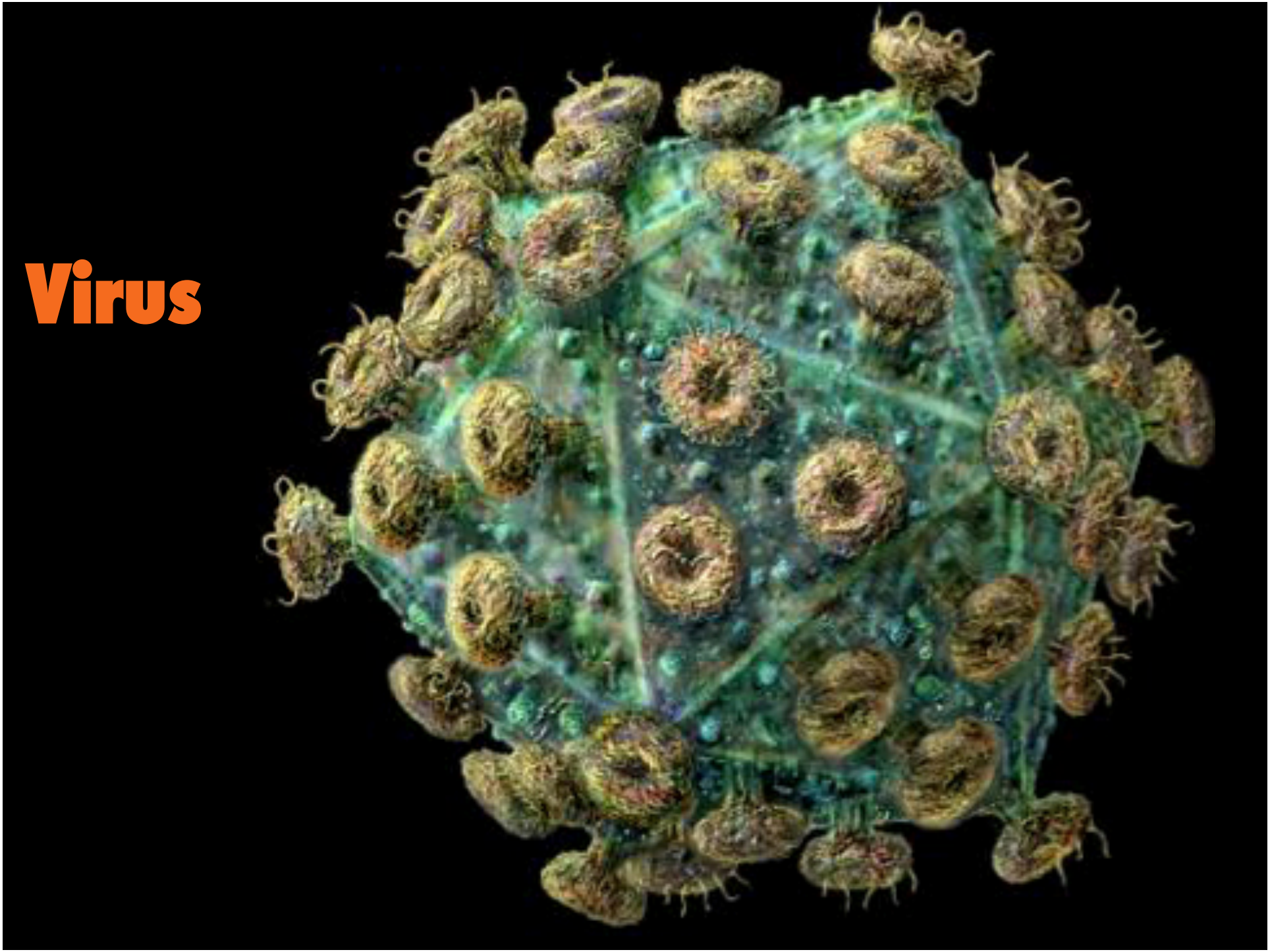
Malware Detection and Evasion

Virus



Virus

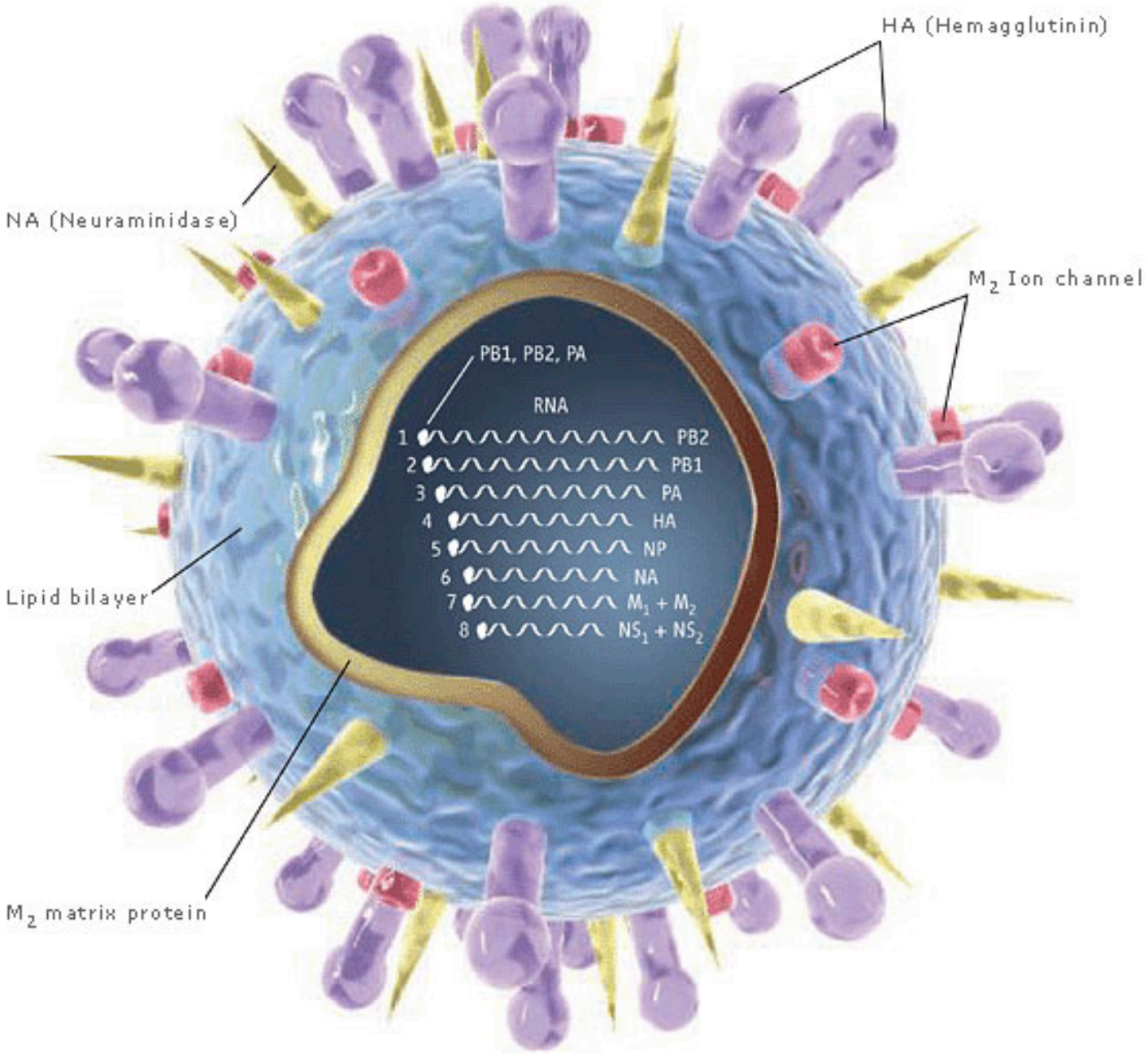


Illustration: Chris Bickel/Science. Reprinted with permission from Science Vol. 312, page 380 (21 April 2006) © 2006 by AAAS

