on hacking & security

Ange Albertini

@angealbertini

✉ ange@corkami.com

http://www.corkami.com

Preamble

Error is human,
so programs have ***bugs***.

Some bugs can be ***exploited***
to ***hack*** into a system.

Java, August 2008

Privilege escalation via hand-made object
→ silent remote execution

```
private static final String ser = "ACED00057372001B6A6176612E [...]";
ObjectInputStream oin = new ObjectInputStream(
    new ByteArrayInputStream(
        PayloadX.StringToBytes( ser )
        )
    );
```

MySQL, June 2012

Invalid authentication check
→ instant login as *root*

```
for i in `seq 1 1000`;
    do mysql -u root --password=bad -h < remote host > 2>/dev/null ;
done
```

Skype, November 2012

Password reset loophole
→ hijack account with just e-mail address

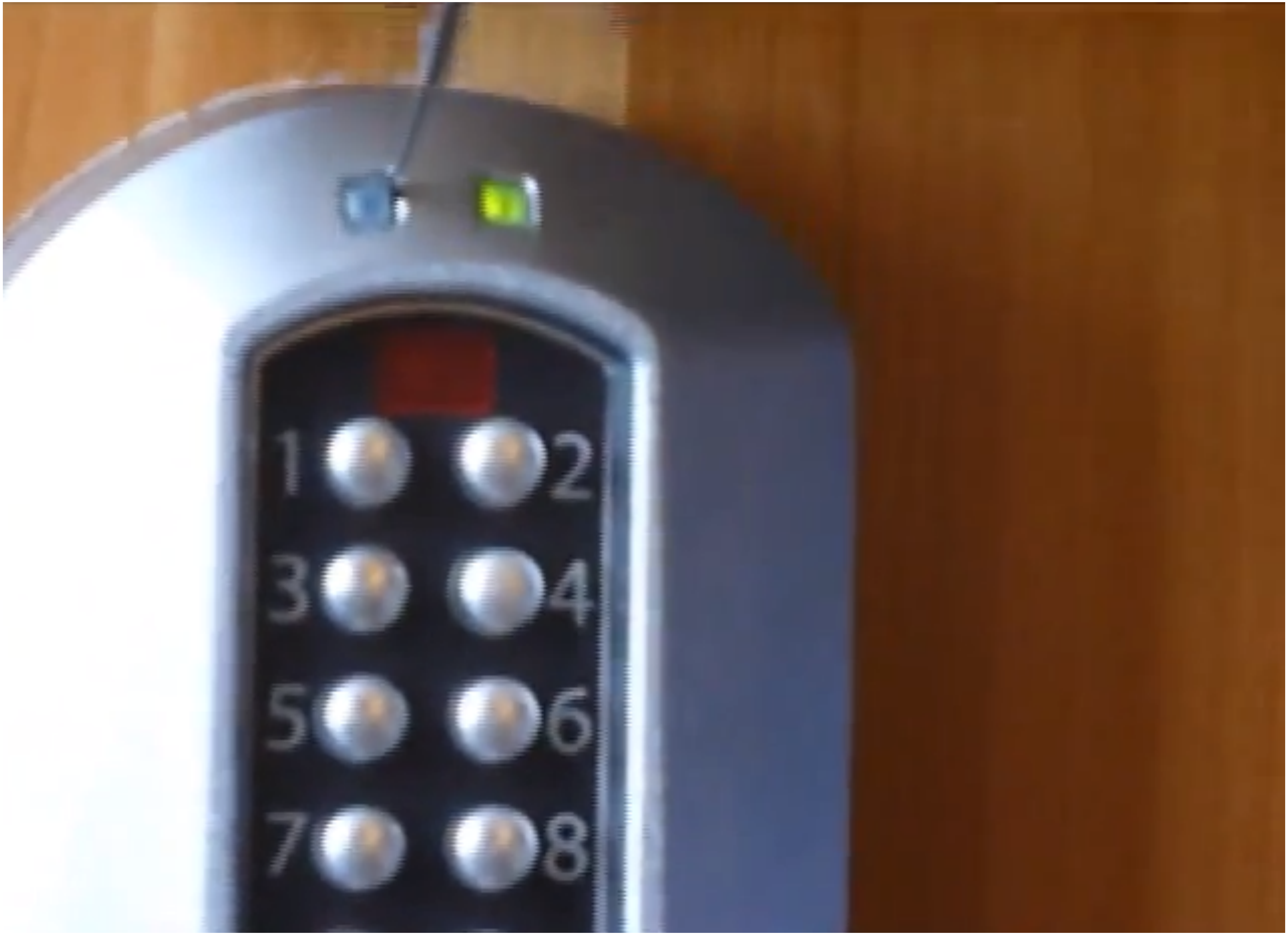
1. enter target e-mail
2. create associated dummy account
3. login with dummy
4. request password reset for target account

→ access contacts + conversations!

Uhlmann & Zacher lock, 2008

electronic lock. uses current to unlock

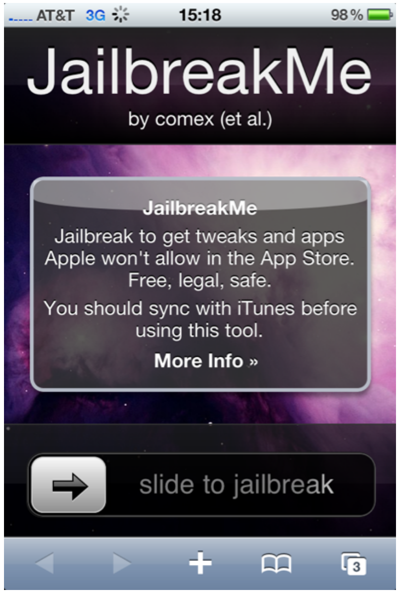
1. rotate ring magnet
    a. generates current
2. open lock


1
2
3
4
5
6
7
8

Kaba E-Plex 5800 lock, 2011

US Government approved (FIPS 201)

- insert pin under the light cover
  - short-circuiting
- open lock



JailbreakMe

by comex (et al.)

