THE A
AND THE P
OF THE T

#APT
#APT
#APT
#APT
#APwot

ADVANCED
[ədˈvɑːn(t)st]

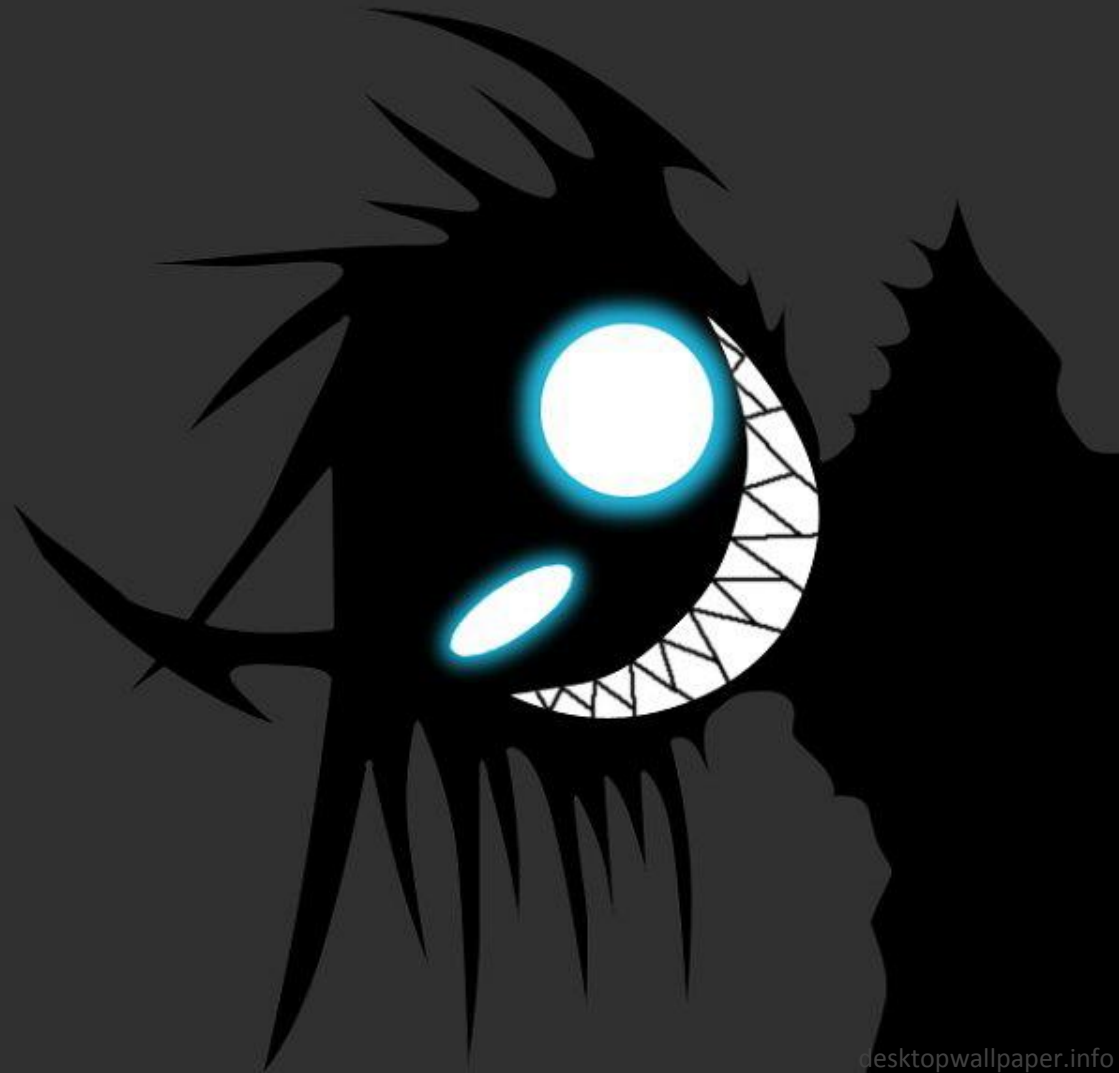
we don‘t
understand it

we detected it
too late

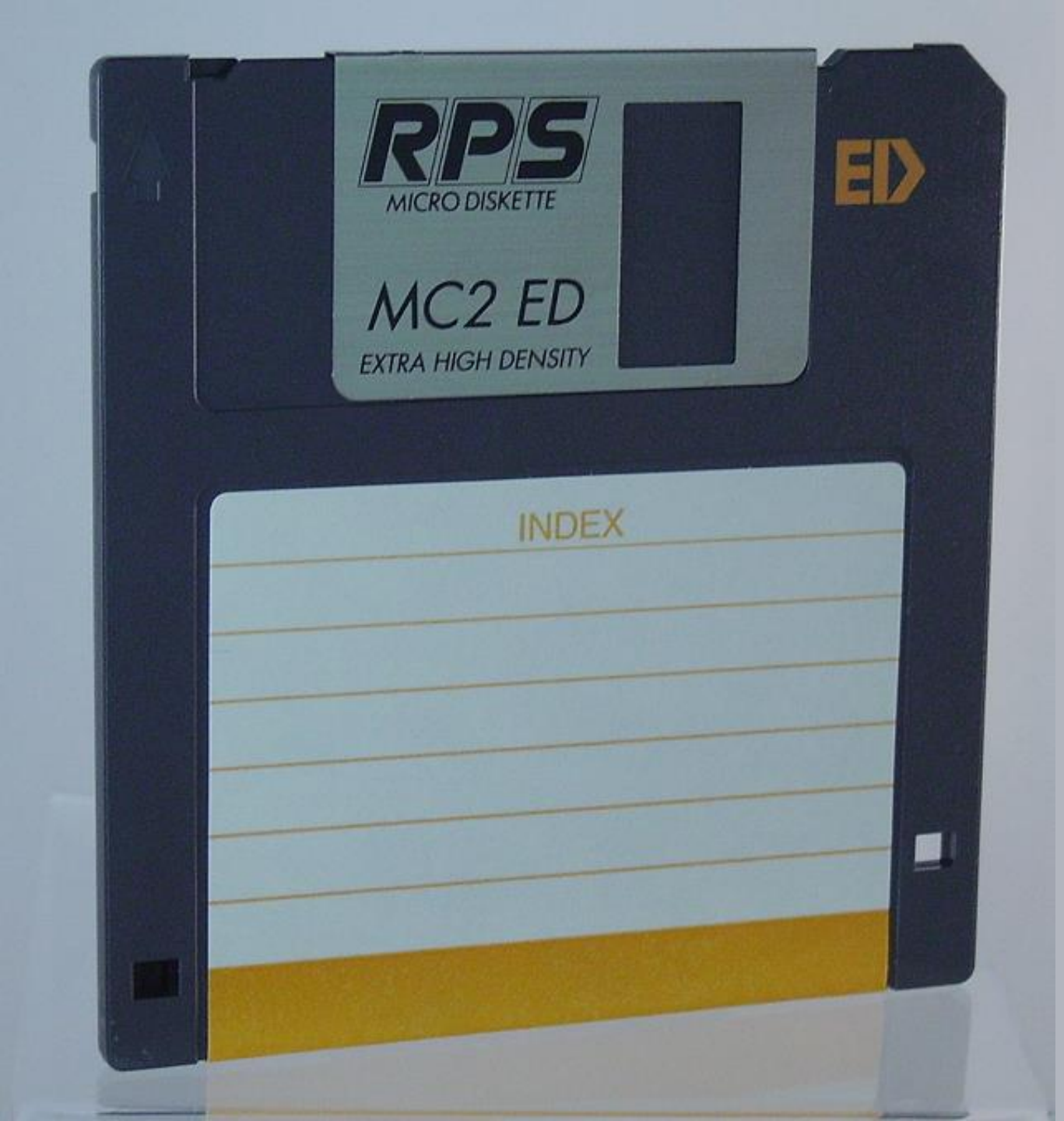
PERSISTENT
[pəˈsɪstənt]