Basic AV Signatures

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

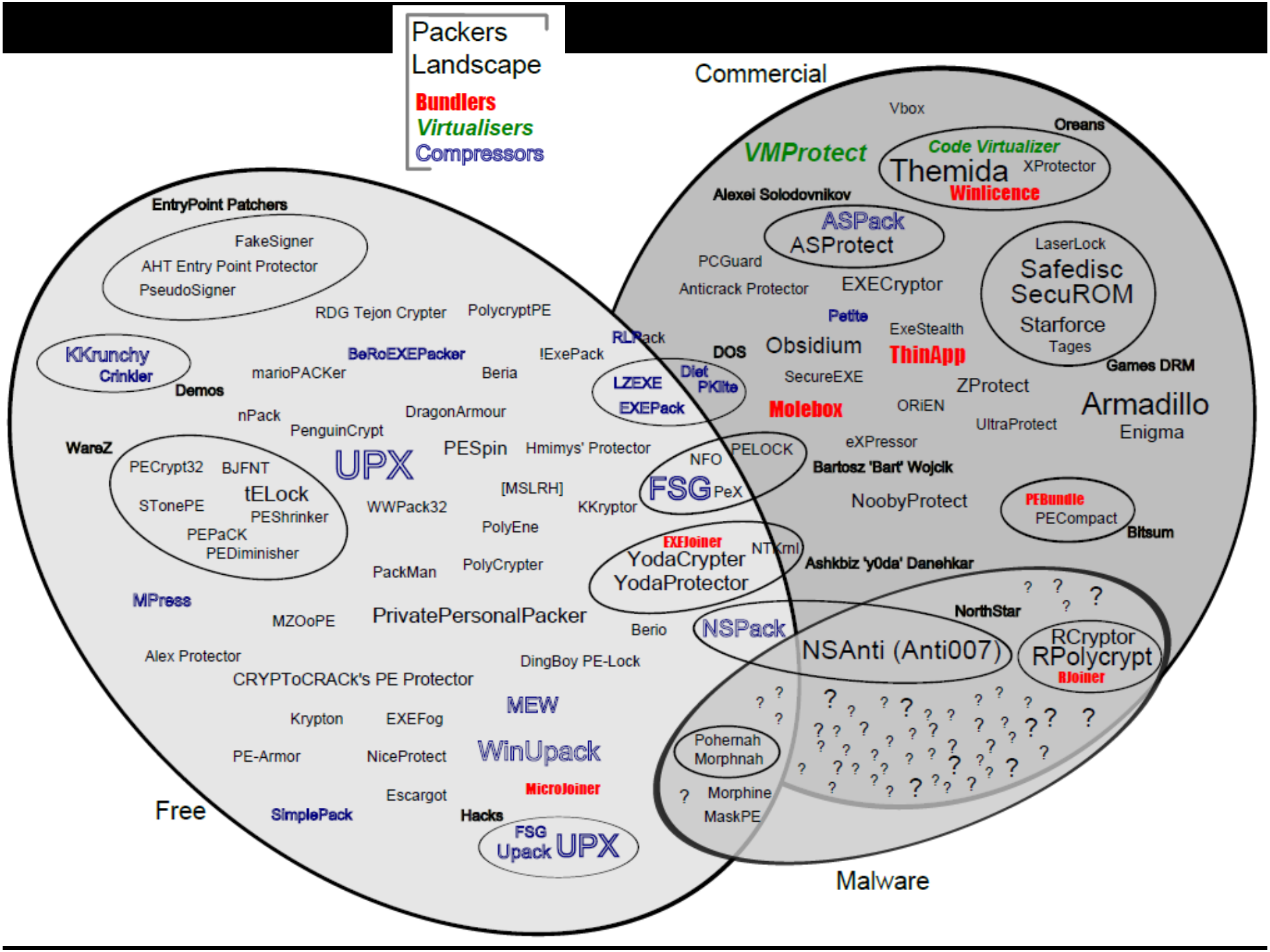
Also: regex, operators, etc.