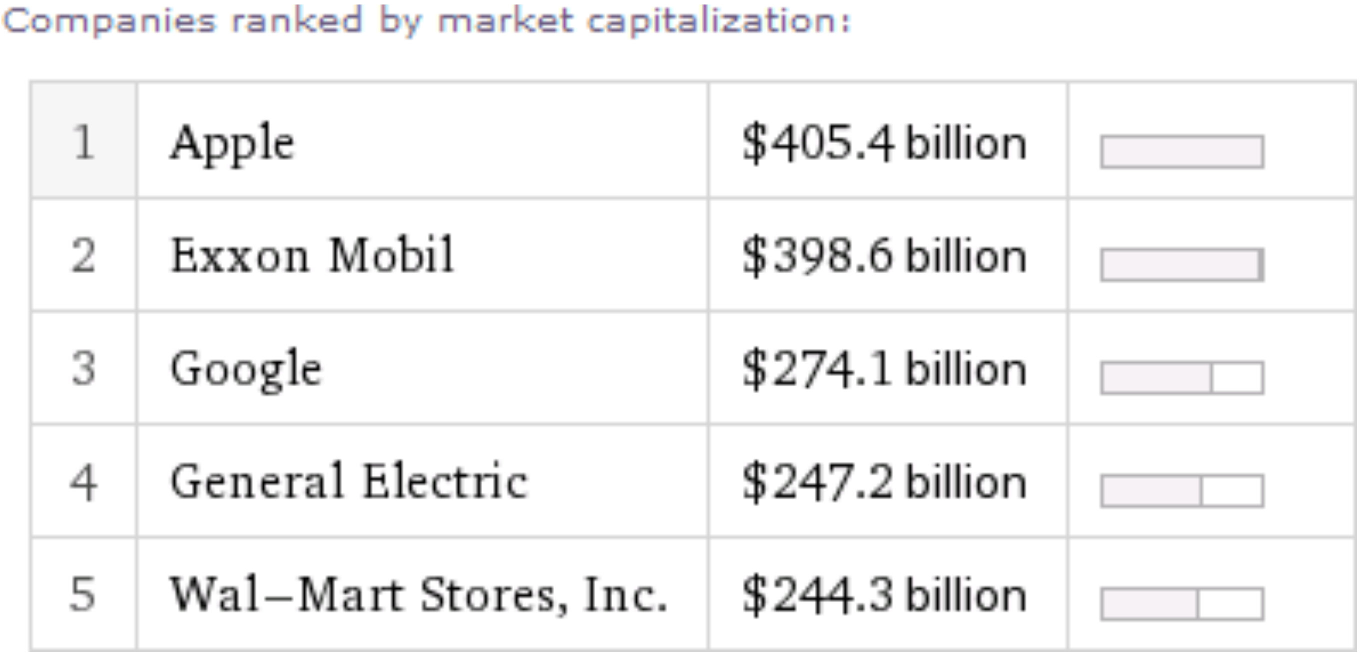
JailbreakMe

Jailbreak to get tweaks and apps Apple won't allow in the App Store. Free, legal, safe.

You should sync with iTunes before using this tool.

More Info »

slide to jailbreak



Companies ranked by market capitalization:

1	Apple	$405.4 billion	
2	Exxon Mobil	$398.6 billion	
3	Google	$274.1 billion	
4	General Electric	$247.2 billion	
5	Wal–Mart Stores, Inc.	$244.3 billion	

Apple's iPhone

- the biggest company
  - focusing on a handful of products
- their flagship product
  - fully controlled, software & hardware
- yet repeatedly hacked
  - for fame(?) only

knitting machine, tamagotchis, cars, CPUs

Hacked compagnies

- Sony, Microsoft, Facebook, Google, LinkedIn..
- T.J. Maxx
  - 45.7 million CCs stolen
  - obsolete Wi-Fi encryption
- NIST's National Vulnerability Database
- Certificate authorities
  - to enable more hacks
- Equifax
  - after their "blind" CISO's keynote

With ***enough*** resources,
any-thing/one can be hacked.

No ***ready-made*** software
will save you:
your attacker can have it too,
and has **time** to prepare

"but I have an anti-virus!"