MARION MARSCHALEK

@pinkflawd
marion@cyphort.com



CYPHORT™



A THREAT DETECTION HISTORY

Source:
obsoletemedia.org

THINGS HAVE CHANGED

Virus

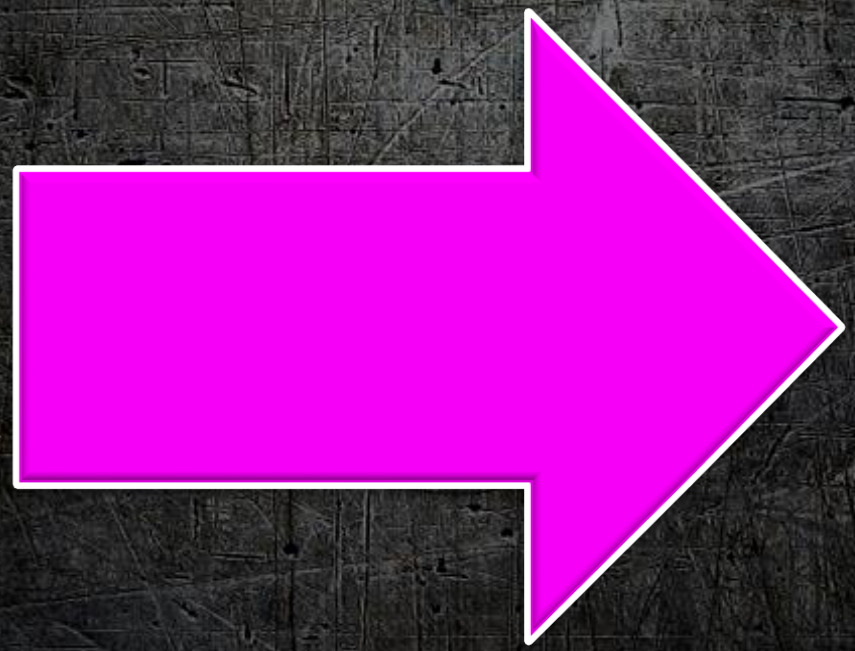
Detection

Signature

Product

Computer

Server



Threat

Prevention

Definition

Solution

Endpoint

Cloud

CYPHORT

Checksums

Byte Patterns

Behavior Patterns

Static / Dynamic Heuristics

Whitelisting

Network Streams

Cloud Protection

2014

..and many, many more!

CYPHORT

BOILS DOWN TO

The binary is known.

The binary is recognized.

The behavior of the binary is recognized.