Virus Concealment

- Undermining the AV
- X-morphism
  - Poly-morphism
  - Meta-morphism

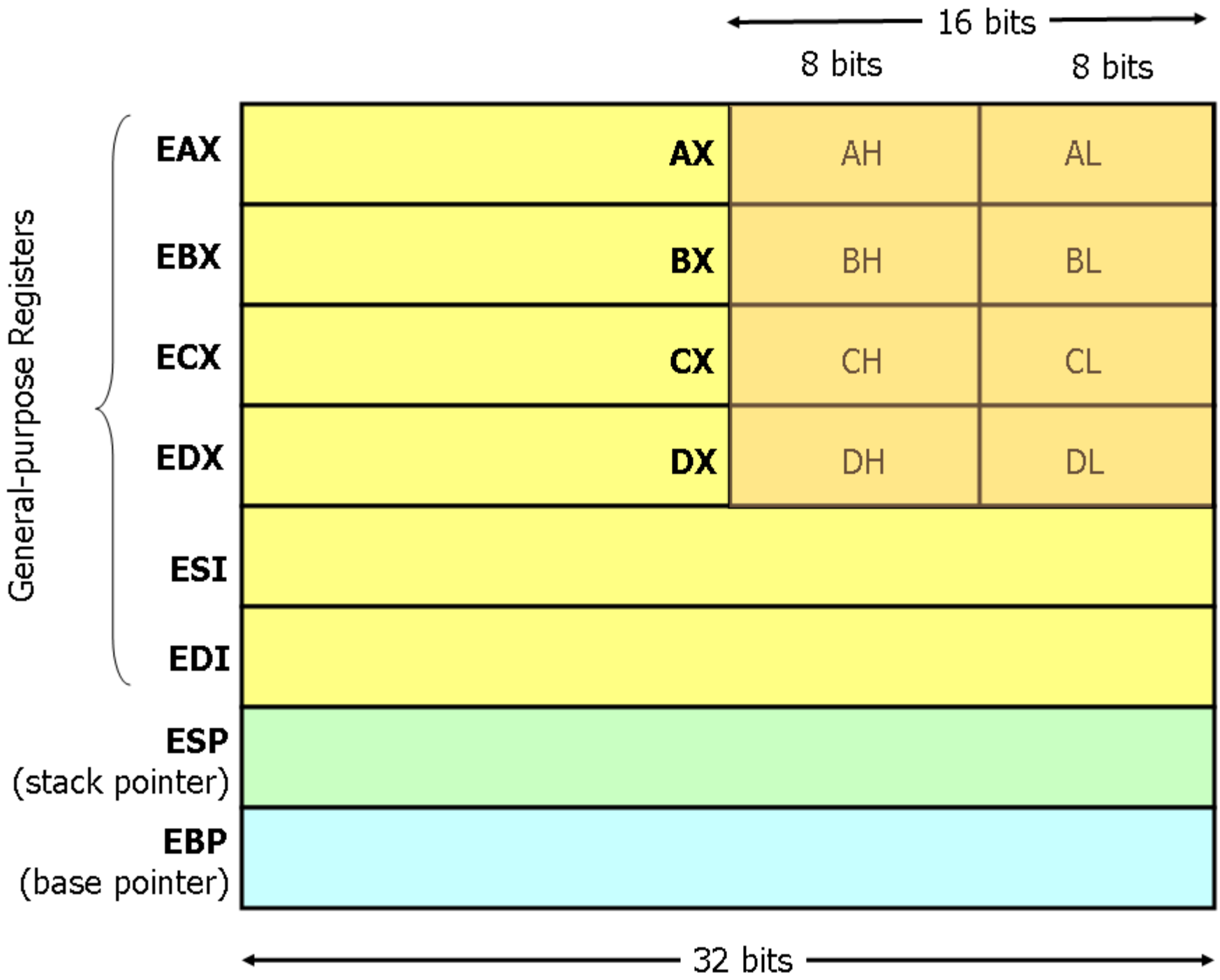
Virus Concealment

- Poly/Meta-morphism
  - Change form upon replication
  - Keep function
- Packers: Encryption + Compression
  - Each iteration: different key


Packers Landscape
Bundlers
Virtualisers
Compressors
Commercial
Free
Malware
Vbox
Oreans
VMProtect
Code Virtualizer
Themida
XProtector
Winlicence
Alexei Solodovnikov
ASPack
ASProtect
PCGuard
Anticrack Protector
EXECryptor
LaserLock
Safedisc
SecuROM
Starforce
Tages
Games DRM
Petite
ExeStealth
ThinApp
DOS
Obsidium
SecureEXE
ZProtect
ORiEN
Armadillo
Enigma
UltraProtect
Molebox
eXPressor
Bartosz 'Bart' Wojcik
PELOCK
NFO
FSG
PeX
NoobyProtect
PEBundle
PECompact
Bitsum
EXEJoiner
NTKrnl
YodaCrypter
YodaProtector
Ashkbiz 'y0da' Danehkar
NorthStar
NSPack
NSAnti (Anti007)
RCryptor
RPolycrypt
RJoiner
Pohernah
Morphnah
Morphine
MaskPE
EntryPoint Patchers
FakeSigner
AHT Entry Point Protector
PseudoSigner
RDG Tejon Crypter
PolycryptPE
KKrunchy
Crinkler
Demos
BeRoEXEPacker
marioPACKer
!ExePack
Beria
RLPack
LZEXE
Diet
PKlite
EXEPack
nPack
DragonArmour
PenguinCrypt
WareZ
PESpin
Hmimys' Protector
UPX
PECrypt32
BJFNT
tELock
STonePE
PEShrinker
PEPaCK
PEDiminisher
WWPack32
[MSLRH]
KKryptor
PolyEne
PackMan
PolyCrypter
MPress
MZOoPE
PrivatePersonalPacker
Berio
Alex Protector
DingBoy PE-Lock
CRYPToCRACk's PE Protector
MEW
Krypton
EXEFog
PE-Armor
NiceProtect
WinUpack
Escargot
MicroJoiner
SimplePack
Hacks
FSG
Upack
UPX

