Apology of 0days

Nicolás Waisman

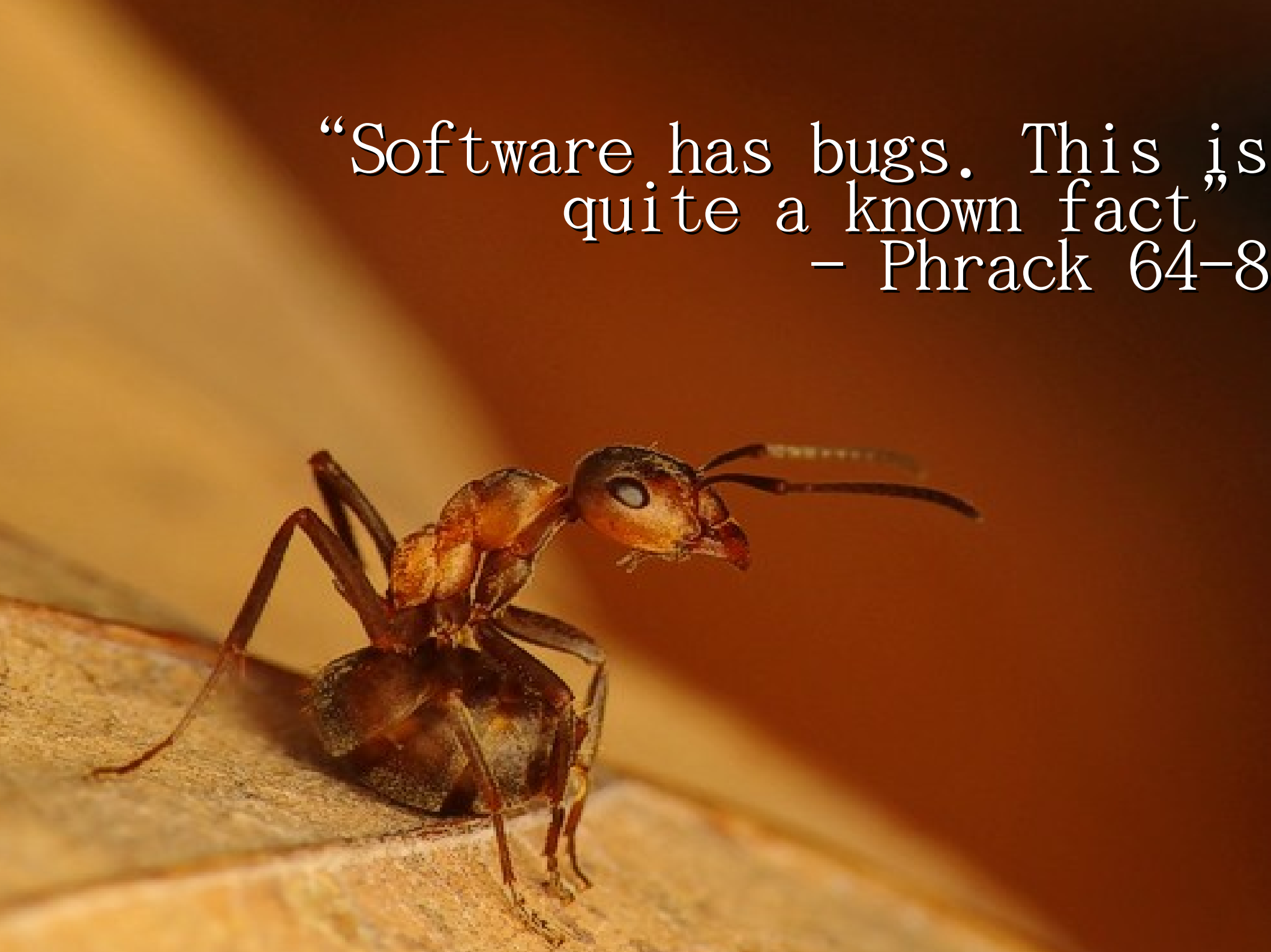
IMMUNITY

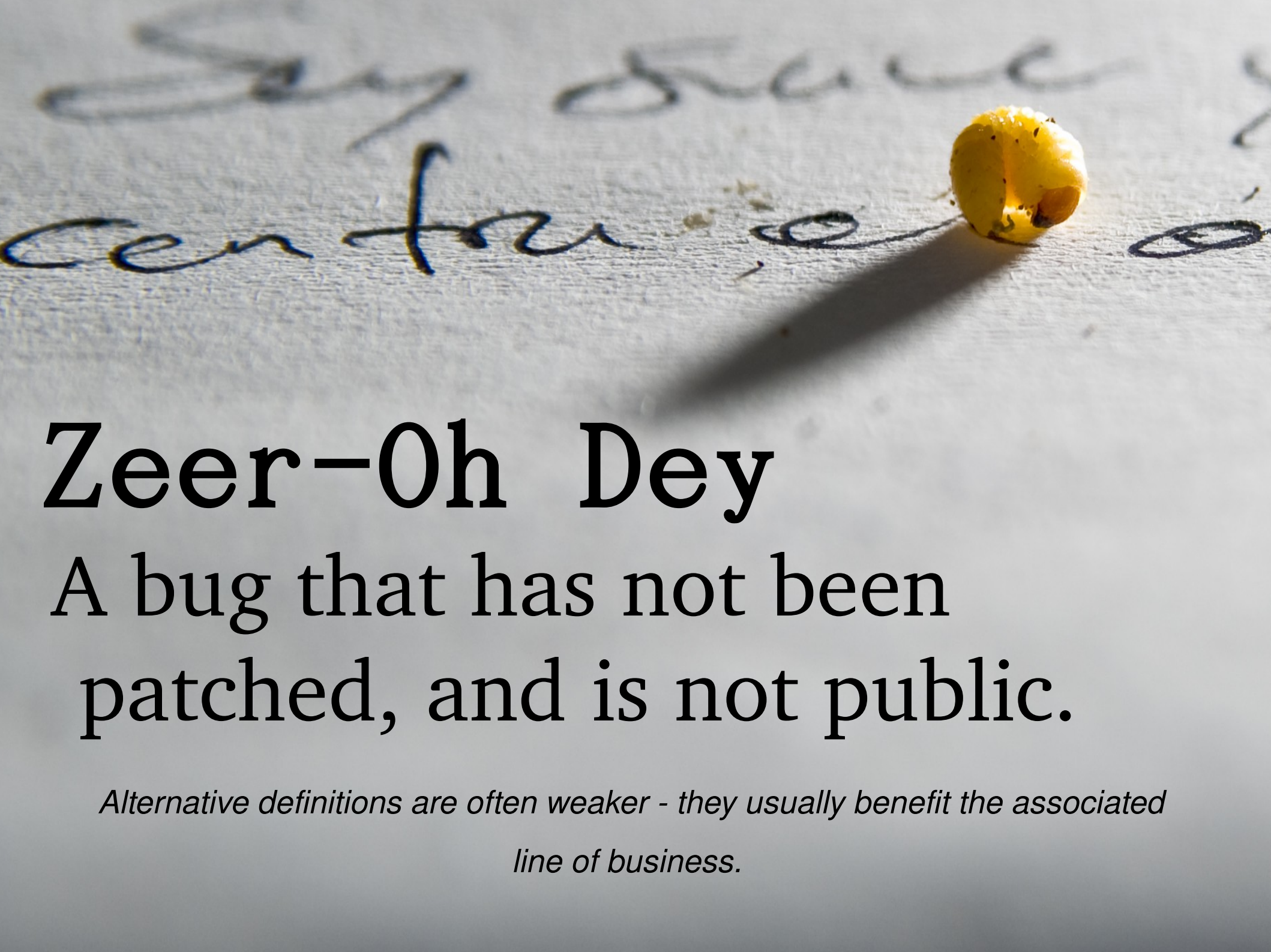
Who Am I?

Senior Security Researcher and Regional Manager at Immunity, Inc.

Research and Development of reliable Heap Overflow exploitation for CANVAS attack framework

ıs.waisman@immunityinc.com


“Software has bugs. This is quite a known fact”
- Phrack 64-8



Zeer-Oh Dey

A bug that has not been patched, and is not public.

Alternative definitions are often weaker - they usually benefit the associated line of business.


“Mors Certa,
hora incerta”

Value of 0day

Four contributing factors:

1. Complexity
2. Uniqueness
3. Relevance
4. Exploitability

Why look for a 0day?

LADIES

Desde Merlo
Alarmó a la Web

Francisco Amato creó el software antihackers del que todos hablan.

Leonardo Correa
lcorrea@clarin.com

FAME

La historia co[n] cua[l] Dan Kamins[ky], encum[brad]o investiga[r] [la] seg[uridad] informática, explicó en la prestigiosa conferencia Black Hat de julio, cómo es eso de que toda Internet está (o estaba) en jaque.

Ante una platea [...] una dirección, en rigor está "marcando" un número, como se hace con el teléfono. Lo que descubrió Kaminsky es que ese número puede ser cambiado por terceros. De modo que si alguien ingresa a un sitio conocido, tipiando como siempre lo hace, podría entrar a una página falsa, melliza. Esto sería **doblemente grave** si se trata de una página de un banco, o de u[n] [...]vel[...]ail [...]on l[...] que se podrían r[...] [...]ves[...] más datos.

[...]aú[...] Cómo el problema [...] de los dominios de Internet, incluye a **todos los sistemas operativos**: Windows, Linux y Mac.

A la hora de la exposición en Black Hat, Kaminsky se refirió a

DIEGO WALDMANN

PRECOZ. A los 24 ya tiene su empresa de seguridad informática.

seguridad del que todo el mundo habla. El famoso Evilgrade. Y basta con tipiar ese nombre en Co[...]

sea que ponga quien lo use. Simula también ser actualización de

MONEY

Every time you publish a bug, God kills a kitten

Who needs 0days?

