  - Vulnerability can be in the browser, ActiveX engine, JVM, Flash Player, PDF reader,…

    "*We analyzed the content of several billion URLs and executed an in-depth analysis of approximately 4.5 million URLs. From that set, we found about 450,000 URLs that were successfully launching drive-by-downloads of malware binaries and another 700,000 URLs that seemed malicious but had lower confidence.*"

    (paper at HotBots'07 wit authors from Google)

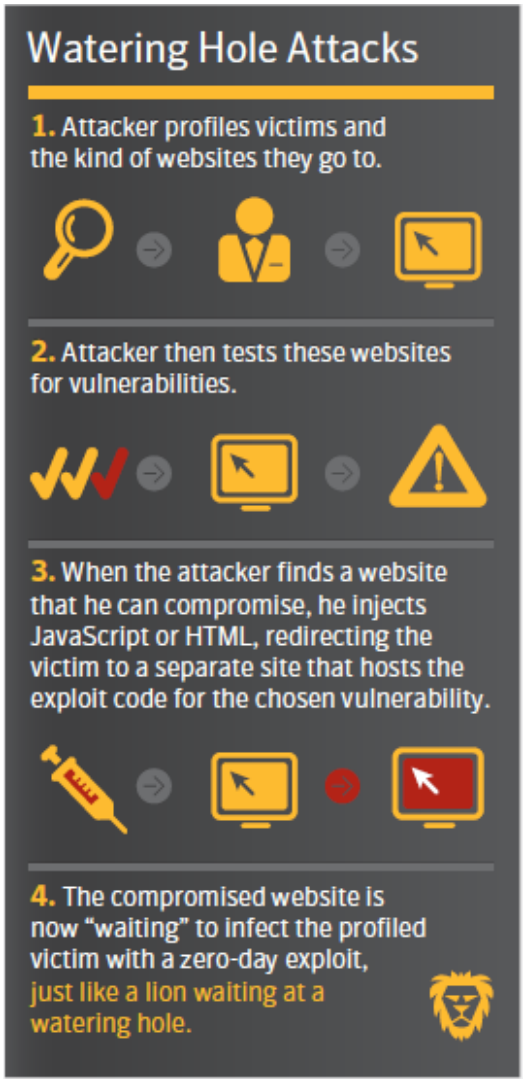
Drive-by download



source: Microsoft Security Intelligence Report vol 17, 2014

Watering Hole

- automated, targeted attack, involving a drive-by download



Picture from Symantec Internet Security Threat Report 2013

Virus and Trojans – automated

- Virus - similar to worms but propagate with physical contact – usb drives, disks, mp3 player, cameras,…
  - Thumb drive attack – leave a thumb drive at the floor; when someone collects it and inserts in a computer, a virus infects it; used against US DoD in 2009, possibly Stuxnet
  - BYOD (Bring Your Own Device) – personal devices such as smartphones, tablets, etc. may bring malware
- Trojan horse – similar but requires user to run an infected program
  - Emails with attachments that are Trojans is one of the most common forms of automated attacks today

Backdoors, Rootkits, Bots, RATs

- Backdoor – allows attacker to come back later; related concepts:
- Rootkit – a malicious program that hides at low level
  - Classical: fake login program that allows users not in /etc/passwd to enter; false ps to hide malicious programs
- Bot or Remote Access Trojan (RAT) – listens at a port until it's contacted by a command&control server (C&C) to do something; ex:
  - Access and extrude information
  - Invade other machines in the organization
  - Send SPAM, send rogueware announces, do DDoS attacks