Metamorphism Examples

- Win32/Ghost
  - Reorder the subroutines
  - 10 subroutines
    - How many possible variants?
- Detection?


16 bits
8 bits
8 bits
General-purpose Registers
EAX
AX
AH
AL
EBX
BX
BH
BL
ECX
CX
CH
CL
EDX
DX
DH
DL
ESI
EDI
ESP
(stack pointer)
EBP
(base pointer)
32 bits

December, 1998 – Win95/Regswap*

```
5A                  pop edx
BF04000000          mov edi,0004h
8BF5                mov esi,ebp
B80C000000          mov eax,000Ch
81C288000000        add edx,0088h
8B1A                mov ebx,[edx]
899C8618110000      mov [esi+eax*4+00001118],ebx

58                  pop eax
BB04000000          mov ebx,0004h
8BD5                mov edx,ebp
BF0C000000          mov edi,000Ch
81C088000000        add eax,0088h
8B30                mov esi,[eax]
89B4BA18110000      mov [edx+edi*4+00001118],esi
```

Unchanged code underlined, so wildcard-string detection should still spot (e.g. 81****181100008B**…).

* does what?

July, 2000 – Win32/Evol

Uses machine code instruction equivalences.
Also inserts garbage.

a. An early generation:

```
C7060F000055      mov dword ptr [esi],5500000Fh
C746048BEC5151    mov dword ptr [esi+0004],5151EC8Bh
```

b. And one of its later generations:

```
BF0F000055        mov edi,5500000Fh
893E              mov [esi],edi
5F                pop edi
52                push edx
B640              mov dh,40
BA8BEC5151        mov edx,5151EC8Bh
53                push ebx
8BDA              mov ebx,edx
895E04            mov [esi+0004],ebx
```

- Magic DWORDS (e.g. 5500000Fh) changed also
  - Wild-card string detection fails after 3rd generation.