- Pentesters
- Government/Mil
- You
- Me :)

Immunity's 0day numbers

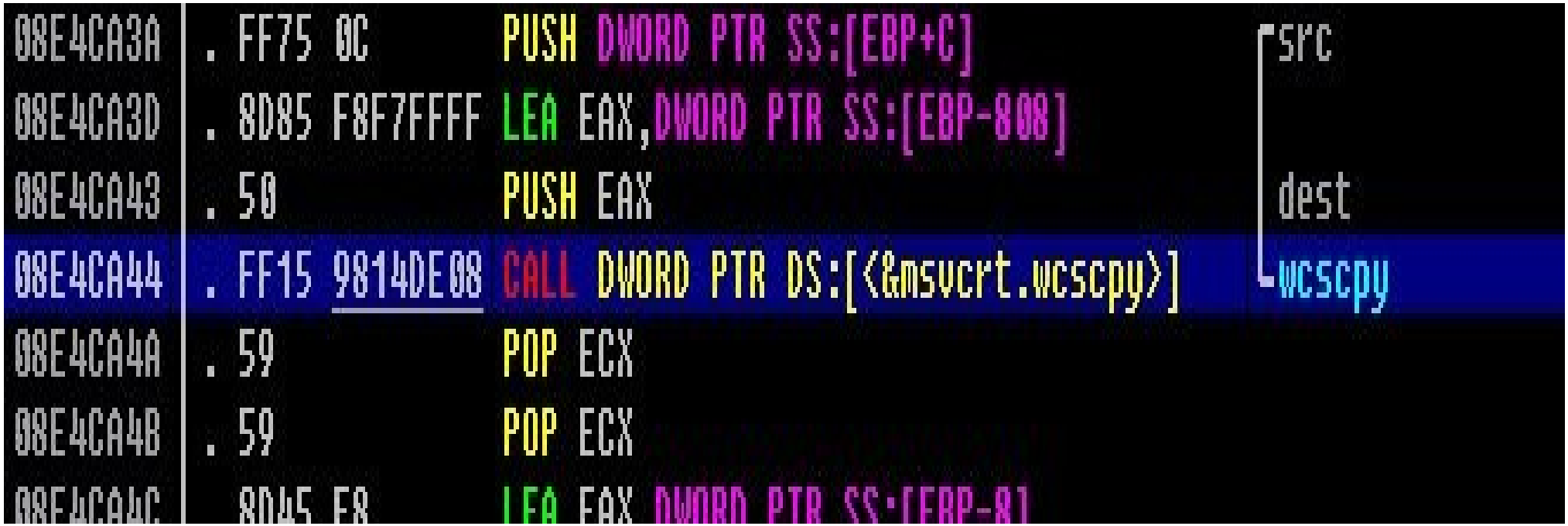
Average 0day lifetime: **348** days

Shortest life: **99** days

Longest life: **1080** (3 years)

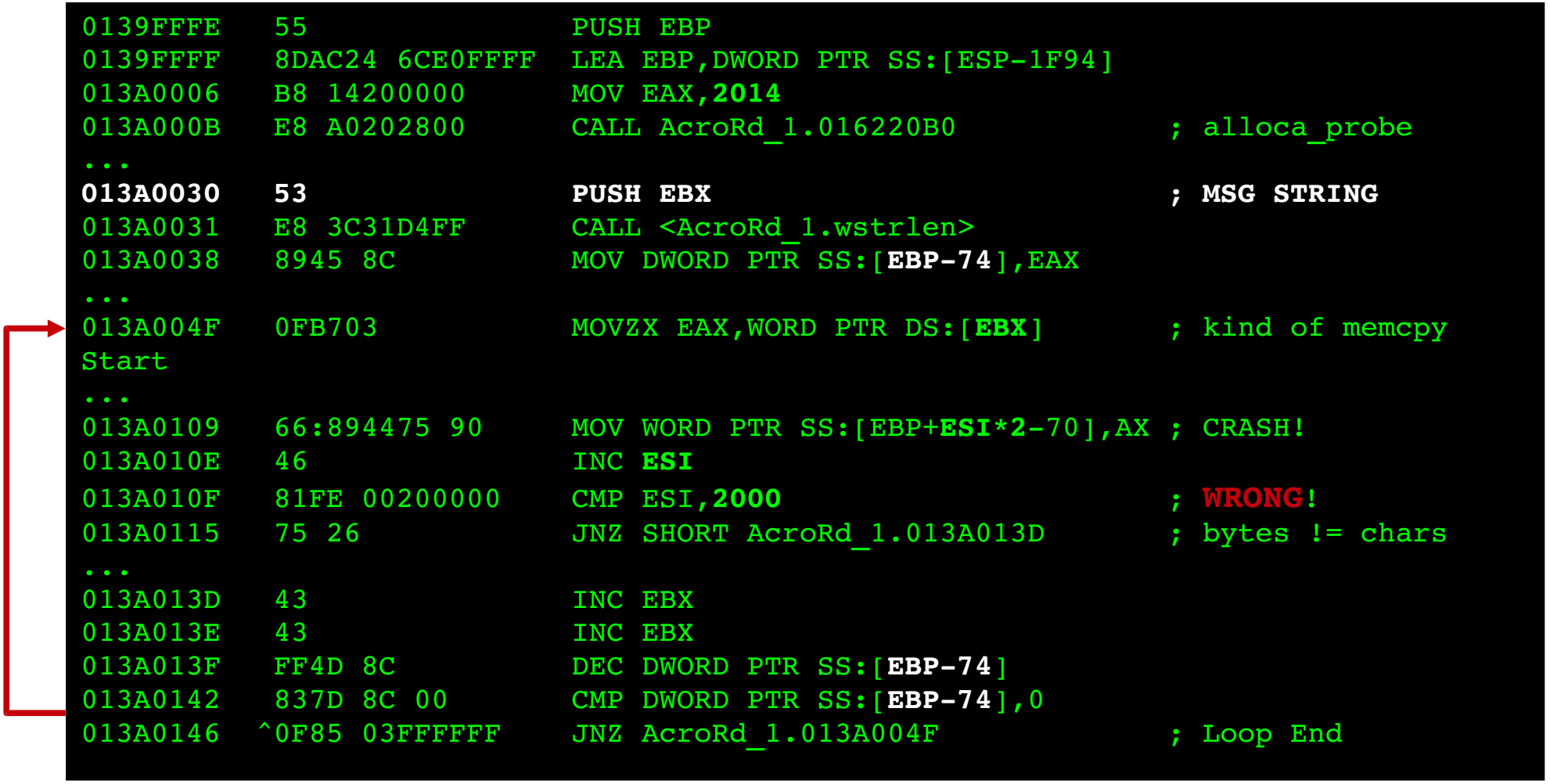
Low Hanging Fruit

Grep is getting old, but still useful sometimes



Low Hanging Fruit

Fuzzing is ok, but vendors also use it a lot.



Racing the fuzzers

education; I think it's important to make people aware that even with great tools and great security-savvy engineers, there are still bugs that are very hard to find.

Fuzz Testing

I'll be blunt; our fuzz tests did not catch this and they should have. So we are going back to our fuzzing algorithms and libraries to update them accordingly. For what it's worth, we constantly update our fuzz testing heuristics and rules, so this bug is not unique.

Defenses

If you want the full details of the defenses, and how they come into play on Windows Vista and Windows Server 2008, I urge you to read the SVRD team's in-depth analysis once it is posted.