Ransomware, Scareware, Rogueware

- Ransomware – malware that encrypts disks or databases and demands a ransom

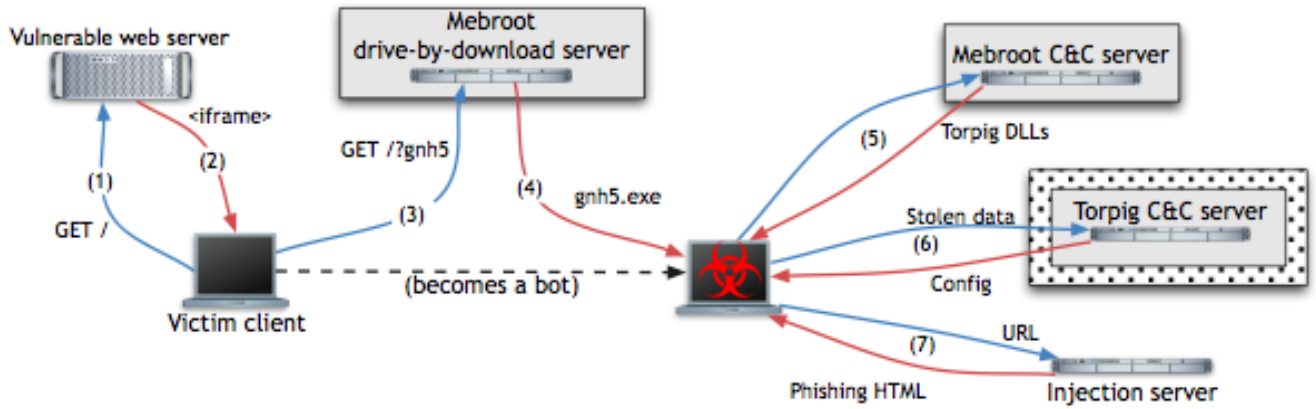
- Cryptojacking - malware that mines Bitcoin or another cryptocurrency, consuming electrical power
- Scareware – scam to convince victims to buy/install useless or malicious software (e.g., fake antivirus software)
- Rogueware – malicious software used in these scams

Phishing and spear phishing

- Phishing – send an email, Facebook post,… that leads user to do a dangerous operation (usually to introduce credentials)
  - Involves social engineering, victim has to “cooperate”
  - http://www.seguranca-informatica.net/2013/03/phishing-e-mulas.html
- Smishing – the same but with SMSs
- Spear phishing – a directed phishing attack
  - Attacker sends email with exploit to person with adequate access level at company

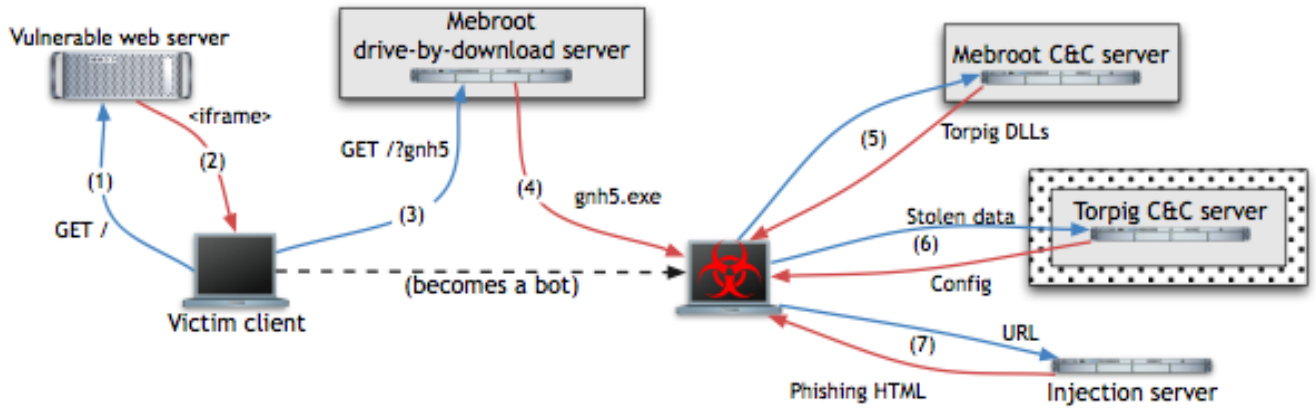
Torpig – a sophisticated malware

- Infection of bots with drive-by download:
- Attackers modify legitimate but vulnerable server for some webpages to request JavaScript code from the attacker's web server
- (1) The victim's browser accesses the vulnerable server
- (2) JavaScript code exploits the browser/plugins/etc.
- (3-4) If an exploit is successful, the script downloads and installs the Mebroot rootkit (replaces Master Boot Record) – victim becomes a bot