CYPHORT

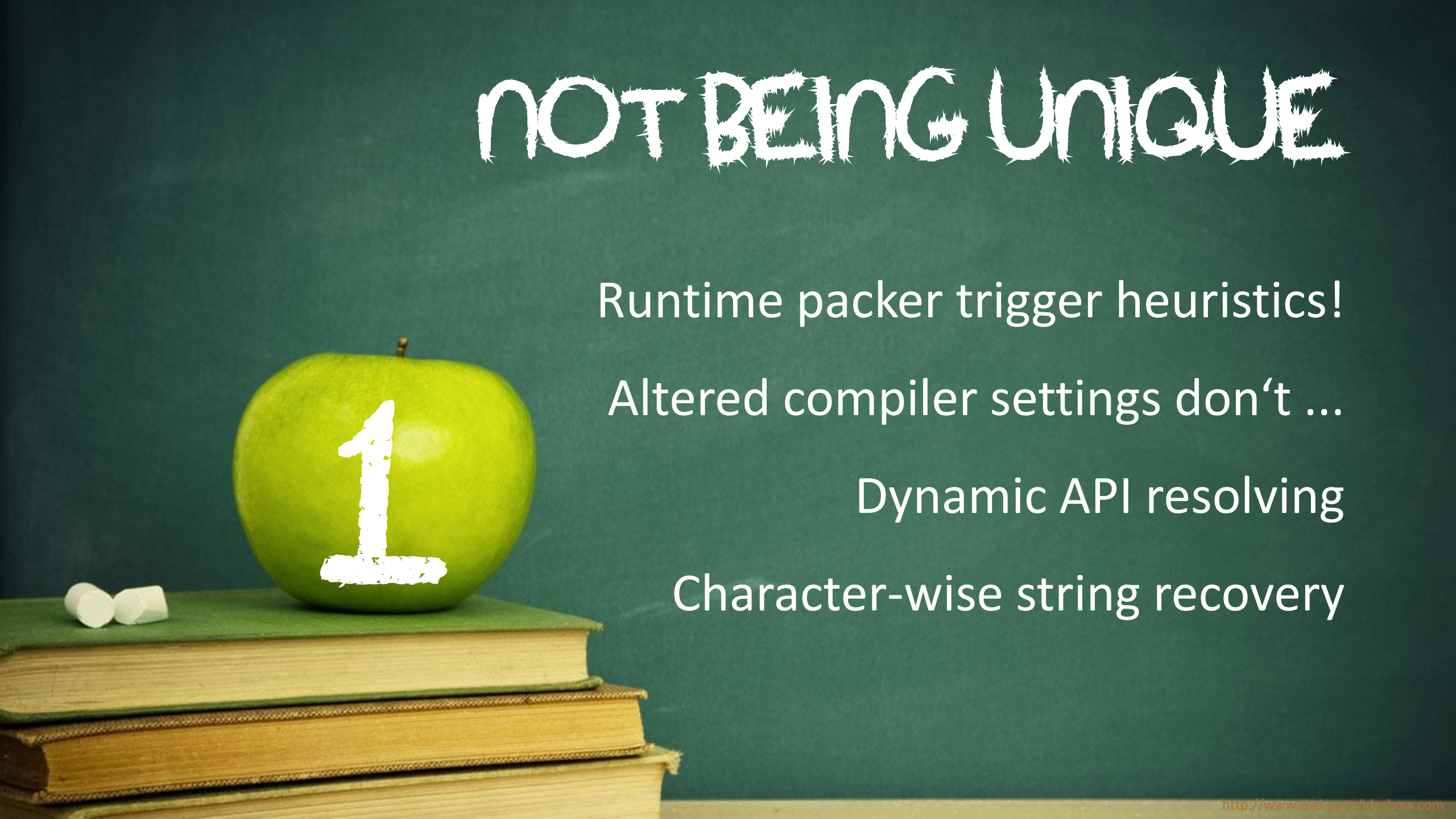
BOILS DOWN TO

KNOWLEDGE BASED THREAT DETECTION

PREDICTIVE THREAT DETECTION

CYPHORT

NOT BEING UNIQUE



Runtime packer trigger heuristics!

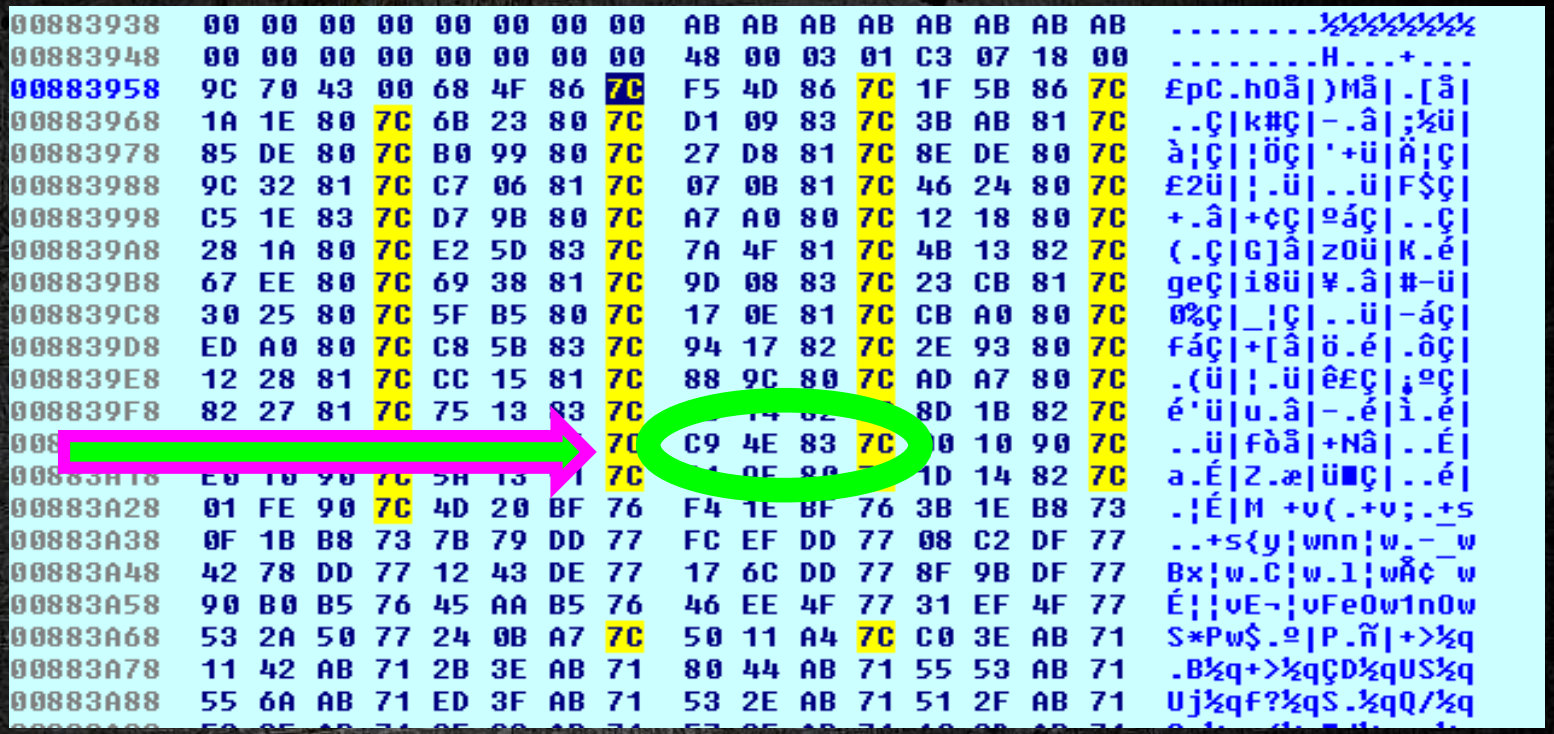
Altered compiler settings don‘t ...