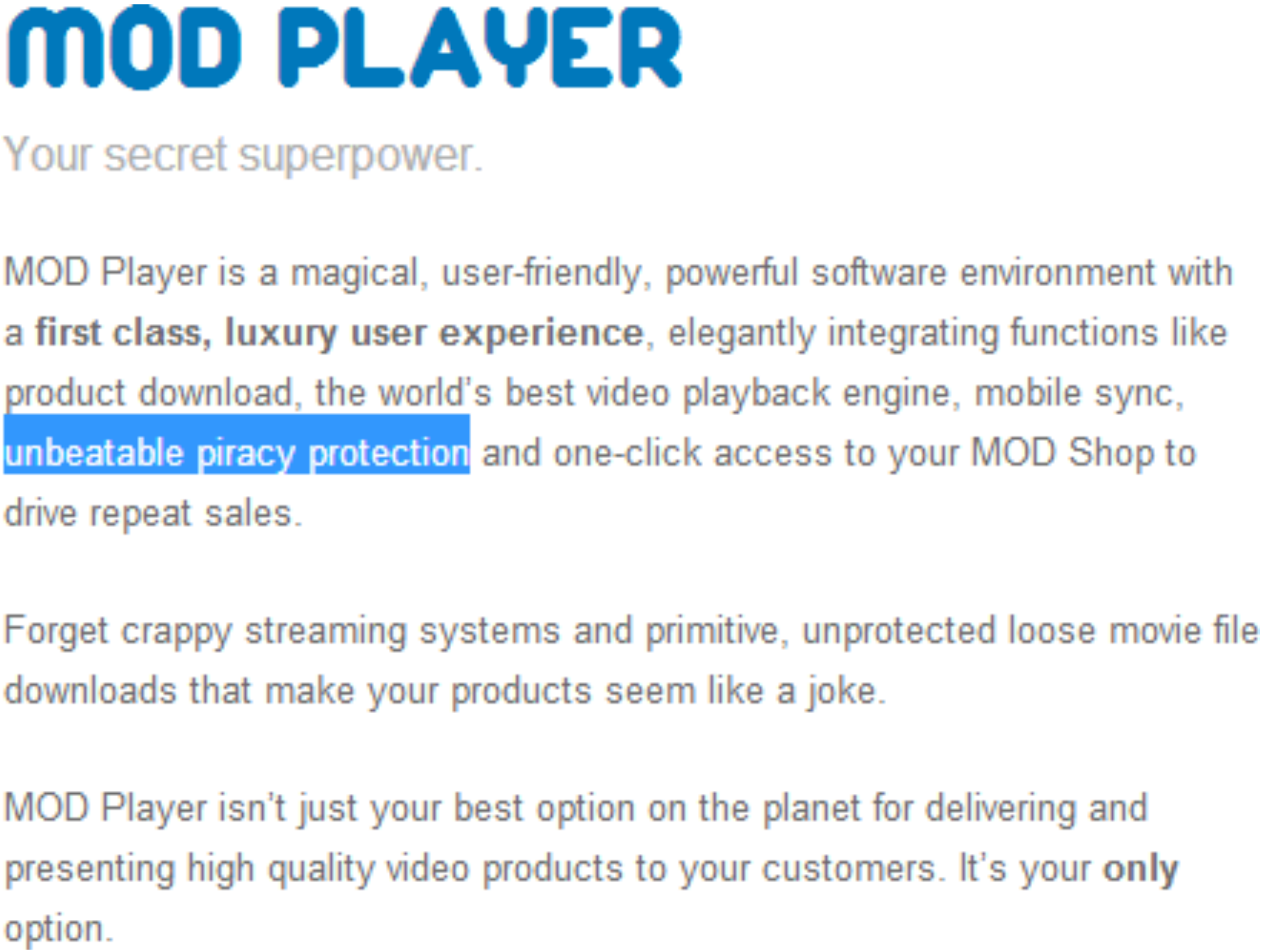
```
repeat {
    1.  modify(virus)
    2.  check(www.VirusTotal.com)
} until (NOT detected)
```

think "Great wall of china"

Ready-made software can only help against ***generic*** attacks!

think about jails

- guards
  - avoid routine, plannification
- reduce points of entry
- increase visibility



MOD PLAYER

Your secret superpower.

MOD Player is a magical, user-friendly, powerful software environment with a **first class, luxury user experience**, elegantly integrating functions like product download, the world's best video playback engine, mobile sync, unbeatable piracy protection and one-click access to your MOD Shop to drive repeat sales.

Forget crappy streaming systems and primitive, unprotected loose movie file downloads that make your products seem like a joke.

MOD Player isn't just your best option on the planet for delivering and presenting high quality video products to your customers. It's your **only** option.

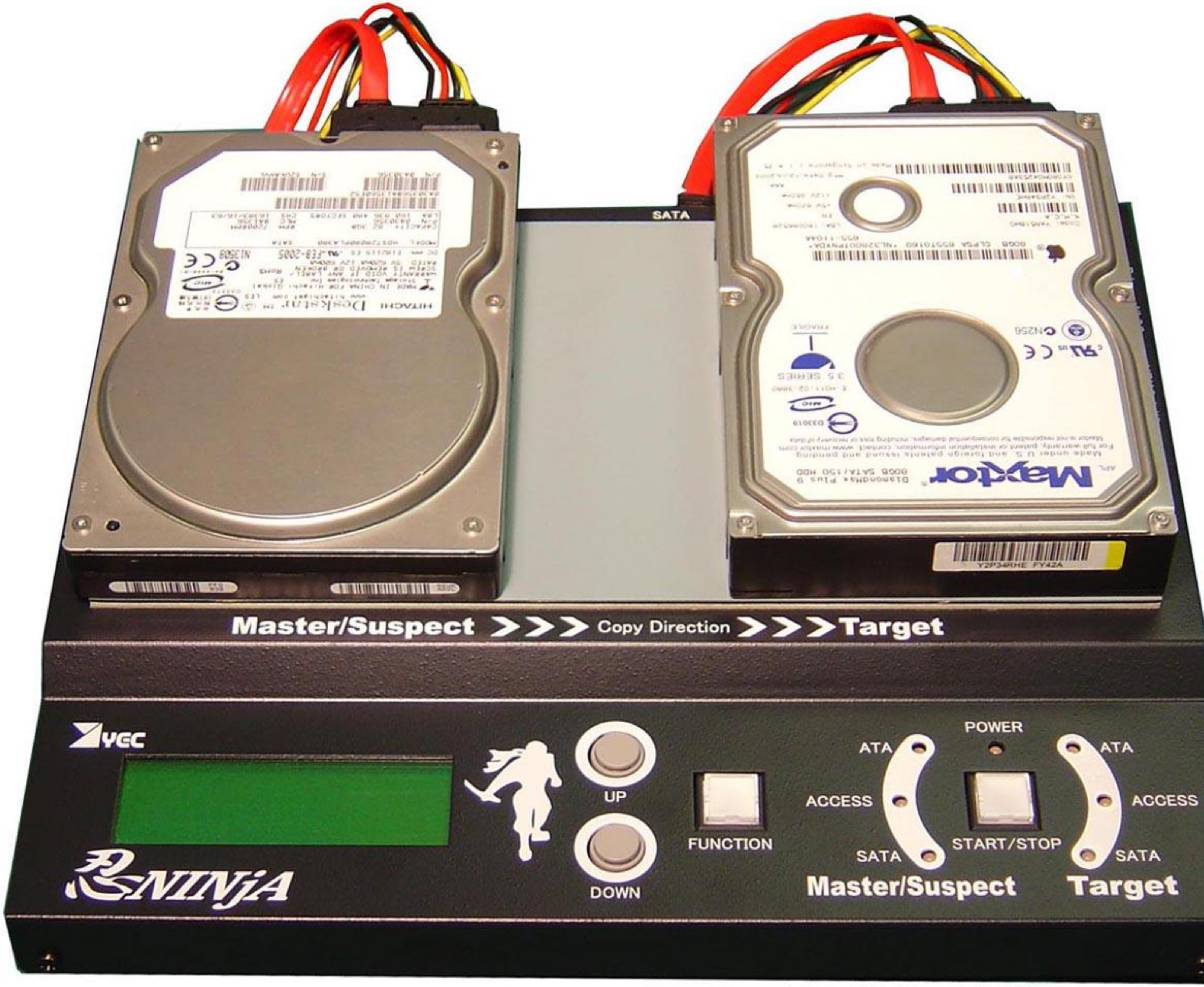
just xored with "RANDOM STRING"