Racing the fuzzers

The Mecca: Manual Auditing

Write Loops

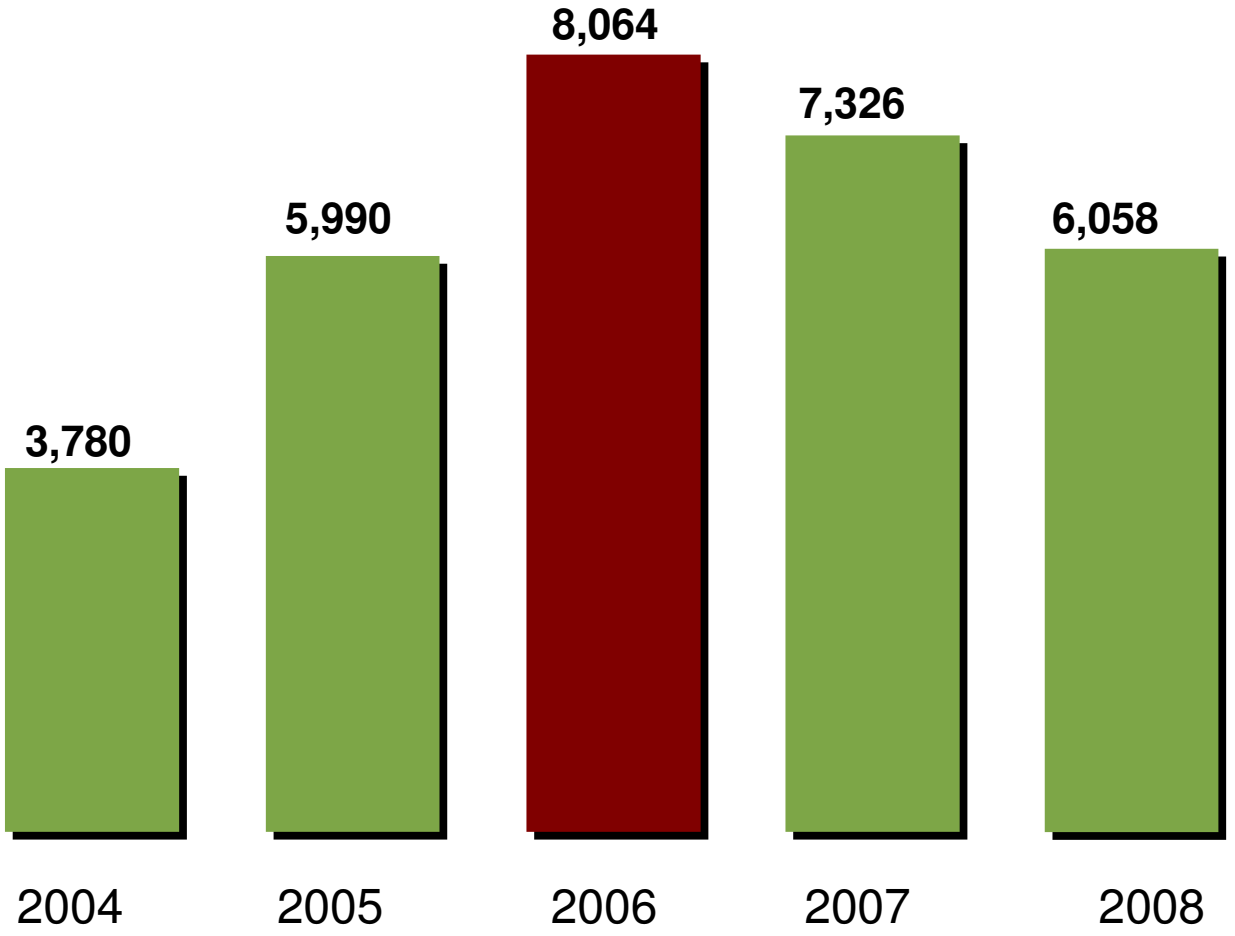
Logic Bugs

Return from functions

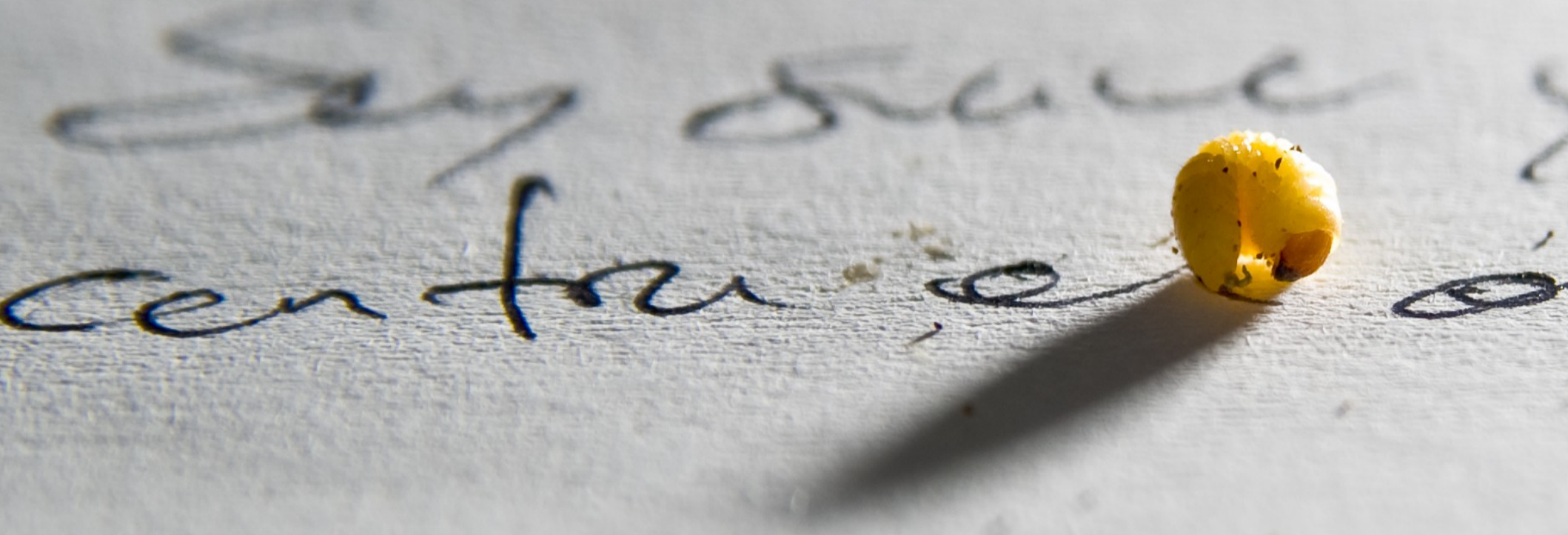
Race conditions

New Bug Class

Vulnerability Remediation Statistics

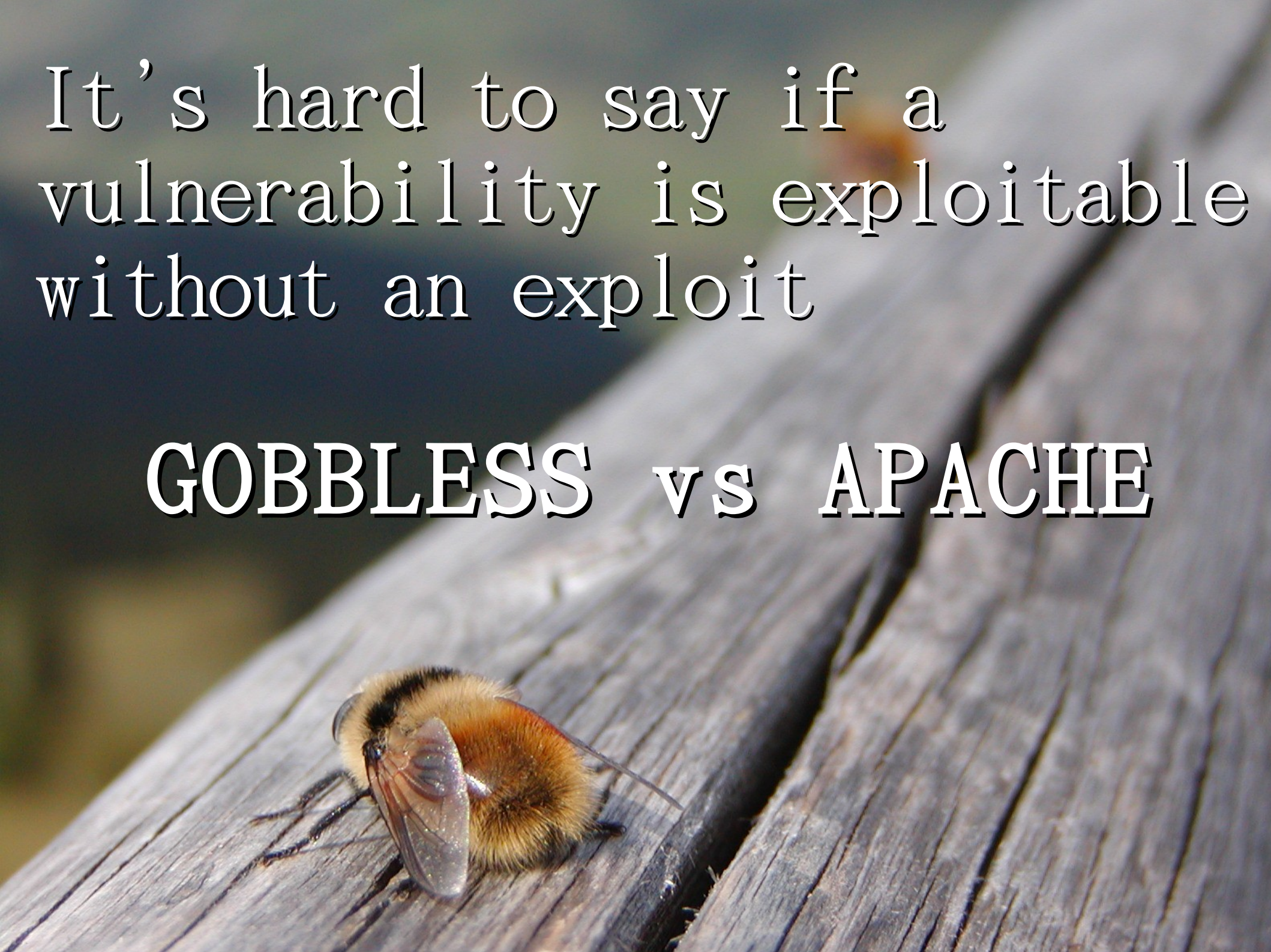


source: CERT/CC 2008



Exploits

An exploit is a working program that takes advantage of one **or more** vulnerabilities in order to break boundaries.


It's hard to say if a vulnerability is exploitable without an exploit
GOBBLESS vs APACHE

Public Exploits

VS

Commercial Exploits

“Mitigating” factors

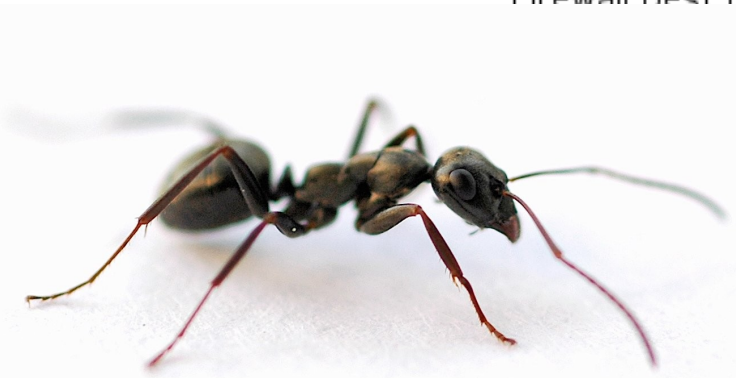
Mitigating Factors for Print Spooler Vulnerability - CAN-2005-1984:

- On Windows XP Service Pack 2 and Windows Server 2003, this vulnerability is restricted to authenticated users. Additionally, in order for this issue to create a remote attack vector on these operating system versions, a local user who has appropriate permissions must first share a printer or try to connect to a shared printer. If no user with appropriate permissions has shared a printer or tries to connect to a shared printer, an attacker would have to have valid logon credentials and must be able to log on locally to exploit this vulnerability.

- On Windows XP Service Pack 2 and Windows Server 2003, this issue would result in a denial of service condition. On Windows XP Service Pack 2 and Windows Server 2003, this issue cannot be exploited for remote code execution or for elevation of privilege.

On other operating system versions, attacks attempting to exploit this vulnerability would most likely result in a denial of service condition. However remote code execution could be possible.

Firewall best practices and standard default firewall configurations can help protect
acks that originate outside the enterprise perimeter. Best practices
ystems that are connected to the Internet have a minimal number of



It could be done!

```
self.connect()
self.MemLeak(0x208,4) #fills in 0x42 sized chunks
self.MemLeak(0x220,4) #fills in 0x45 sized chunks
self.RpcAddPrinterConnection('A'*0x54) #creates a hole for 84 byte allocations
self.setProgress(40)
self.log('[*] Populating lookaside table')
what=0x7ffdf300; self.log('[*] Write4(0x%08x,0x%08x)'%(what,what+8))
self.Write4(what,what+8)
what=0x7ffdf310; self.log('[*] Write4(0x%08x,0x%08x)'%(what,what+8))
self.Write4(what,what+8)
what=0x7ffdf320; self.log('[*] Write4(0x%08x,0x%08x)'%(what,what+8))
self.Write4(what,what+8)
self.log('[*] Overwriting PEB lock function')
what=0x7ffdf318; where=0x7ffdf020 #PEB lock function
self.log('[*] Write4(0x%08x,0x%08x)'%(what,where))
self.Write4(what,where)
self.log('[*] Triggering PEB lock function')
self.RpcEnumPorts()
if self.ISucceeded():
    self.setInfo('%s attacking %s:%d (succeeded!)'%(self.name,self.host,self.po
```

FAIL!