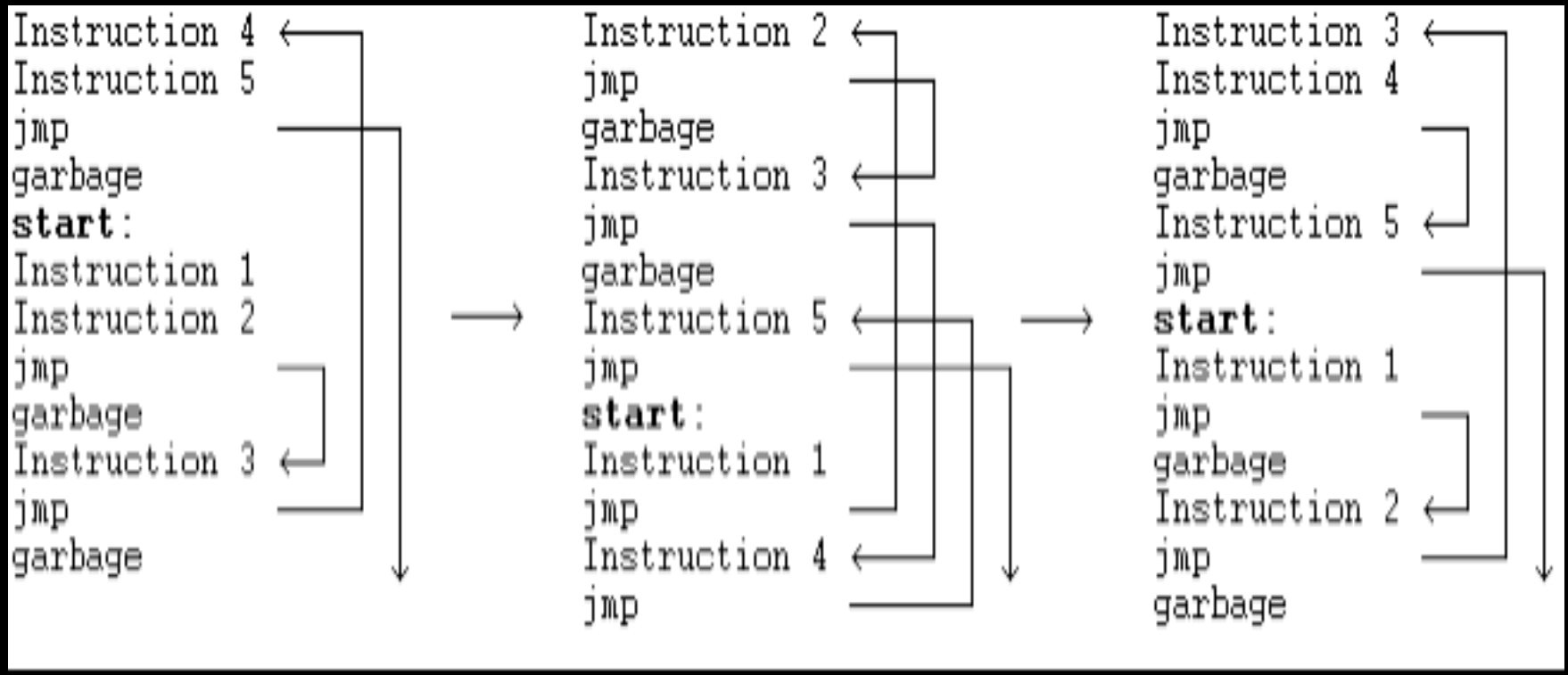
September, 2000 – Win95/Zperm

- Inserts garbage instructions
- Replaces single instructions with equivalent ones.

`xor eax, eax` → `sub eax, eax`

- Reorders jump instructions
- Search string detection will not work.
- Permutations are n!
  - Where n = number of core virus code instructions.

Zperm Example



The End

PCs vs. UNIX

- Why were PCs more vulnerable to viruses?

- Hence

Undermining AV

- AV
  - TSR: Terminate-Stay-Resident
  - Modified interrupts
- Undermining AV
  - Get underneath the AV's interrupts

Virus Concealment

- Code changes
  - Basic: Intersperse instructions with NO-Ops
  - Intermediate: Reorder instructions that are not dependent or exchange registers
  - Intermediate: Use equivalent operations
  - Advanced: Redirection of data access through pointers, strange jumps, etc.

Class Business

- Exam 1
  - Monday 10/17, in class
  - 80 min.
  - 1 page of notes, 2-sided
    - Any font size
- Grades on Moodle

Lab 2

- Appended virus
- Tricky
  - (partial credit)
- Lab Timings

Virus Signatures

- Virus cannot be completely invisible
  - Stored somewhere in the system
  - Need to actively "play" in the system
  - Have patterns
- Virus scanner: looking for virus signatures

First Generation

- Simple scanners
  - Storage: file size, file checksum
  - Bit patterns
- Limitations?

Advanced Defenses

- Heuristic Detection
- System-level Defenses
- Malware Analysis

Heuristic Detection

- Watching for possibly malicious strings
  - Any examples?
- Host-based IDS
  - Statistical Methods

Integrity Checking

- Tripwire
  - Perhaps just start/end of file
  - Must keep the DB somewhere
    - Access control can help
  - Targeted: only commonly mod'd files
- Bait files
  - If modified, likely malware

System-level Defense

- Behavior-blocking software (book)
- Clear distinction between data and executable
  - Virus must write to program
    - Write only allowed to data
  - Must execute to spread/act
    - Data not allowed to execute
  - Auditable action required to change data to executable

Malware Analysis

- Complex systems approaching the PVC:
  - variable/memory emulator
  - parser
  - flow analyzer
  - disassembler/emulator
  - weight-based and/or rule based system
- Not real-time
  - Part of the Digital Immune System (book)

Emulation

- Sandbox
- Emulate initial program activity
  - Does it modify it's code?
    - Does it eventually look like a known virus?
  - Does it search for executable files?