Advanced
Solutions ©
Made in China
PX-1005-1337
780863 185779

PWR-UPS 770
Model APD-00133-770
RESET
OFF

Power Pwn & PwnPlug

- Wireless, Bluetooth, Ethernet, GSM
- internal storage
- stealth mode
- pre-loaded with offensive tools

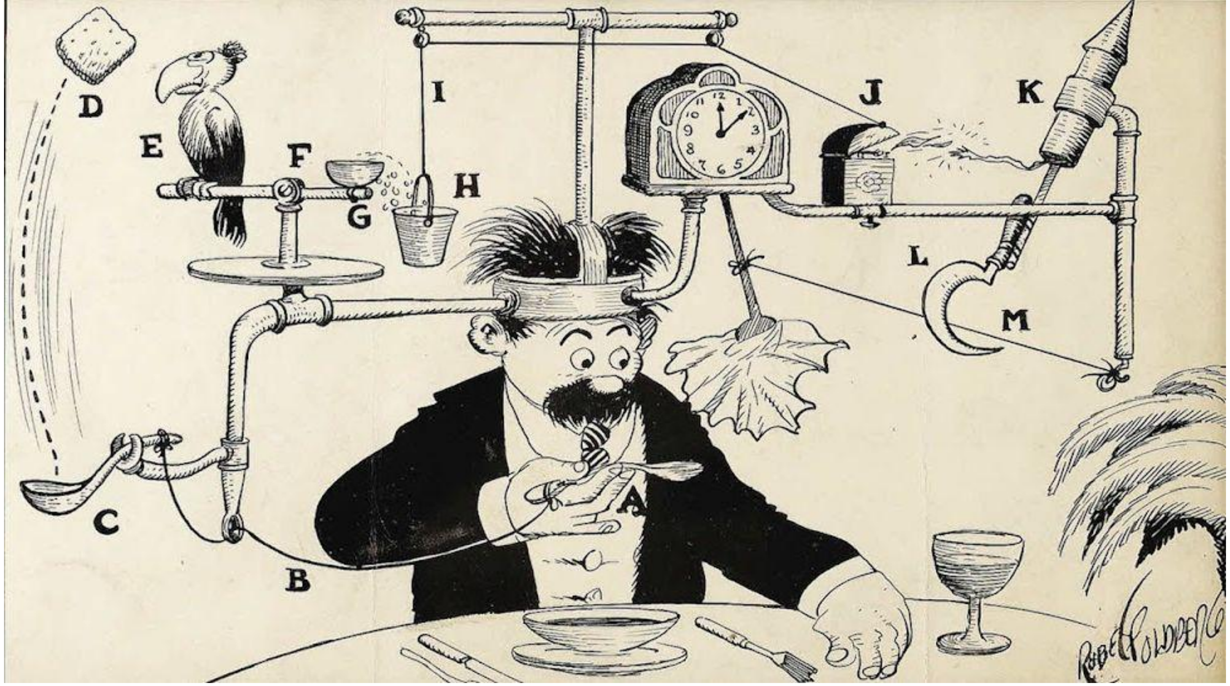

SATA
Maxtor
HITACHI Deskstar
Master/Suspect >>> Copy Direction >>> Target
YEC
NINjA
UP
DOWN
FUNCTION
POWER
ATA
ACCESS
SATA
START/STOP
ATA
ACCESS
SATA
Master/Suspect
Target

Removing advanced malware

1. re-flash bios
   - infecting BIOS is a reality
2. hardware wiping
   - encrypted & hidden FileSystem is a reality
3. re-install everything

Introduction

"hackers"?



D
E
F
G
H
I
J
K
L
M
A
B
C
RUBE GOLDBERG

↕

?

"hackers", for hackers

- explorer, inventor, ***finder***
- freedom, curiosity, experiment, technical
- use things in an unexpected way
  - get ***extraordinary*** results, out of normal things

"hackers", for others (media)

- system intruder
- illegal, malicious, thief, ***perpetrator***
- script kiddie, defacing, "Anonymous"

Why 2 definitions?

before

- a culture

→ intruders = experts

now

- a business

→ many 1-click tools exist

→ trivial to hack a weak system

→ *security researcher* instead of *hacker*

Agenda

Agenda

1. A hacking glossary
2. Why hacking?
3. Who are the actors?
4. What/how to hack?
5. A word on viruses

A hacking glossary

1. bug
2. vuln
    a. CVE
3. exploit
    a. 0-day
        i. 1-day
4. cyber weapon