Dynamic API resolving

Character-wise string recovery

jump table FTW

FindNextFileA



```
00883938  00 00 00 00 00 00 00 00  AB AB AB AB AB AB AB AB  ........½½½½½½½½
00883948  00 00 00 00 00 00 00 00  48 00 03 01 C3 07 18 00  ........H...+...
00883958  9C 70 43 00 68 4F 86 7C  F5 4D 86 7C 1F 5B 86 7C  £pC.hOå|)Må|.[å|
00883968  1A 1E 80 7C 6B 23 80 7C  D1 09 83 7C 3B AB 81 7C  ..Ç|k#Ç|-.â|;½ü|
00883978  85 DE 80 7C B0 99 80 7C  27 D8 81 7C 8E DE 80 7C  à¦Ç|¦ÖÇ|'+ü|Ä¦Ç|
00883988  9C 32 81 7C C7 06 81 7C  07 0B 81 7C 46 24 80 7C  £2ü|¦.ü|..ü|F$Ç|
00883998  C5 1E 83 7C D7 9B 80 7C  A7 A0 80 7C 12 18 80 7C  +.â|+¢Ç|ºáÇ|..Ç|
008839A8  28 1A 80 7C E2 5D 83 7C  7A 4F 81 7C 4B 13 82 7C  (.Ç|G]â|zOü|K.é|
008839B8  67 EE 80 7C 69 38 81 7C  9D 08 83 7C 23 CB 81 7C  geÇ|i8ü|¥.â|#-ü|
008839C8  30 25 80 7C 5F B5 80 7C  17 0E 81 7C CB A0 80 7C  0%Ç|_¦Ç|..ü|-áÇ|
008839D8  ED A0 80 7C C8 5B 83 7C  94 17 82 7C 2E 93 80 7C  fáÇ|+[â|ö.é|.ôÇ|
008839E8  12 28 81 7C CC 15 81 7C  88 9C 80 7C AD A7 80 7C  .(ü|¦.ü|êÉÇ|¡ºÇ|
008839F8  82 27 81 7C 75 13 83 7C  [illegible]  8D 1B 82 7C  é'ü|u.â|-.é|ì.é|
00883A08  [illegible]  7C C9 4E 83 7C  [illegible]  10 90 7C  ..ü|fòâ|+Nâ|..É|
00883A18  [illegible]  7C [illegible]  1D 14 82 7C  a.É|Z.æ|ü■Ç|..é|
00883A28  01 FE 90 7C 4D 20 BF 76  F4 1E BF 76 3B 1E B8 73  .¦É|M +v(.+v;.+s
00883A38  0F 1B B8 73 7B 79 DD 77  FC EF DD 77 08 C2 DF 77  ..+s{y¦wnn¦w.-_w
00883A48  42 78 DD 77 12 43 DE 77  17 6C DD 77 8F 9B DF 77  Bx¦w.C¦w.l¦wÅ¢ w
00883A58  90 B0 B5 76 45 AA B5 76  46 EE 4F 77 31 EF 4F 77  É¦¦vE¬¦vFeOw1nOw
00883A68  53 2A 50 77 24 0B A7 7C  50 11 A4 7C C0 3E AB 71  S*Pw$.º|P.ñ|+>½q
00883A78  11 42 AB 71 2B 3E AB 71  80 44 AB 71 55 53 AB 71  .B½q+>½qÇD½qUS½q
00883A88  55 6A AB 71 ED 3F AB 71  53 2E AB 71 51 2F AB 71  Uj½qf?½qS.½qQ/½q
```

```
.text:00404358 lea     ecx, [esp+179D4h+var_16458]
.text:0040435F mov     [esp+179D4h+var_179A5], 's'
.text:00404364 mov     [esp+179D4h+var_179A4], 'e'
.text:00404369 mov     [esp+179D4h+var_179A3], 'H'
.text:0040436E mov     [esp+179D4h+var_179A2], 'a'
.text:00404373 mov     [esp+179D4h+var_179A1], 'n'
.text:00404378 mov     [esp+179D4h+var_179A0], 'd'
.text:0040437D mov     [esp+179D4h+var_1799F], 'l'
.text:00404382 mov     [esp+179D4h+var_1799E], 'e'
.text:00404387 mov     [esp+179D4h+var_1799D], 0
```

spot the string

CYPHORT

One binary to rule forever

- Filehash-based detection
- Updating of binaries in irregular intervals
- Route traffic through local proxy

ZEUS E(DDIE) VASION

CYPHORT

%APP%\Uwirpa	10.12.2013	23:50
%APP%\Woyxhi	10.12.2013	23:50
%APP%\Hibyo	19.12.2013	00:10
%APP%\Nezah	19.12.2013	00:10
%APP%\Afqag	19.12.2013	23:29
%APP%\Zasi	19.12.2013	23:29
%APP%\Eqzauf	20.12.2013	22:23
%APP%\Ubapo	20.12.2013	22:23
%APP%\Ydgowa	20.12.2013	22:23
%APP%\Olosu	20.12.2013	23:03
%APP%\Taal	20.12.2013	23:03
%APP%\Taosep	20.12.2013	23:03
%APP%\Wokyco	16.01.2014	13:22
%APP%\Semi	17.01.2014	16:34
%APP%\Uheh	17.01.2014	16:34