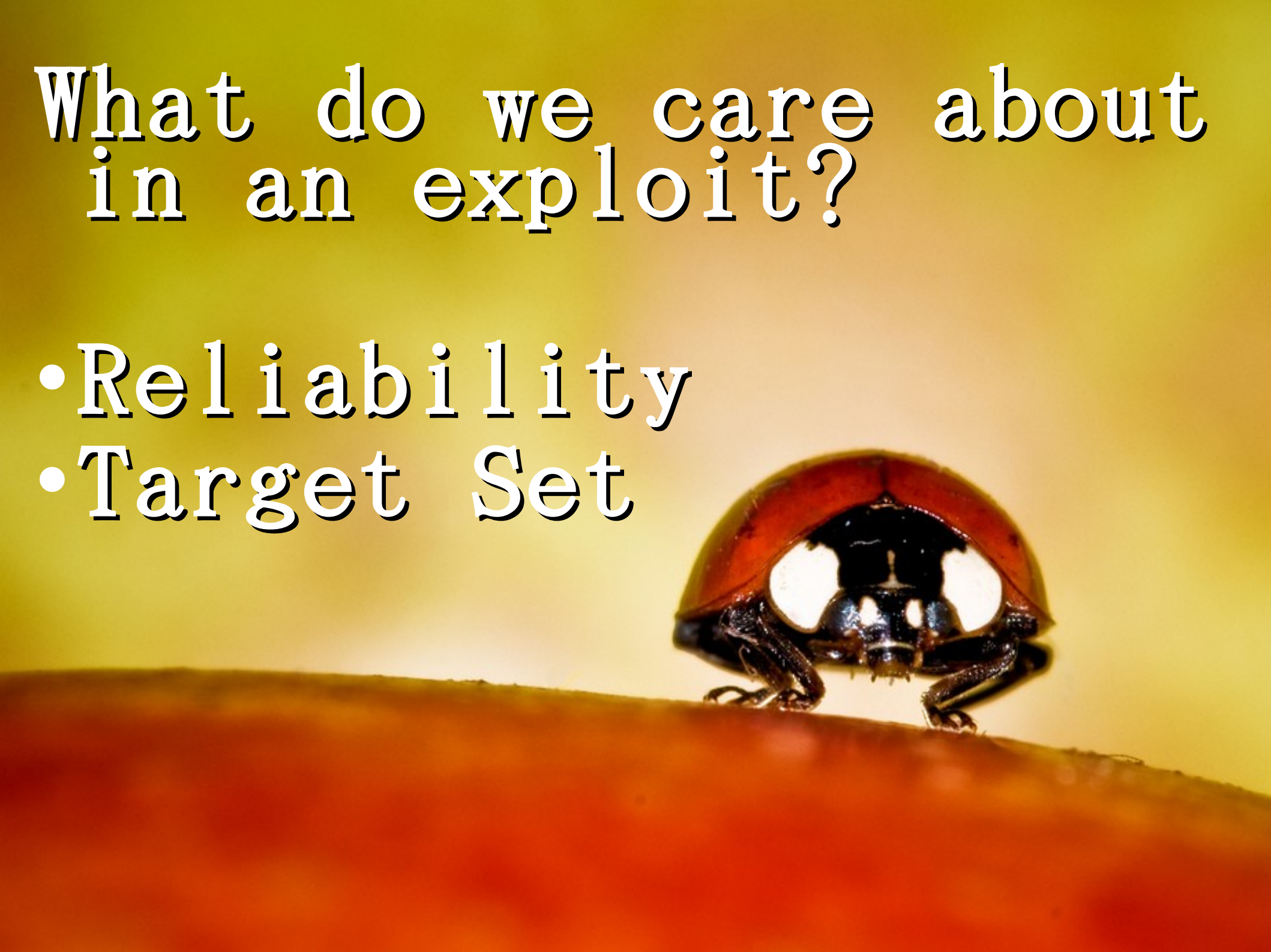
You know that your exploit is gonna fail...

when it only connects once to the target...

```
$request = "A"x30 . $JMP . $EAX . $ECX .
  "B"x100 . $SC;
my $left = 1000 - length($request);
$request = $request . "C"x$left;
$request = $cmd . $request . "\r\n";
send $socket, $request, 0;
```

What do we care about in an exploit?

- Reliability
- Target Set



Welcome to Windows Protections...

/GS

DEP/NX/W^X/PAX

ASLR

Heap Protections

SafeSEH

etc

A change in the old paradigm...

Are bugs more valuable than exploits?

YES!

New vulnerabilities classes and complex bugs

MAYBE!

Stack Overflow bug in Server 2003

NO!

Heap overflow bugs

(yes, including Win2k)

What will you choose?

RealServer

Dtlogin

Corollary

If we use **TIME** & **SKILLS** as variables, writing exploits is a similar investment to finding bugs

Every time you publish a bug, Maradona scores against Brazil

2000 A.D.

Stack Overflow

- 26' minutes to exploit NOP Certification target
- 1 or 2 days to find address for all SPs and Language packs
- 3 minutes of victory dancing

Demo Time

2003 A.D.

Stack Overflow bypassing DEP

- 26' minutes to exploit NOP Certification
- 2 to 4 days to make it universal
- 6 minutes of victory dance

Heap Overflows

Windows 2000

- 1 day: Triggering the bug
- 1-2 days: Understanding the heap layout
- 2-5 days: Finding Soft and Hard Memleaks
- 5-8 days: Finding a reliable Write4
- 1-2 days: Function Pointers and Shellcode

Heap Overflows

Windows 2003/XP SP2

- 1 day: Triggering the bug
- 1-2 days: Understanding the heap layout
- 2-5 days: Finding Soft and Hard Memleaks
- 10-30 days: Overwriting a Lookaside Chunk
- 1-2 days: Getting burned out, crying like a baby, trying to quit, doing group therapy

- 2-5 days: Finding a Function pointer

Heap Overflow

Vista

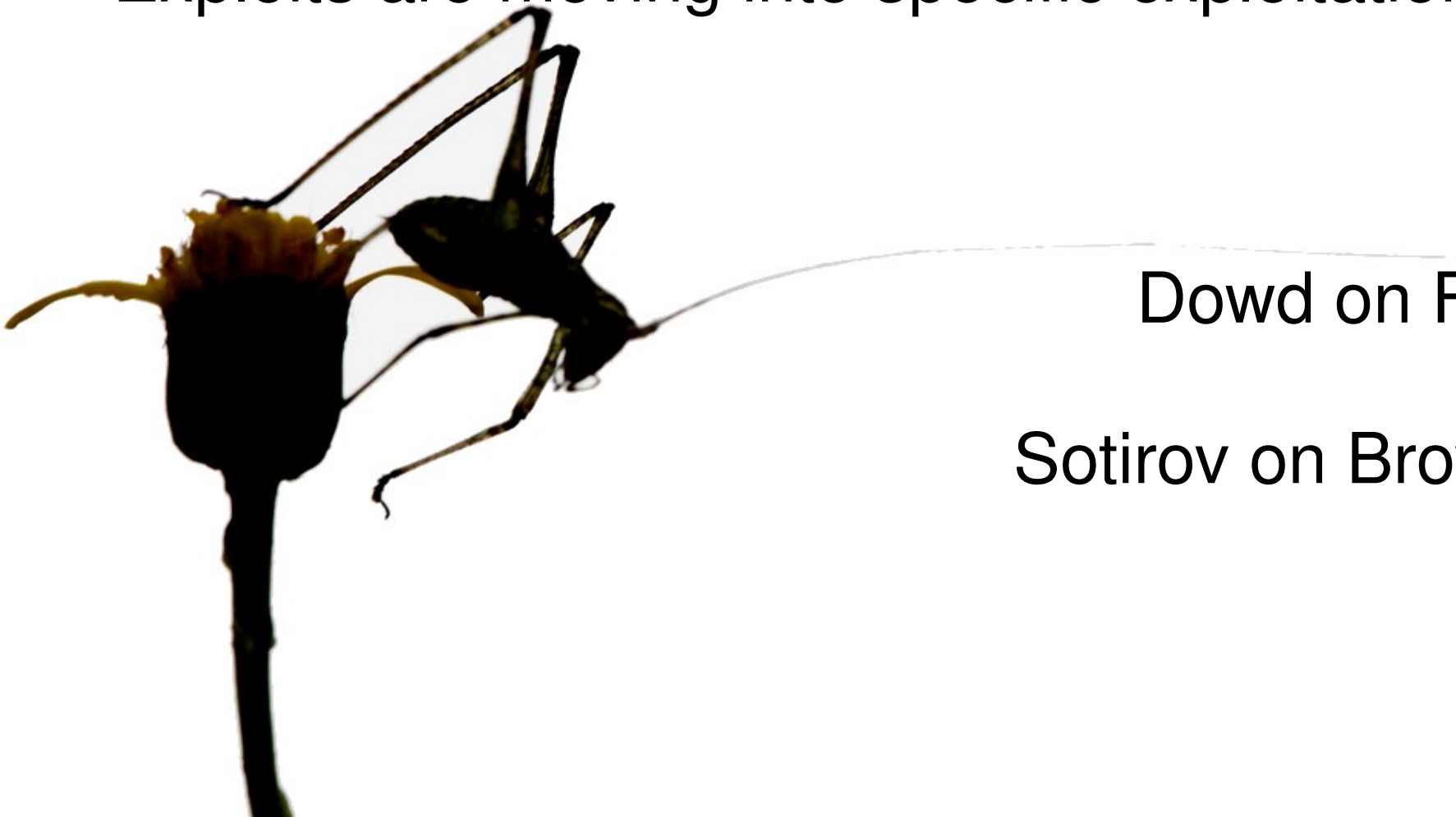
Take your estimated time of development for Server2k3/XP SP2 and double it

(36-94 days)

Exploitation

Generic techniques are a thing of the past!