- full/responsible disclosure

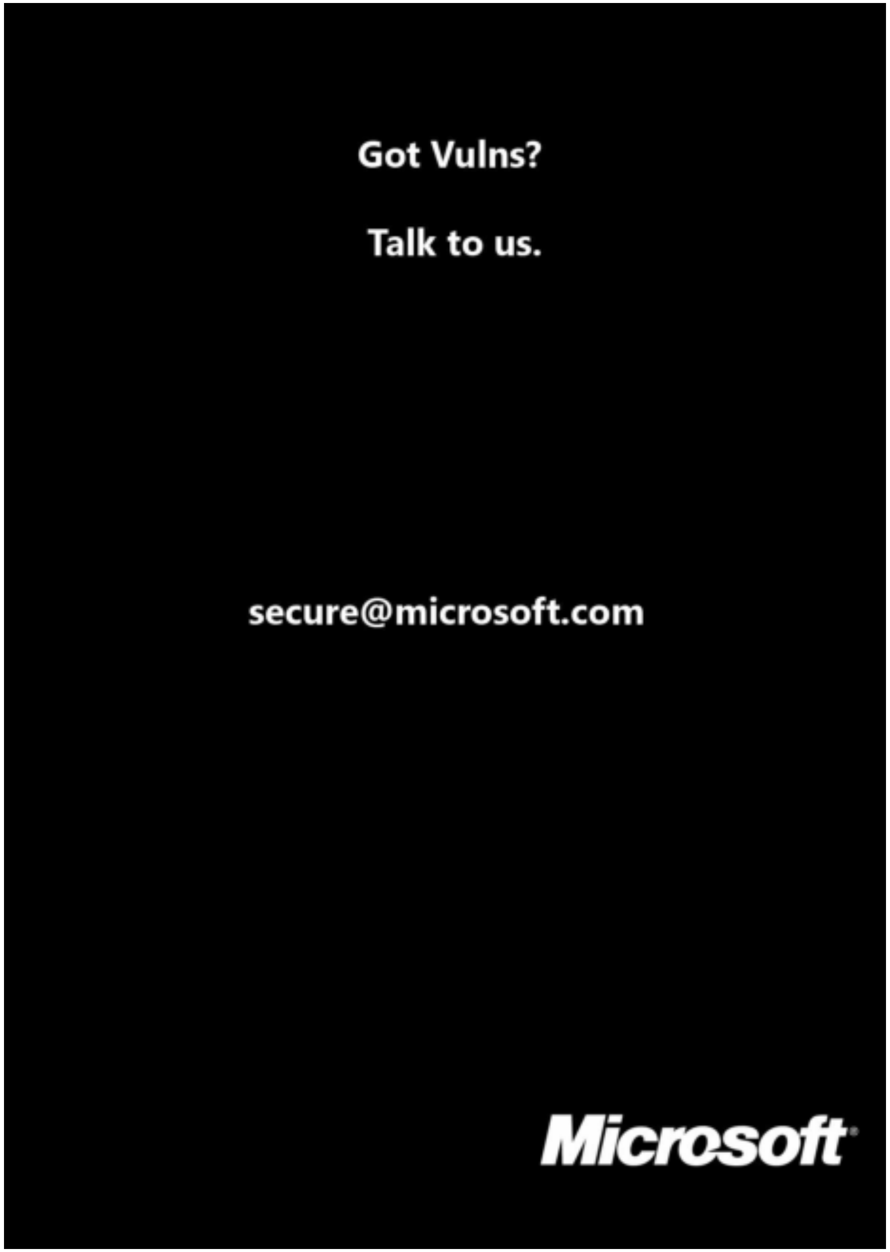
"bug"

- a problem in a software/hardware
  - 180 official bugs in Intel's i7
- an unwanted path of execution
- to be fixed?
  - maybe one day, maybe "WontFix"

"vulnerability" (*vuln*)

- a bug that creates some weakness
    - a security bug
- crash/hang/information leak

- ***NOT*** always an exploit
- a single vuln might be enough for a hack
- minor vulns can be combined



Got Vulns?

Talk to us.

secure@microsoft.com

Microsoft

ad published in "**H**ack ***I***n ***T***he ***B***ox magazine"

"***C***ommon ***V***ulnerabilities & ***E***xposures"

- a universal ID for a specific vuln
  - ex: CVE-2012-0217 = "Xen Escape"
- booked in advance
  - not all IDs are documented
- other companies have their own IDs
  - ex: Microsoft's MS12-042
- not all vulns have IDs

"exploit"

- using one or more vulnerabilities at your advantage, in a user-controllable way.
  - "it's like getting random pieces at IKEA, and try to make a piece of furniture out of it" Thomas Dullien
- it's hard!
  - exact configuration
    - OS/software version
  - escape sandbox
  - avoid compiler/system mitigations

Many vulnerabilities are ***not*** exploitable!

↕

Several ***innocent*** bugs might be combined into a fully-working ***exploit***!

"*P*roof *o*f *C*oncept"

- binary/source
- triggers the exploit
  - proves it's real
  - might not work reliably

"to pwn"

- to own, to take control, to defeat
- hacked/exploited = pwned = game over

"0-day"

- an exploit not publicly known yet
  - $5,000 - $600,000
  - ***I***n ***T***he ***W***ild
- no documentation or PoC

"1-day"

- exploit is now known
- likely not patched everywhere yet
- generate exploit
  - from before/after patching comparison
  - from PoCs
  - from write-ups

→ exploitation is ***much*** easier

PATCHING IS ***CRITICAL***!

removing/isolating ***obsolescence*** too!

"cyber weapon"

an exploit with a well built payload

(pseudo-hype word)

- stealth
  - anti-forensics
  - self-encryption to avoid memory/disk footprint
  - decrypts necessary parts only on final target

Full/responsible disclosure

report to everybody or the vendor only?

- give the vendor time to react
  - maybe the vendor will never patch, or sue you, leaving users vulnerable
- some vulns are known yet hidden for years
  - until exploited ITW

full disclosure is:

- bad for PR
- 'good' for security
  - force people to act

Why hacking?

For fun / fame!