REPETITIVE ARTIFACTS

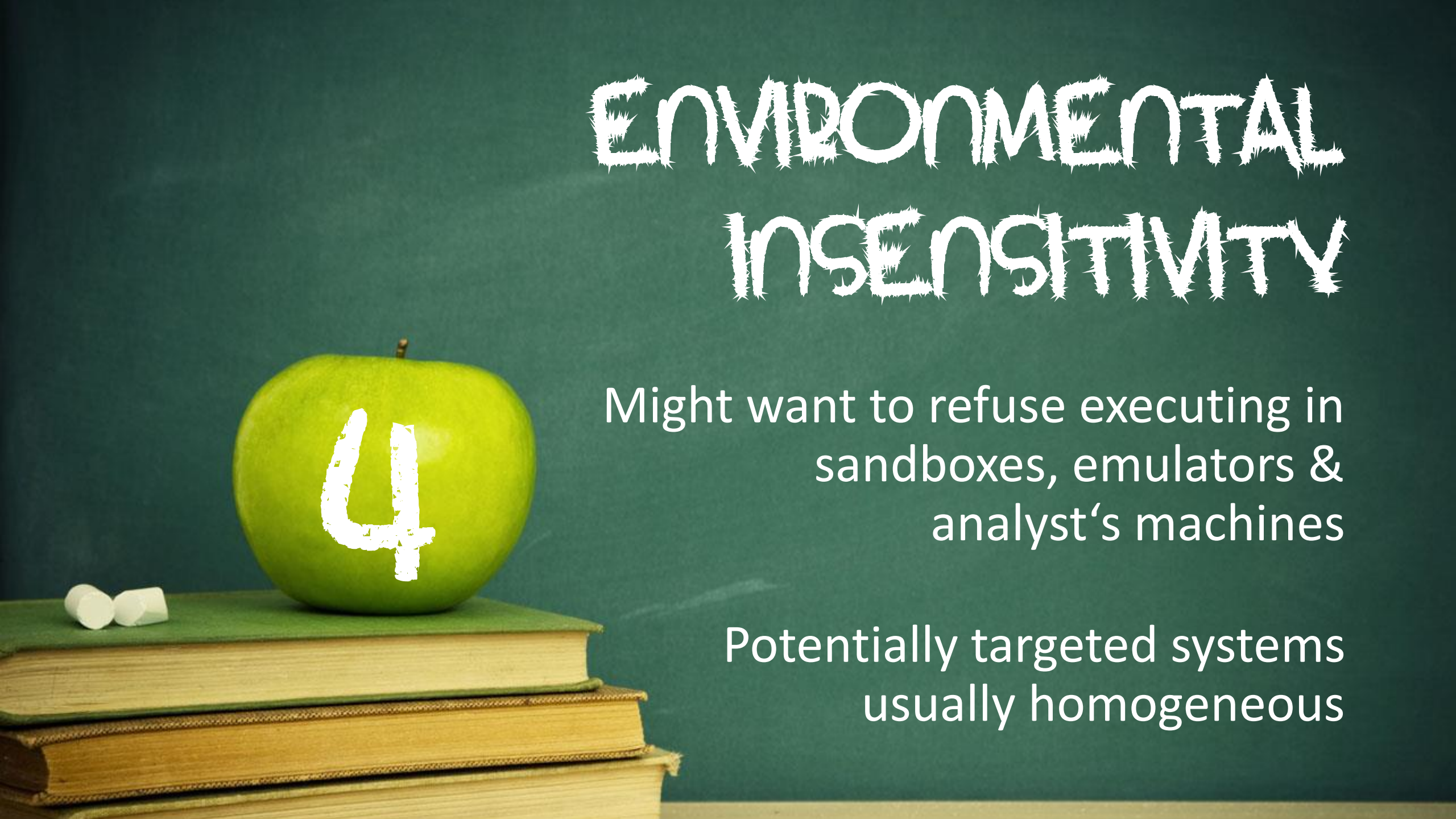
File names

Domain names

Registry key names / value names

Infiltration methods

Persistence methods



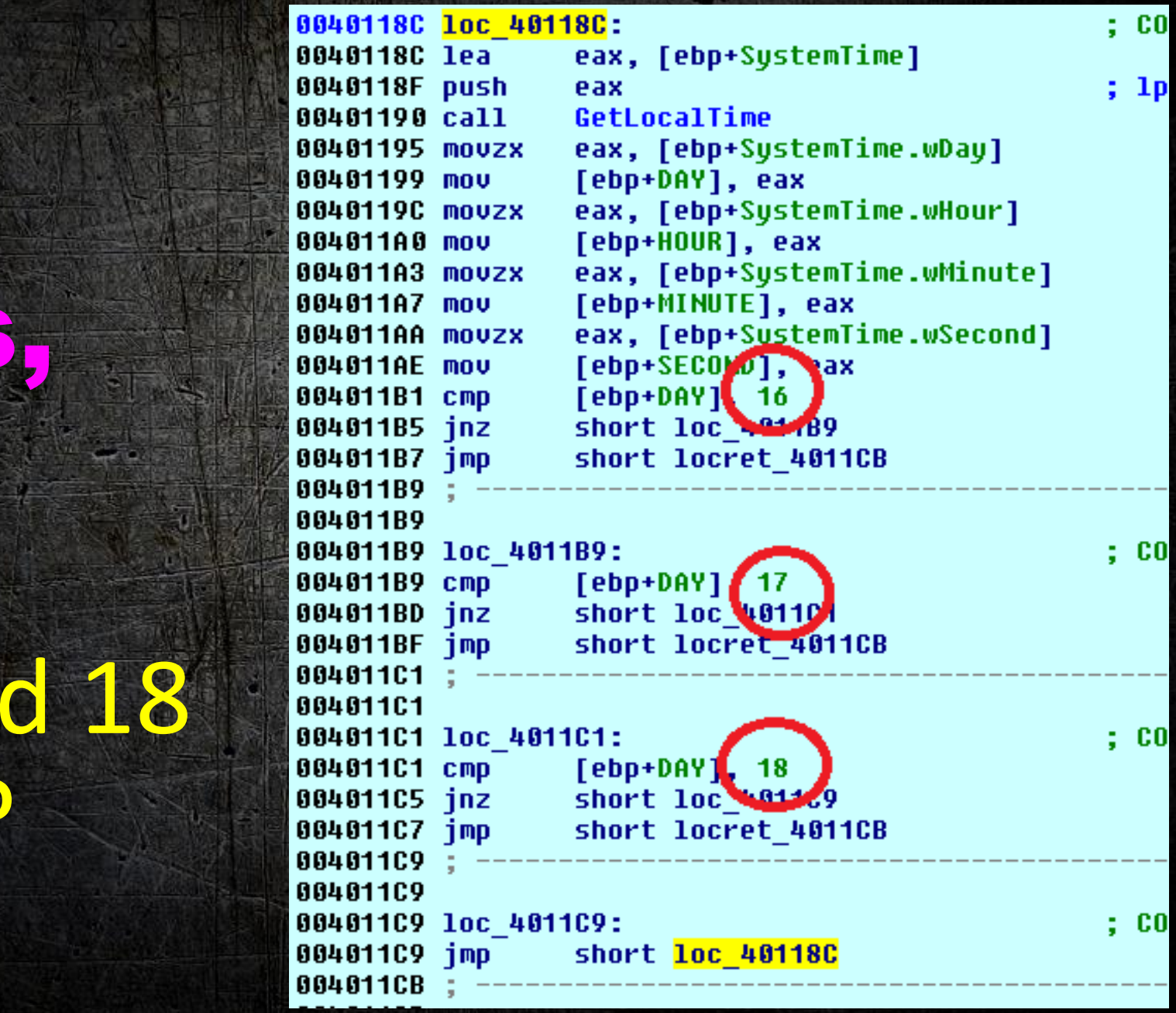
Environmental Insensitivity

Might want to refuse executing in sandboxes, emulators & analyst‘s machines

Potentially targeted systems usually homogeneous

Only infecting Tuesdays, sorry.

Or 16, 17 and 18 next month?



CYPHORT

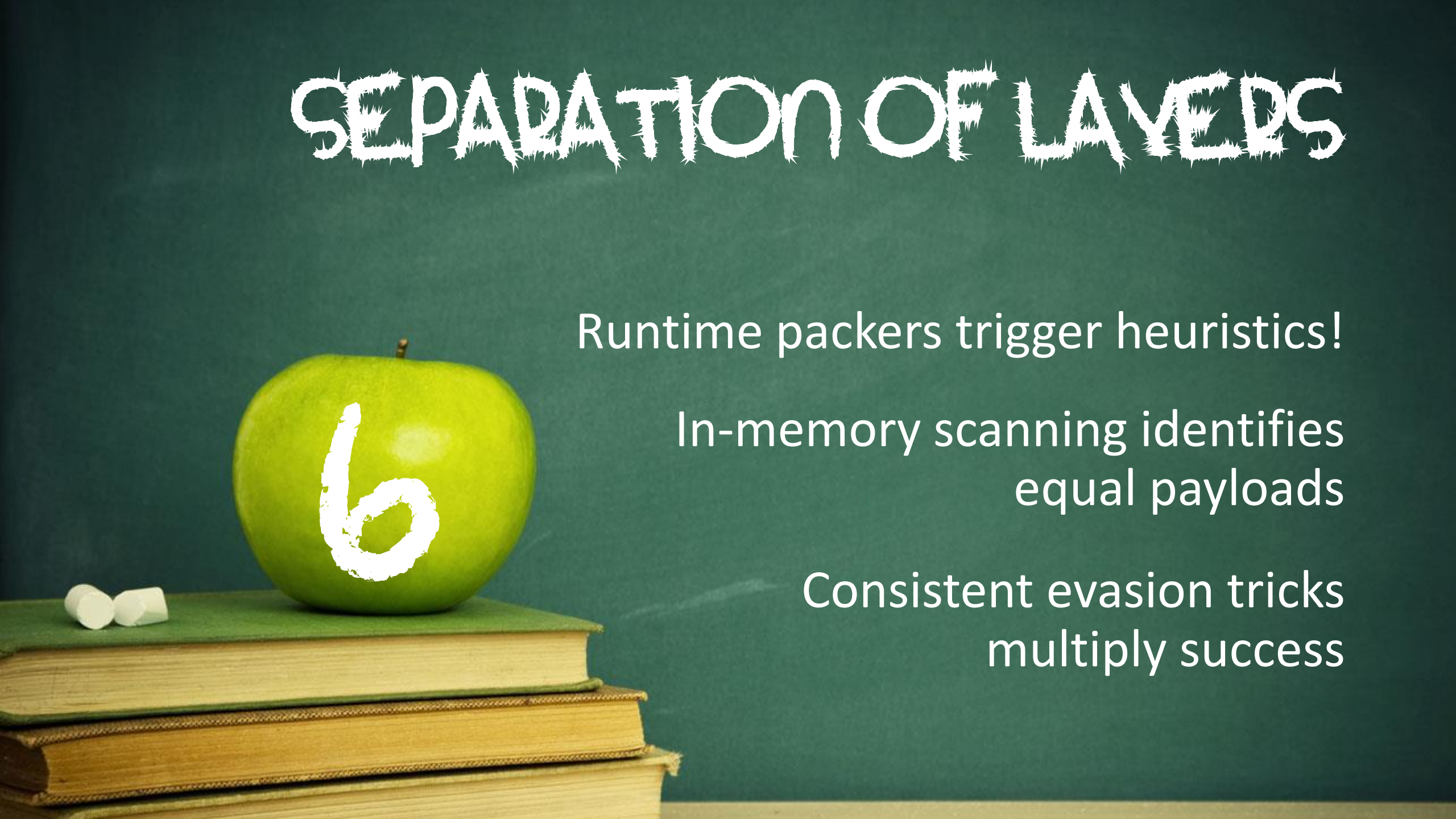
SINGULAR PERSISTENCE

Remember the P?

Registry & service list monitored
One process easy to kill
MBR regularly scanned

Why not do all?

SEPARATION OF LAYERS



Runtime packers trigger heuristics!

In-memory scanning identifies equal payloads

Consistent evasion tricks multiply success

Known spheres

Remember the A?

Find new battle fields

Virtual machine execution
Kernel land code
Bootkits

BIOS


BATTLE
FIELD
you said?

That moment a researcher tells you what‘s wrong with your system, an attacker is already exploiting it.