Exploits are moving into specific exploitation:



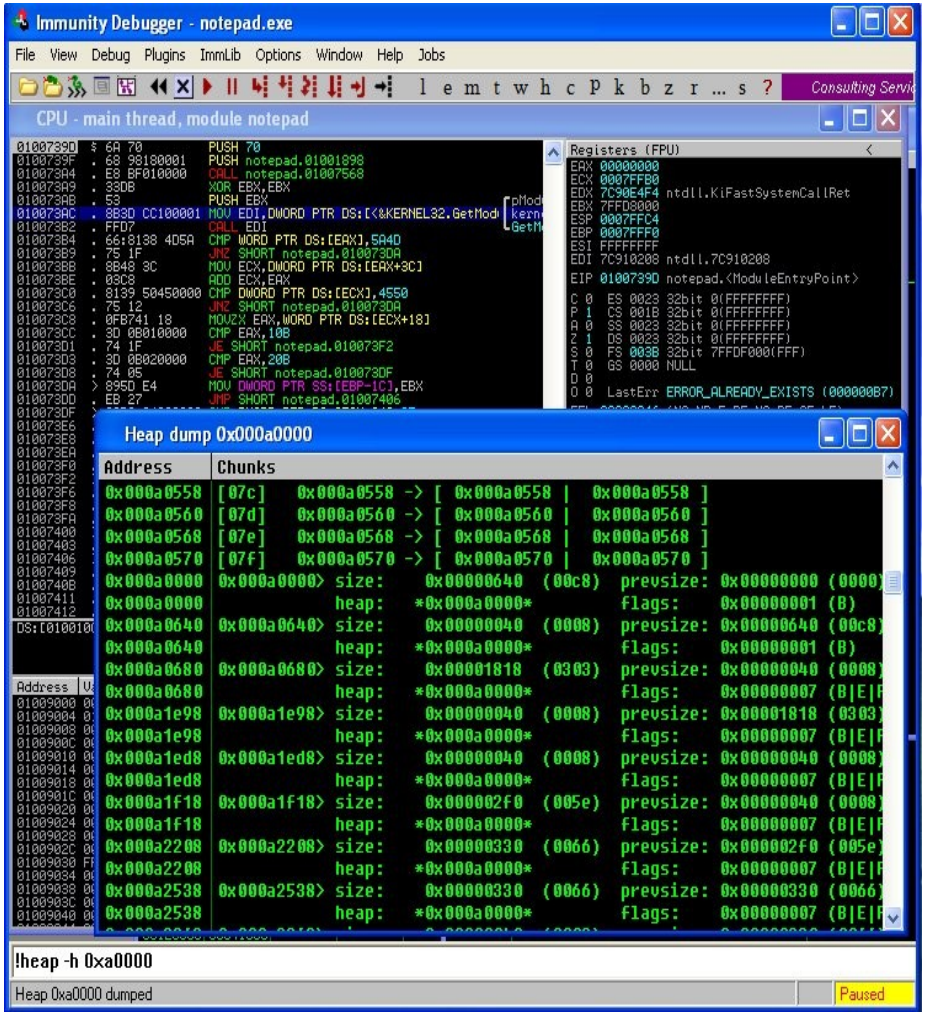
Dowd on Flash

Sotirov on Browser

Conclusion

Improve your tools:

- easy to **u**se
- easy to **s**hare
- easy to **e**xpand
- easy to **r**euse



- Train your employees

- Train yourself (Don't give up)

Every time you publish a bug, PR0J3KT M4YH3M will go after you ;)

[Full-disclosure] i sh0t the white hat eDiçãO 4 (PR0J3KT M4YH3M BR4Z1L)

From: H2G-Labs Information Security (h2glabs.infosec@gmail.com)

Date: Sun Nov 02 2008 - 17:34:35 CST

- **Messages sorted by:** [date] [thread] [subject] [author]

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

The new version (4) of the "i sh0t the white hat" zine (PR0J3KT M4YH3M BR4Z1L).

URL: http://rs417.rapidshare.com/files/160091755/istwh4.txt

These guys do a good job counter some pseudo elite kids and CISSPs at Brazil.

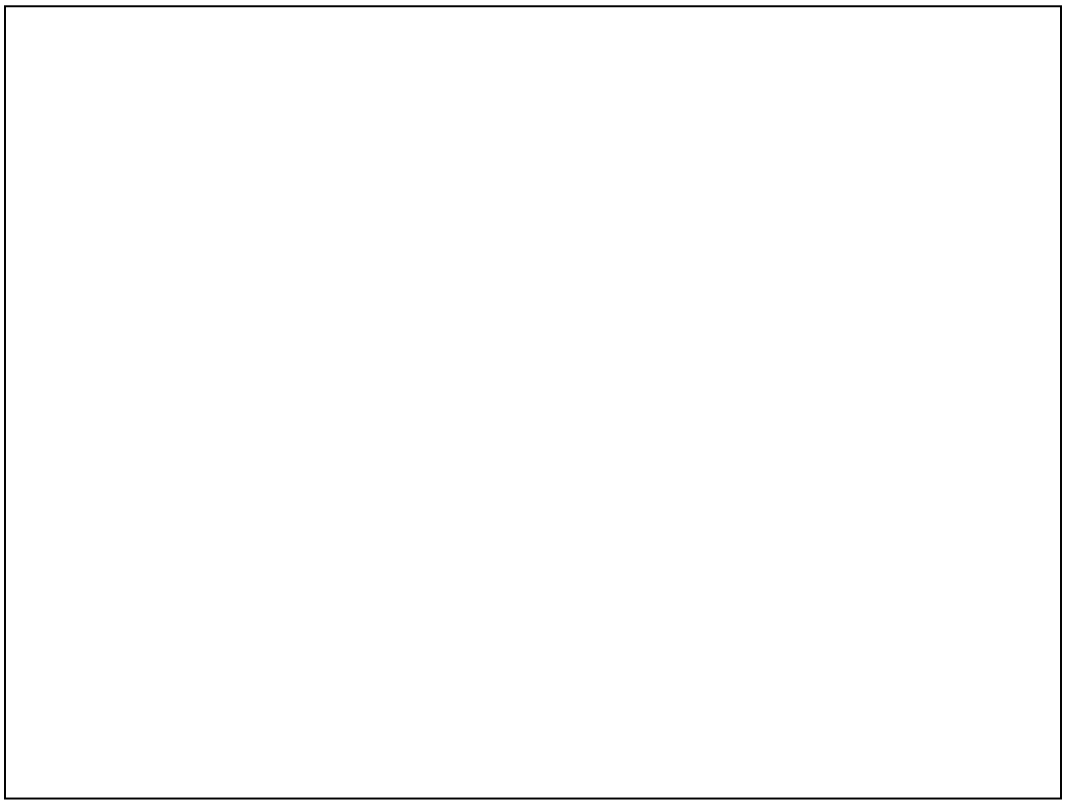
In this version, we can see a funy hack counter Nash Leon (Glaudson O Campos).