- "because I can"
- cool/clever
  - dark magic
    - Super Mario World stack overflow via joypad!
- not necessary over-complex
  - we exploit kids' mind all the time ☺

For money!

it takes time and skill to generate an exploit.

- why for free?
  - try to feed your family with 'thank you'...
- bug bounties
  - pwn us, tell us how, get paid
  - Facebook hiring former security employees
- pen-testing
  - try to pwn us for XX days

Why buying exploits?

- which company/country wouldn't want to get secrets "magically"?
  a. buy exploit
  b. pwn your competitor
  c. profit

Why attacking me?

- customer informations
    a. bank accounts
- financial informations
- internal developments
    a. research project

0-day prices

$600K? remote iPhone (2nd JailbreakMe)

CanSecWest's *Pwn2own 2013*

- $100K Chrome + W7 / IE 10 + W8
- $75K IE 9 + W7
- $65K Safari + Mountain Lion
- $60K Firefox + W7
- plugins, IE9 + Win7
  - $70K Reader 11 / Flash
  - $20K Java

Google's *Pwnium 3* on ChromeOS

- $150K remote + device persistence
- $110K remote
  - $40k extra bonus

Bounties

- the original error bounty: Donald Knuth
  - $2.56 per error/mistake/suggestion
    - worth much more than the money!
- qmail
  - $500 per exploit, since 1997!
- Google, Mozilla, Avast, IDA, twitter, FB, github
  - slowly becoming mainstream

No money for you

'thank you' only ☹

- Microsoft, Nokia...

report for free, get lawyers' threats

- sadly too many vendors ☹

Who are the actors?

Independant researcher

- whitehat/'ethical hacker'
  - for bug bounties
- blackhat
  - to get it sold via a broker

the only difference?

- if vendors gets informed
  - which doesn't mean it will be patched

Private exploit sellers

- to any customer
    - Core, ZDI, Exodus, Immunity
        - many others, 'undercover' or not
- to governments
    - VUPEN

not sellers, but active private developers

- defense contractors
    - Northrop Grumman, Crystal Clear, EndGame

Open-source scene

- metasploit
- freedom to check for exploits ITW

What/how can you hack?

Hack what?

anything (that can execute code)!

- computers, browsers, processors
- (smart)phones (SIM unlock, jailbreak)
- printers, conference phones
- routers

- hotel room locks, cars, TV, camera
- tamagotchi, calculator, knitting machine, toys
- SCADA, Step 7
- keyboard, network card, floppy drive

How is it possible?

- error is human

- nobody controls the whole process anymore
  - CPUs and OSes are documented
  - manufacturers want developers to use their product
  - 3rd parties APIs and libraries everywhere
- everything gets more complex
  - increasing attack surface
    - more applications, more libraries, more protocols
    - web browser: CSS 3D, WebGL, MathML

How do you find vulnerabilities?

- pure accident
  - "it just crashed"
- happy accident
  - unexpected crash while researching a topic
- monitor official sources/bug trackers
- (smart) bruteforcing
  - fuzzing, gathering crash info
  - a silent crash might do the trick
- analysis
  - disassembly (very time consuming)

Methodology

"it's like reviewing a paper: just look for errors"

"if you rely on public tools or approach,
you will limit yourself like everyone else before"

Notable vulnerabilities

Pentium's *LOCK CMPXCHG8B*

- computer crash in one instruction

Tavis Ormandy's *KiRaiseAssertion*

- Windows crash in 2 instructions
  - patched in one instruction

my own example

- researching on PE. accidental BSOD

Why turning vulns into exploit?

people don't move until they're pwned

- "I personally consider security bugs to be just 'normal bugs' " Linus Torvald
- Oracle: critical vuln known for months until exploited for malware

exploit = vulns + control + defeating mitigations!

(+ anti-forensics if weaponized)

Notable exploits

- Sergei Golubchik's MySQL CVE-2012-2122
  - keep knocking until (admin) door wide open
- Sergey Glazunov's Chrome Pwnium
  - 14 chained vulnerabilities
    - including downgrading privileges
  - $60K
- Tavis Ormandy's CVE-2010-0232
  - 17 year old, all 32b NT versions affected

Exploit effects

parameter checking

- sql injection (blind)
  - customer/banking information?
  - add malware contents to websites
- browser vulnerabilities
  - bypass authentication, steal token, exfiltrate files

foreign code execution

- download malware
- privilege escalation
- host escape

Mitigations

- separation
  - process: sandbox
  - network
- predictability
  - OS randomization
  - configuration randomization (difficult)
  - ~~hardcoded passwords~~

Software targets

- the OS itself

most common software

- ***Java***
- PDF
- Flash
- Office

anything else?

- lowest hanging fruit
  - any installed software increases the attack surface

Why is Java the most targeted?

- Oracle is like Adobe 5 years ago
  - no patch until public
  - started hiring known hackers only recently
- Java exploitation is (very) easy
  - hardly no mitigations
    - no mitigations at OS level
  - just a missing 'if (access==granted)' somewhere
- it's a reality
  - a "Java every-day"
    - last 0-day ***really*** went unnoticed
  - ***J***ust ***A***nother ***V***ulnerability ***A***nnouncement
  - hacked 4 times at Pwn2Own

How do you hack a company ? (1/3)

- gather information
  - search credentials via google
  - scan network
  - hack wifi
  - visit and plug your notebook
  - buy a used laptop/hard disk on e-bay

How do you hack a company ? (2/3)

- exploit information
  - any obsolete software?
    - ex: PC Anywhere
  - any internal software?
  - anyone vulnerable?
    - buy, bribe, convince
    - take hostage ☺
- exploit humanity
  - drop USB keys
  - send targeted e-mails
    - most companies have clueless employees
    - the worst the better ☺
  - waterhole attack

How do you hack a company ? (3/3)

- attack
  - use known attack
    - NMap, Nessus, AutoPwn...
  - develop your own attack
  - buy/trade a 0-day
    - "hackers' standard currency"
  - get in. elevate privileges. get further.
- stay in, stay stealth
  - in the printer,...?
- exfiltrate information
  - random copy metadata on USB sticks
  - visit again

Advanced physical attacks

"evil maid attack"

- bios/iPXE (Brossard's Rakshasa)
- boot from other drive (Bania's Kon-Boot)
- firewire/thunderbolt access (Inception)
    - bypass password + elevates privilege
- network card (Delugre)
- keyboard controller (Gazet's Sticky Finger)

Physical access = pwned

Commercial solutions failure (1/2)

bound to fail against ***targeted*** attacks!