CYPHORT

BLACKENERGY

Crimeware going APT: Sandworm

Runtime Packer

Malware-like startup & infiltration

Driven by plugins

CYPHORT

HAVEX

RAT used by EnergeticBear

Targets ICS data, accessed via Windows COM/DCOM

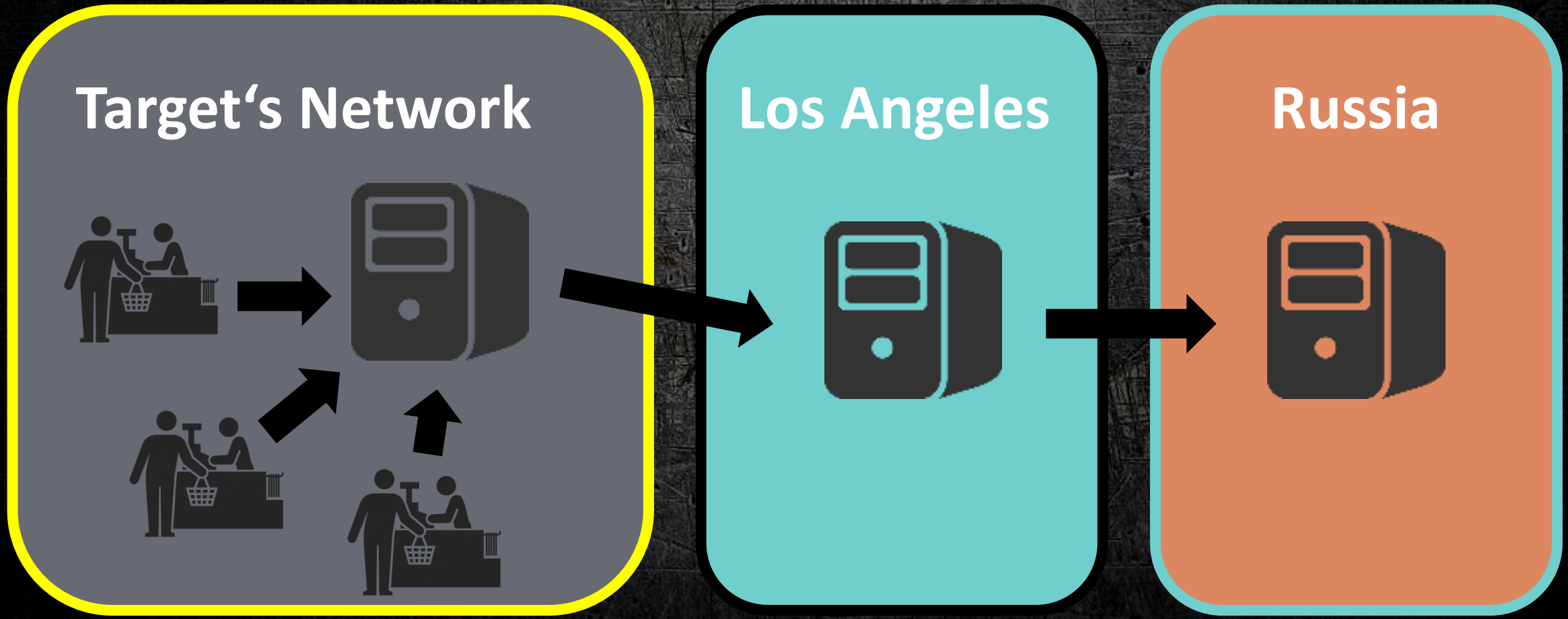
(T)EDDIE

Standard system infiltration

No protection

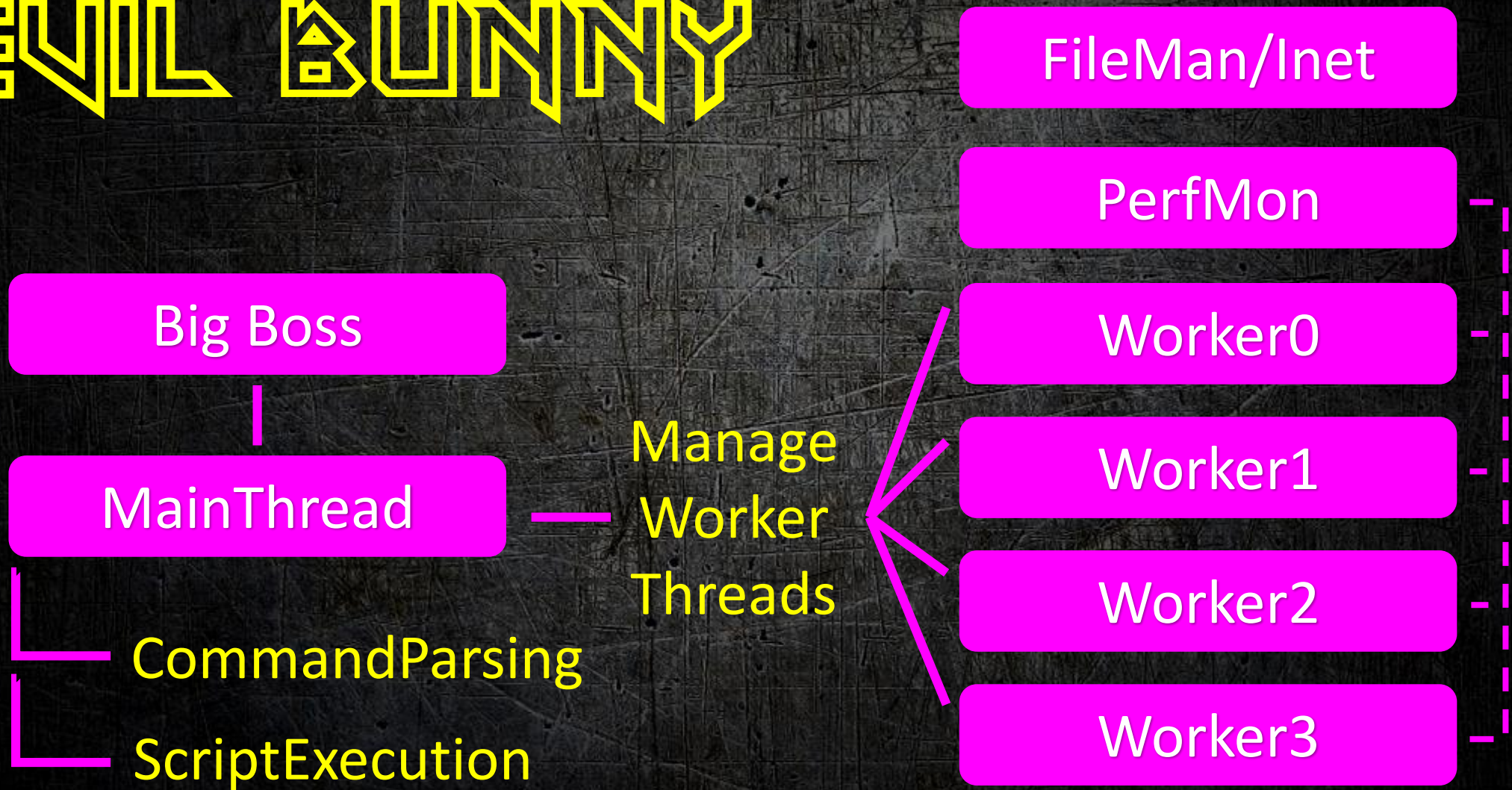
CYPHORT

BLACK POS anatomy of a genius hack



CYPHORT

EVIL BUNNY



CYPHORT

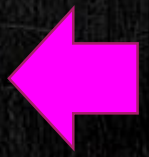
1. Unique binaries
2. Irregular updates
3. No repetitive artifacts
4. Environmental sensitivity
5. Multiple persistence techniques
6. Consistent evasion
7. Unknown spheres

CYPHORT

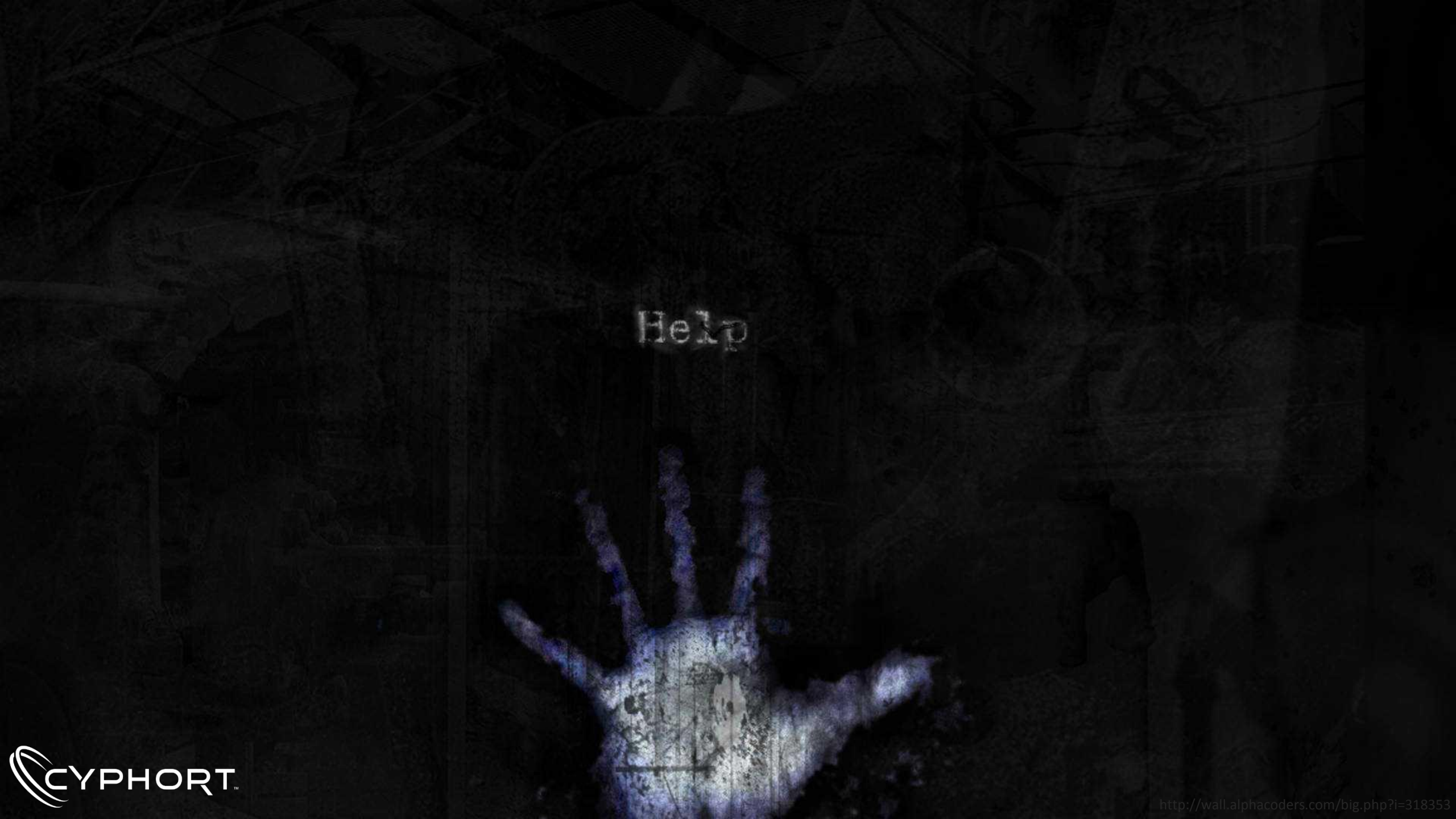
The A and the P of the T

	1	2	3	4	5	6	7
BlackEnergy	■	■					
Havex							■
BlackPOS							
EvilBunny	■	■		■			■

estimated
56 Mio.
credit cards
compromised



CYPHORT



CYPHORT™

http://wall.alphacoders.com/big.php?i=318353

RESOURCES

- **Havex** - http://www.cyphort.com/windows-meets-industrial-control-systems-ics-havex-rat-spells-security-risks-2/
- **BlackPOS** - http://www.cyphort.com/parallels-among-three-notorious-pos-malwares-attacking-u-s-retailers/
- **EvilBunny** - https://drive.google.com/a/cyphort.com/file/d/0B9Mrr-en8FX4M2lXN1B4eElHcE0/view
- **Eddie** - http://maiden-world.com/downloads/wallpaper.html

CYPHORT

Thank you!

Marion Marschalek
@pinkflawd
marion@cyphort.com

CYPHORT™

http://karmadecay.com/