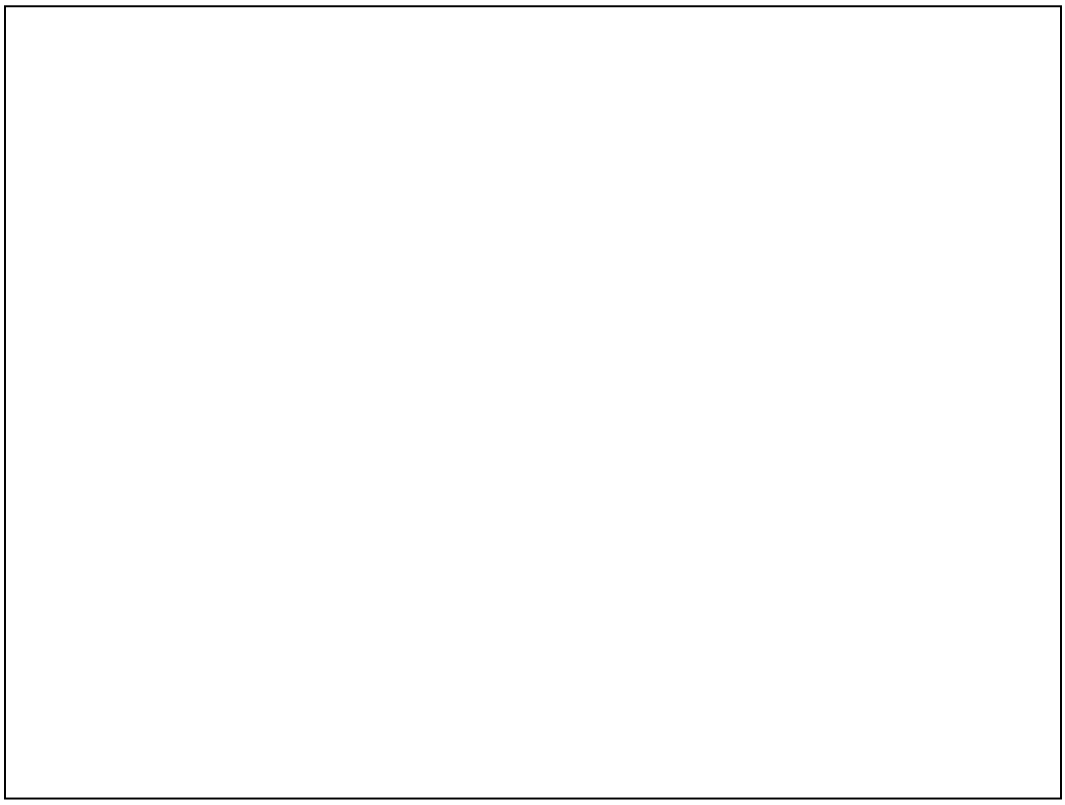
:P

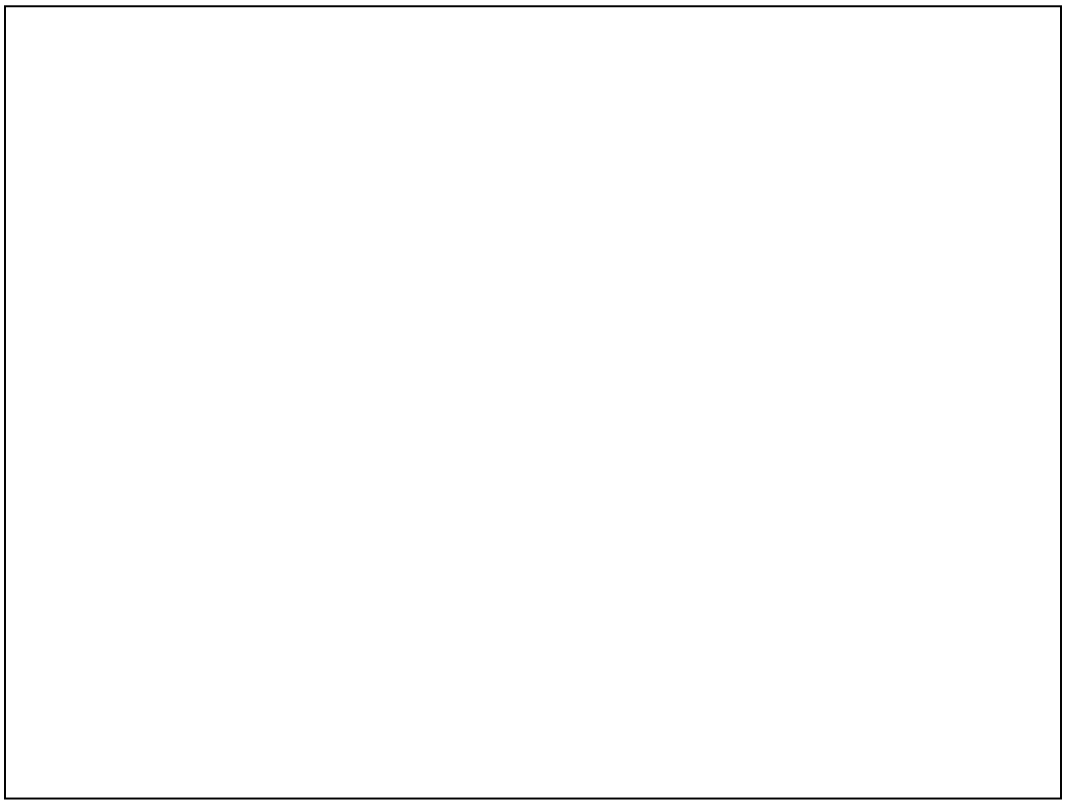
Regards...

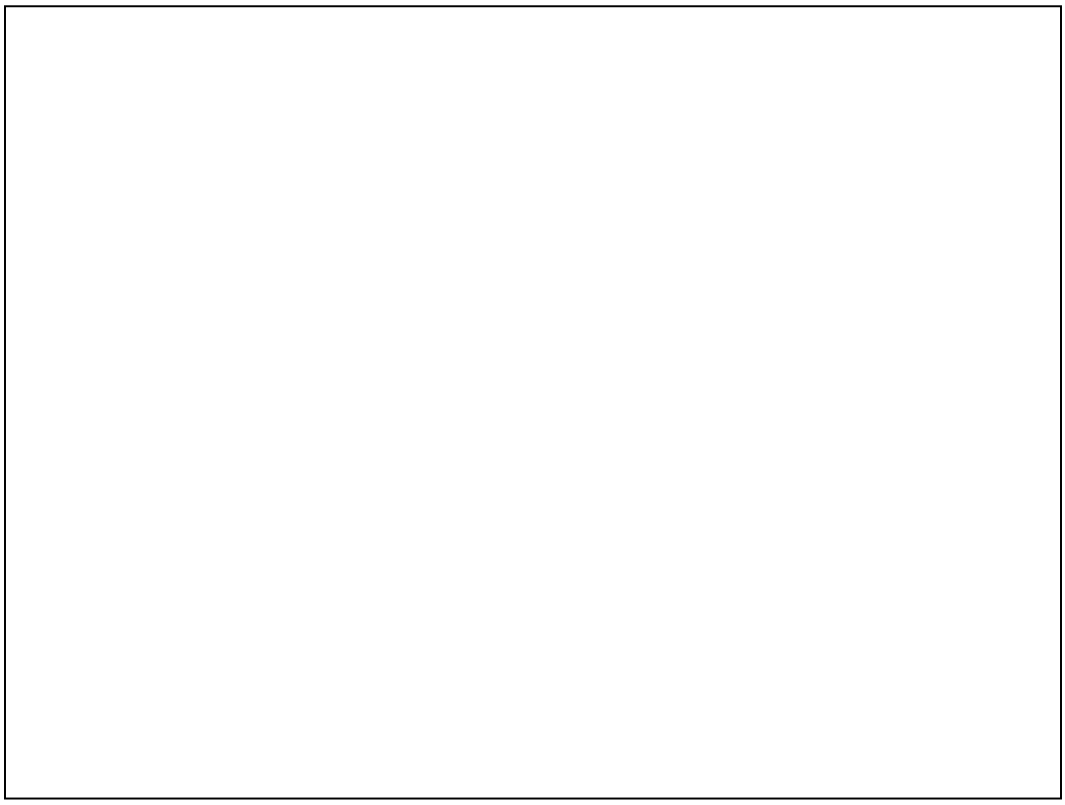
- --
H2G-Labs Information Security
Igor Marcel - Information Security Consultant
H2GLabs.InfoSec "at" Gmail.com

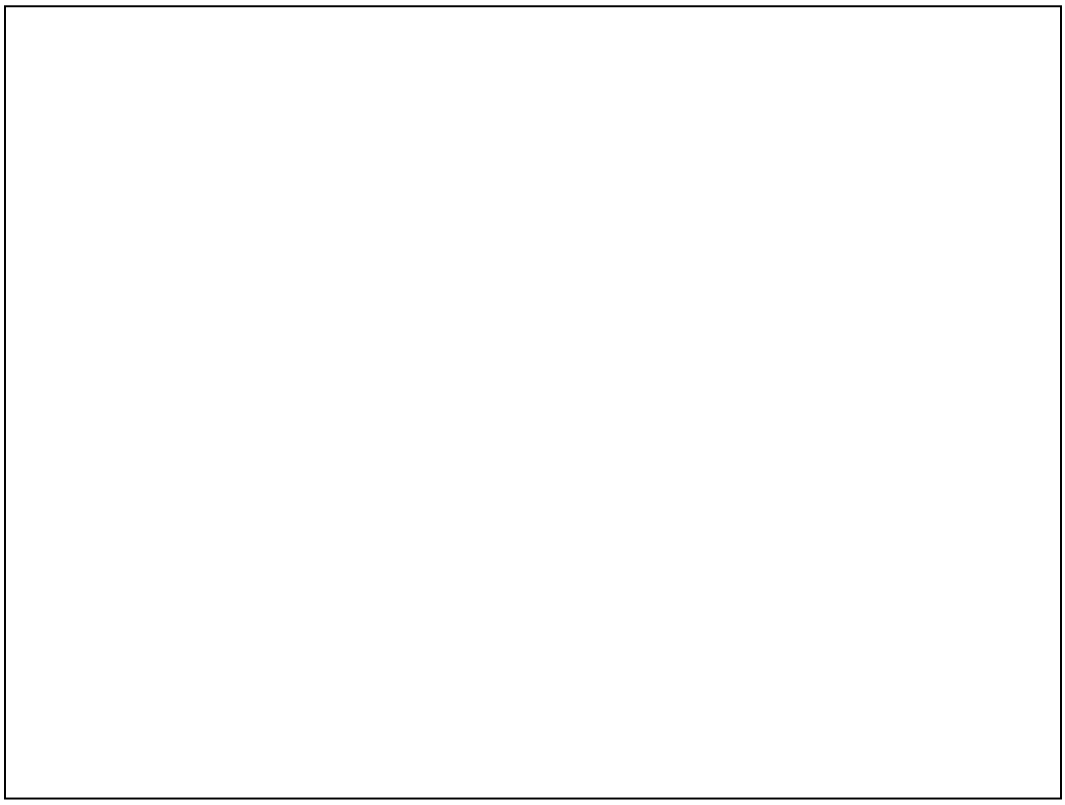
-----BEGIN PGP SIGNATURE-----
Version: GnuPG (PRIVATE)
Comment: H2G-Labs Information Security