- predictability
  - everybody's copy is identical
- limitations
  - can't be exhaustive
    - compared like washing powders on scanning speed.
- time
  - modify binary until not detected
  - use VirusTotal to check
    - or black market equivalent to avoid sharing

Commercial solutions failure (2/2)

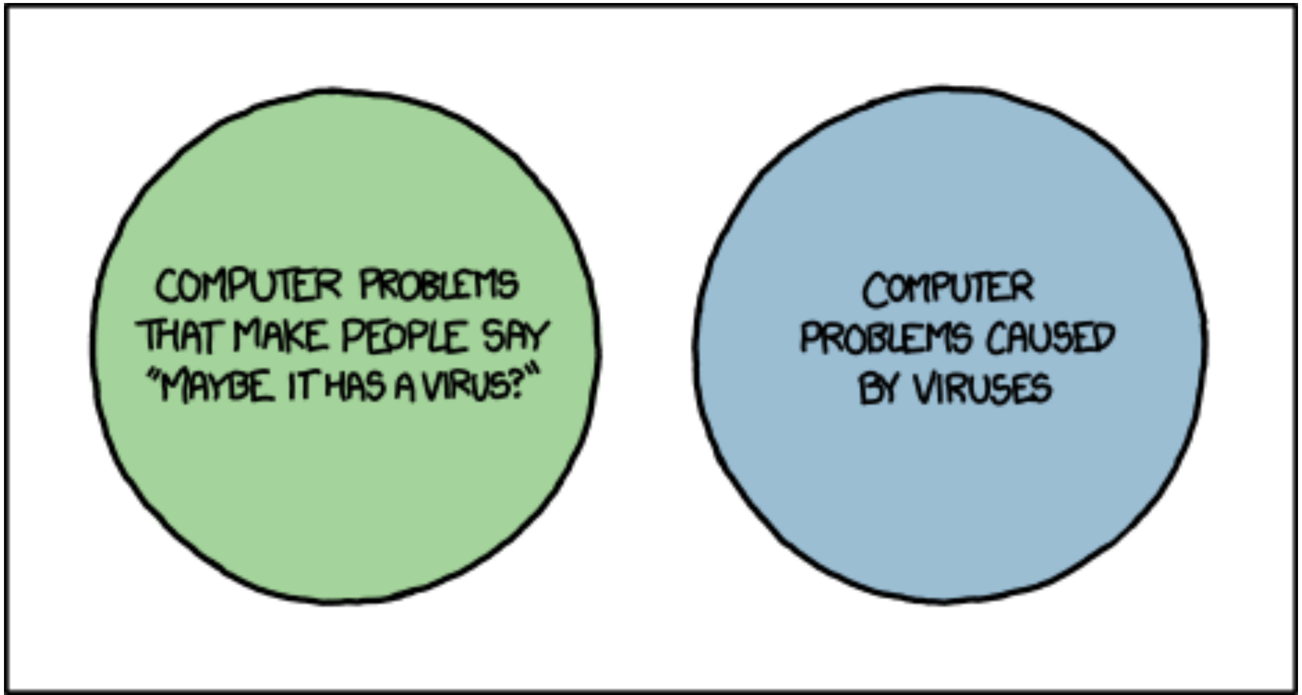
might ***increase*** the attack surface!

- deeply integrated into the OS
  - present in each process
- remote connection
- trusted

→ useable as a trampoline for attack

- Tavis Ormandy's Sophail
  - "installing Sophos Antivirus exposes machines to considerable risk"
- Kasperky's remote DoS (March 2013)

A word on viruses


COMPUTER PROBLEMS THAT MAKE PEOPLE SAY "MAYBE IT HAS A VIRUS?"
COMPUTER PROBLEMS CAUSED BY VIRUSES

Viruses (virii) glossary

how they spread

1. trojan
2. worm
3. infector
4. rootkit
   - bootkit

what they do

1. ransomware
2. fakeAV
3. infostealer
4. zombie (→ botnet)

"virus" (malware)

- malware for professional
  - virus for others
- generic name, no implication

"trojan [horse]"

- pretends to be clean
- contains ill-intentioned greek soldiers

1. hack a known open-source site
2. backdoor binaries

"worm"

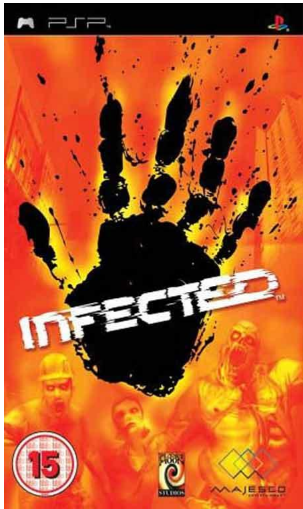
- just replicates to survive
  - network, usb key, 0-days, mail, p2p
  - standard modern feature

Slammer

- one single packet containing
  1. packet infos
  2. MS02-039 server exploitation
     - yet patched 6 months before!
  3. replication