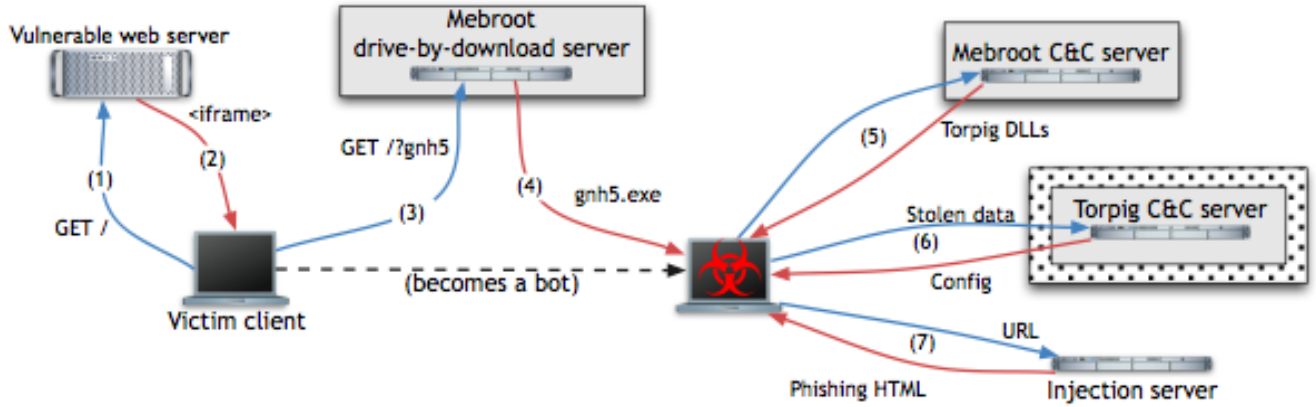
Torpig (cont.)

- Mebroot has no attack capacity:
- (5) Contacts C&C server to obtain malicious modules
- Stores them encrypted in directory system32 and changes the names and timestamps to avoid suspicions
- Every 2h contacts C&C server: sends its configuration (type/version of modules); gets updates; communication is encrypted over HTTP



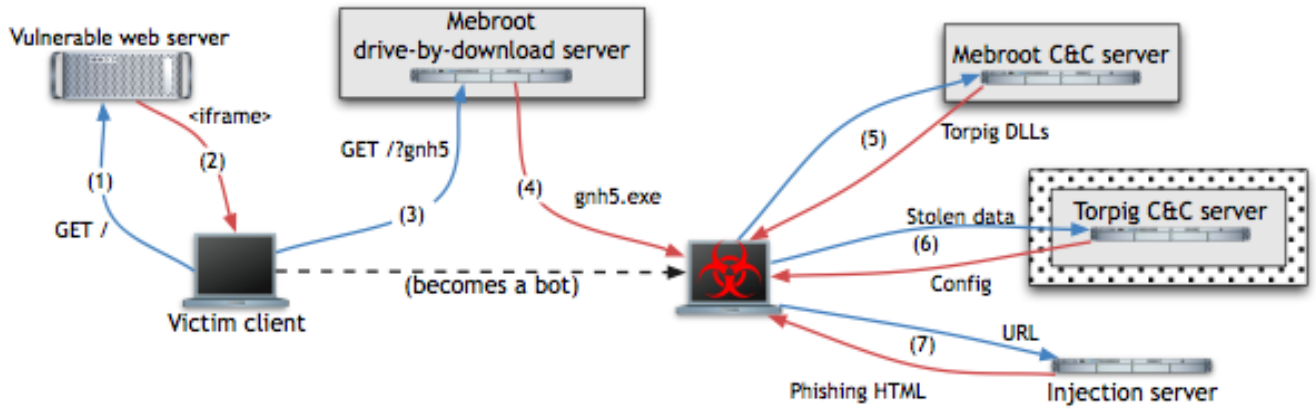
Torpig (cont.)

- (5) For Torpig, the Mebroot modules are Torpig's
  - They are injected in legitimate software: service control manager (services.exe), file manager, web browsers, email clients, etc.
- Torpig inspects those programs and steals data
  - e.g., credentials for online accounts, passwords
  - (6) Every 20 minutes contacts C&C to upload stolen data
  - C&C replies ok or tells bot to do… (next slide)



Torpig (cont.)

- Man-in-the-browser phishing attack
  - (7) When victim visits domain from a list (e.g., a bank), the bot contacts an injection server
  - Injection server returns attack data: URL of trigger page in the legitimate domain (typ. the login page), where to send results, etc.
  - When user visits trigger page, Torpig asks injection server for another page (e.g., that asks for credit card number)



Intelligence-driven security

- Data like the previous is important to know what to protect
- Current trend in security: intelligence-driven
  - Security based on recent intel about threats
  - Security vendors get “intel” from monitoring their customers, the dark web, and other sources
  - then sells it to other customers

Summary

- Security attributes
- Vulnerability, attack,…
- Types of attacks and malware