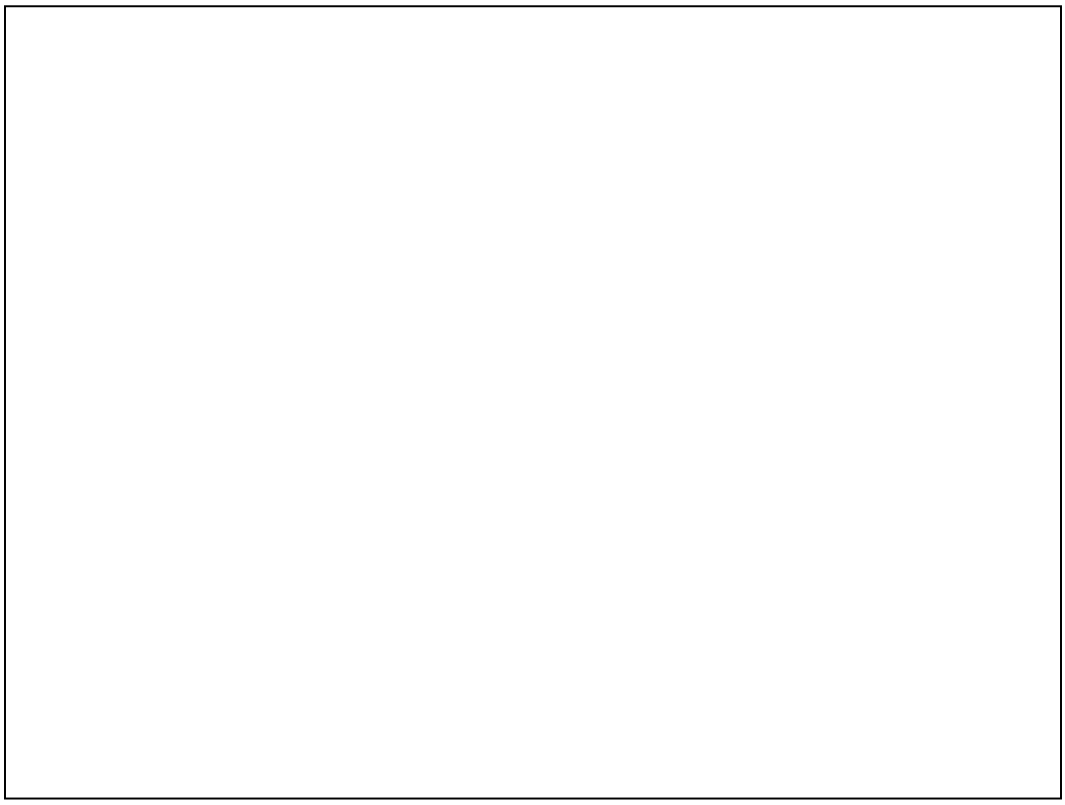


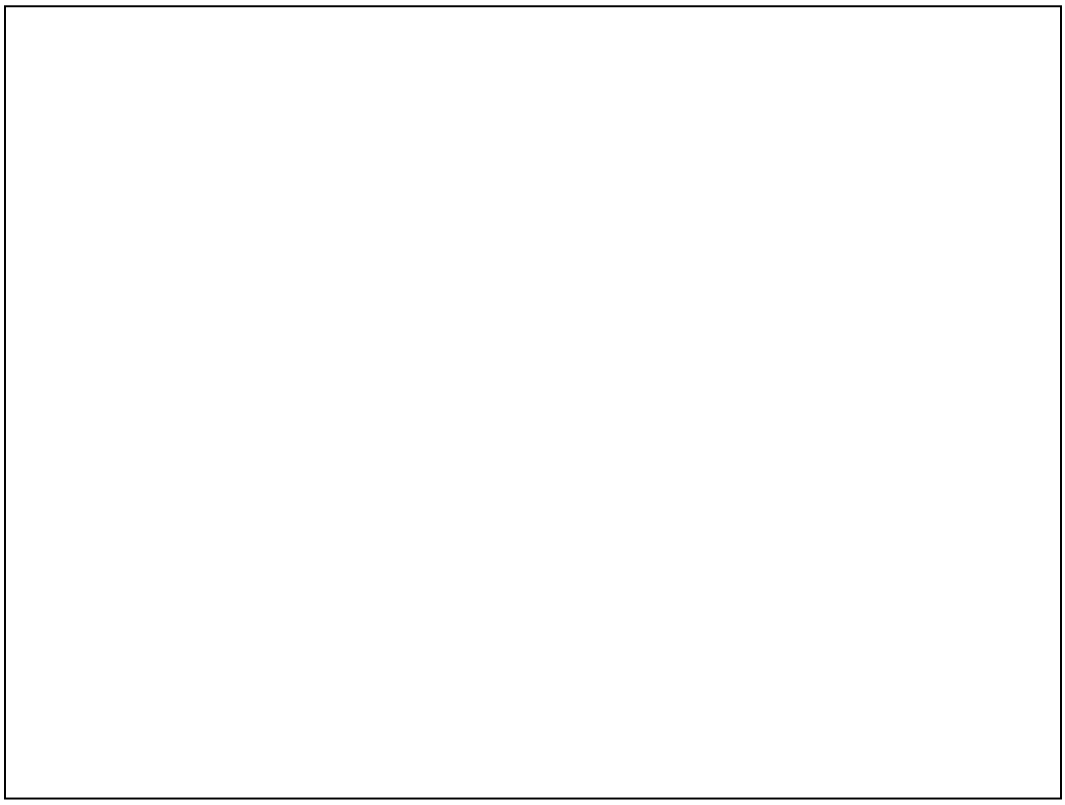


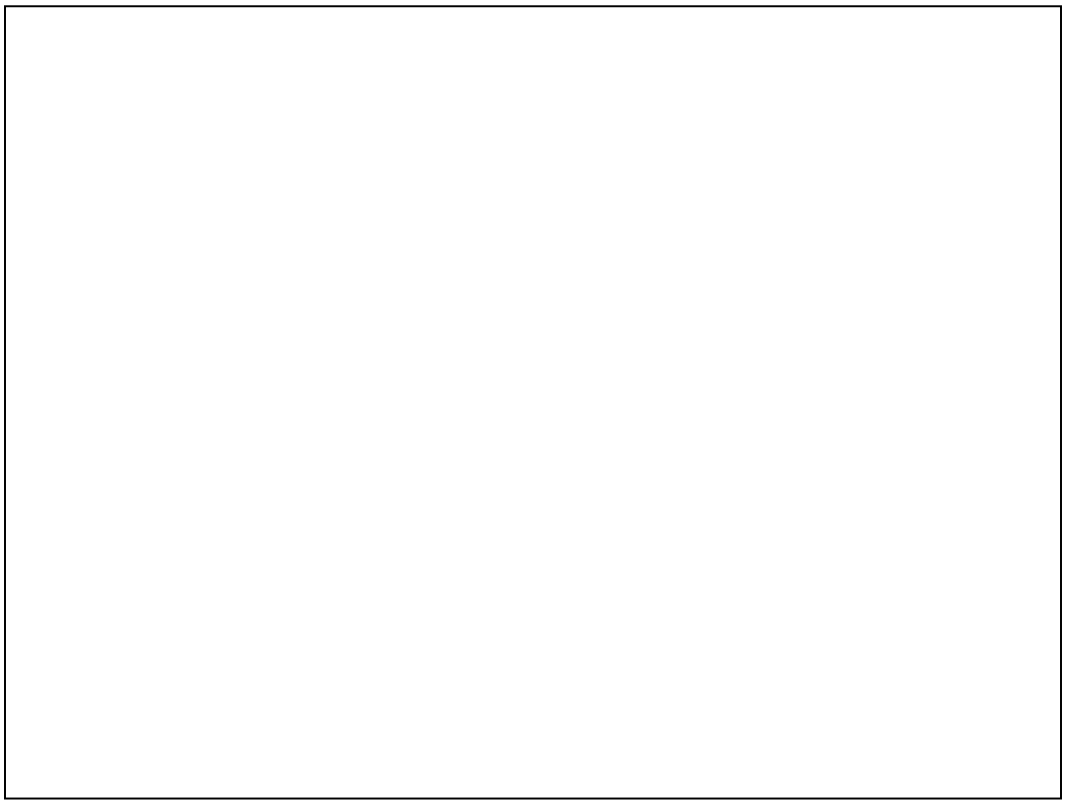


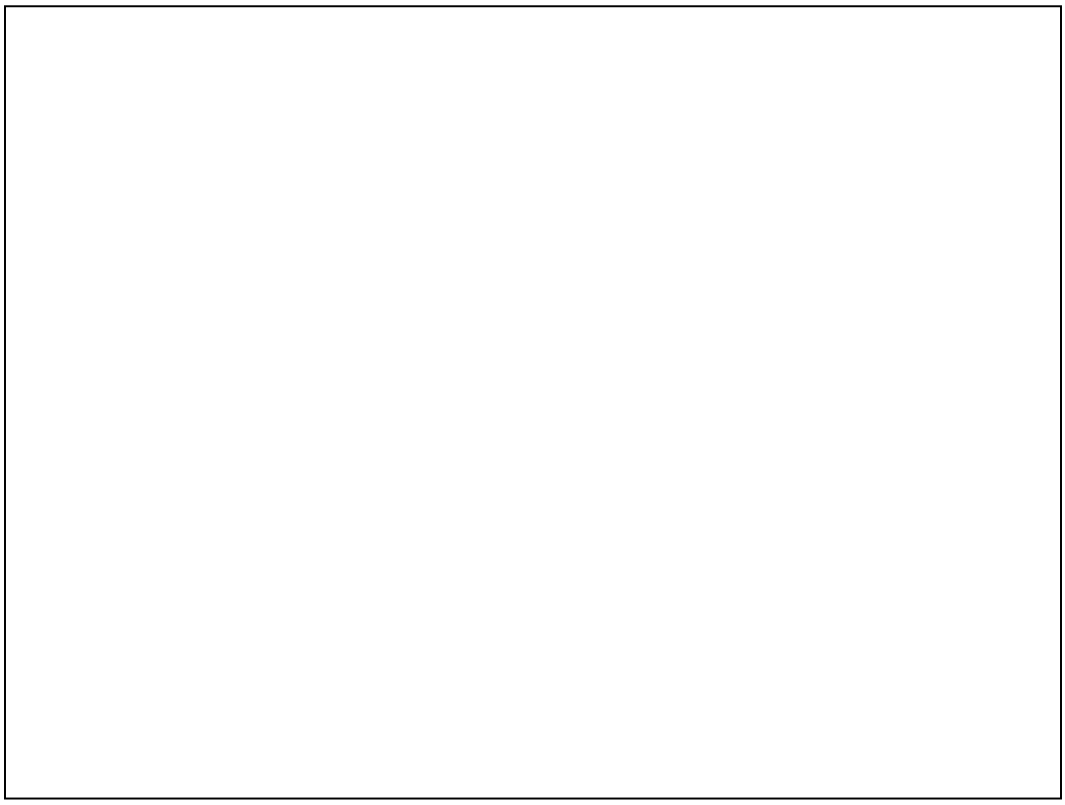