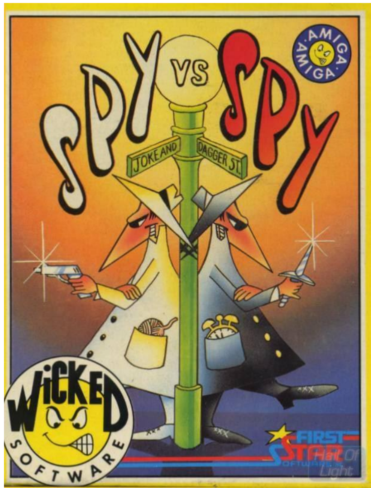
"infectors"

- adds itself to target to spread
  - may be hard/impossible to repair
  - file or disk infectors
- true definition of a virus?
  - not trendy anymore
  - technically advanced
- known file is not innocent anymore
  - tricky for compiling environments



"infostealer/spyware"

- steals (banking/gaming/login) information



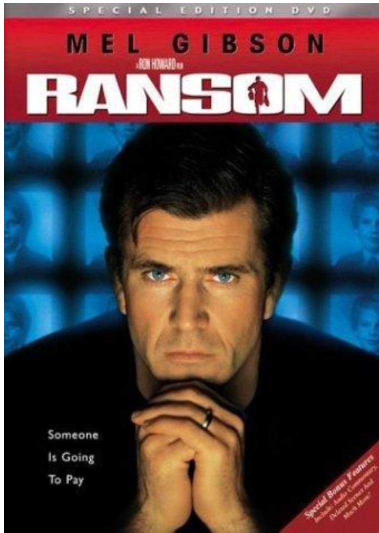
banking infostealers technics

- login → keylogger
- virtual keypad → take screenshot
- Tan → hook display / fake page
- mTan
    - Bochum's Nokia
    - smartphone → infect smartphone

- chipTan → fake transaction message
        - there's no patch for human stupidity

"ransomware"

- pay to unlock your system
- either
  - prevent booting
    - usually (very) easy
  - encrypt your personal documents
    - can be hard
    - or impossible if buggy



"rootkit"

- hider, cloaker
  - used by Sony, Blizzard,...
- just a component to hide the main part

"zombie"

- a device (most likely PC)
- pwned by a generic malware

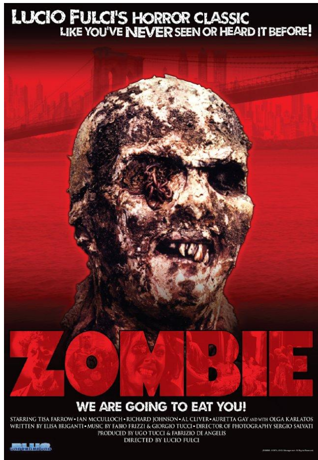
"botnet"

a set of zombies connected together

typically in a P2P way.

"sinkholing"

exploit a botnet to it take over


LUCIO FULCI'S HORROR CLASSIC
LIKE YOU'VE NEVER SEEN OR HEARD IT BEFORE!
ZOMBIE
WE ARE GOING TO EAT YOU!
STARRING TISA FARROW • IAN McCULLOCH • RICHARD JOHNSON • AL CLIVER • AURETTA GAY AND WITH OLGA KARLATOS
WRITTEN BY ELISA BRIGANTI • MUSIC BY FABIO FRIZZI & GIORGIO TUCCI • DIRECTOR OF PHOTOGRAPHY SERGIO SALVATI
PRODUCED BY UGO TUCCI & FABRIZIO DE ANGELIS
DIRECTED BY LUCIO FULCI

standard malware

- a bit of everything
- just rent services
  - binary obfuscation
  - credit card checking
  - captcha solvers
  - hosting
- uses of a botnet
  - spying
  - distributed parallel filestorage (child pornography)
  - anonymous proxy
  - spam, DDOS
  - click ads
  - bitcoin mining

"exploit kit"

- ready-made malware infection kit
- complete infection and maintenance software
- from a single script on a page to full remote management of the botnet

easy 0-days (java/pdf/html/flash) → download

"bootkit"

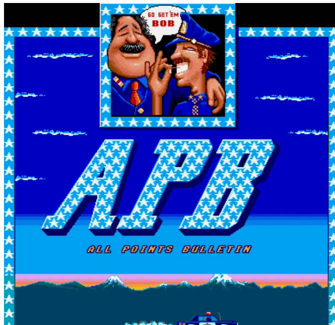
- boot infector + on-the-fly patcher
- the OS is modified during loading
  - no file footprint
- originally used to install rootkit
- bootkit-based tools
  - Piotr Bania's Kon-Boot
    - bypass log-in+elevate rights
  - Saferbytes x86 memory bootkit
    - enable more memory usage

"Advanced Persistant Threat"

- hype
  - created by US AirForce in 2005
    - public for operation Aurora, 3/2010
  - you're just pwned, but your company is famous
- targeted attack? not even always

StuxNet, Flame = awesome

most others are just 'standard'



resilient yet ITW

- bootkit + encrypted FS at the end of the drive
- no visible file from the system
    - yet updateable
- resist formatting

state-sponsorised spyware

- a reality
    - Finfisher
    - Bundestrojan
    - got a job offer for that!
- stealth
    - low footprint (Duqu)
    - no replication
- recent laws make it possible
    - public french regrets
        - for ***not*** having one!

generic vs targeted

Generic:quick and efficient, avoid AV

- malicious from the start
- evades AVs, infect

Targeted: stealth

- look 100% clean
  - even at 2nd look (integrate in existing software)
  - does nothing on non-target
    - might be impossible to get it working
  - don't disclose any information

Conclusion

security is hard!

secure = powered off

not good for business ☹

"secure"

=

resisting to attack

**the more predictable,
the more manageable...**

...and the more hackable!

Face reality

error is human

software have bugs

hardware have bugs

→ you **will** be pwned, if someone **really** wants

- but for how long?
  - kill the **time** factor
- and to what extend?
  - kill the **predictability** factor
- anything can be a target
  - any minor hack will lead to "X has been hacked"

Thank YOU!

Questions?

@angealbertini

✉ ange@corkami.com