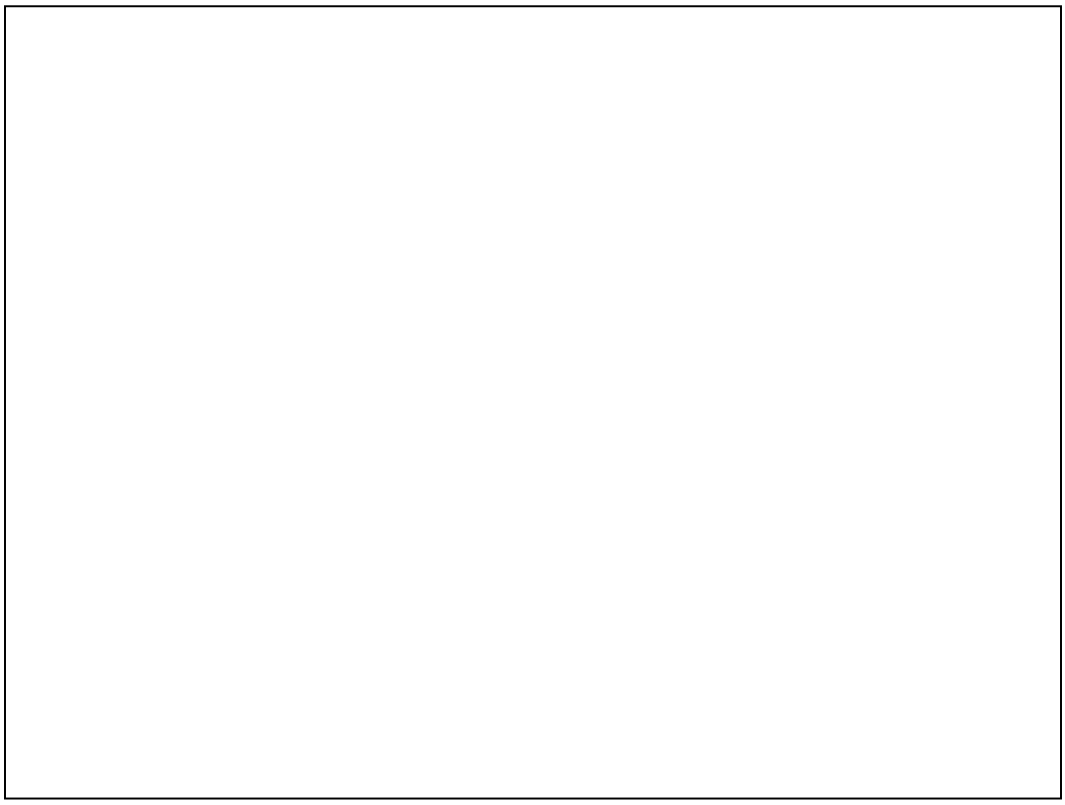


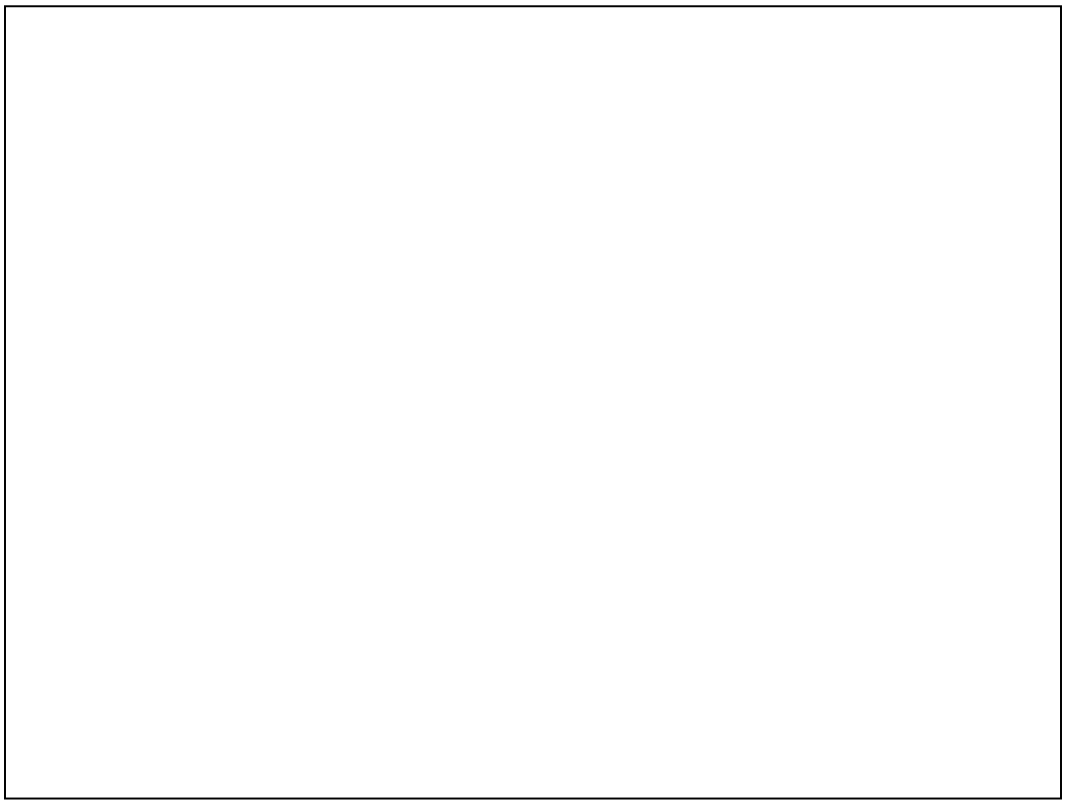


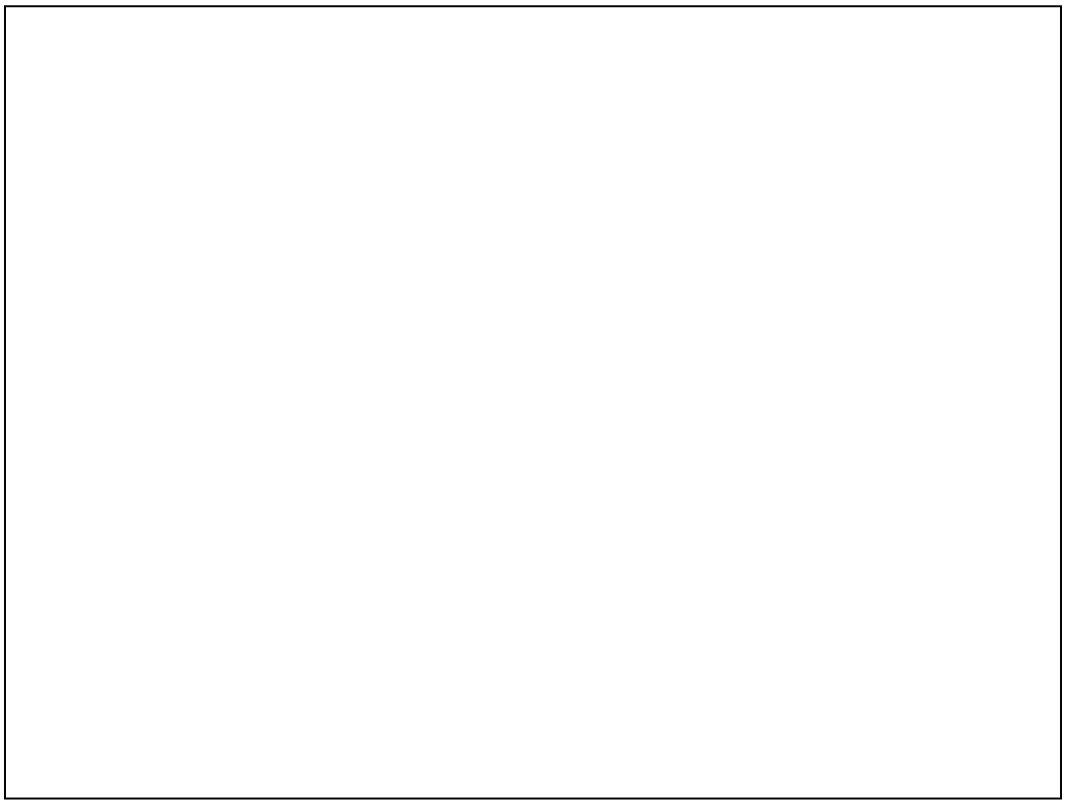


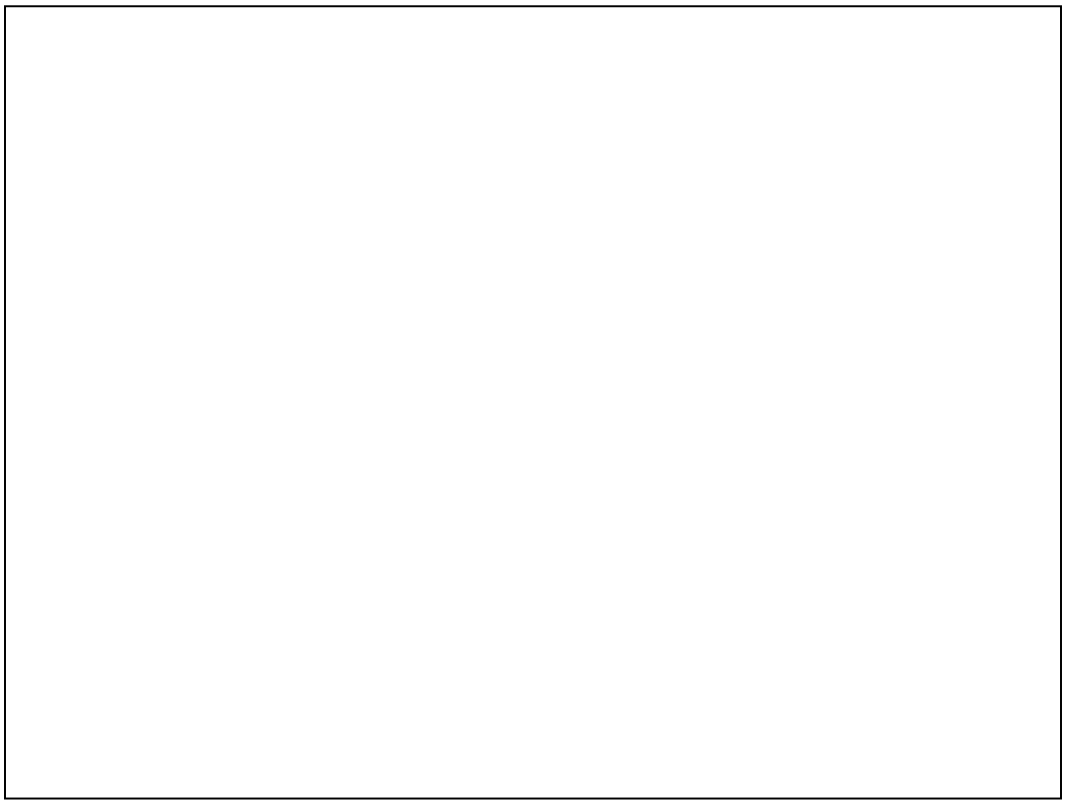


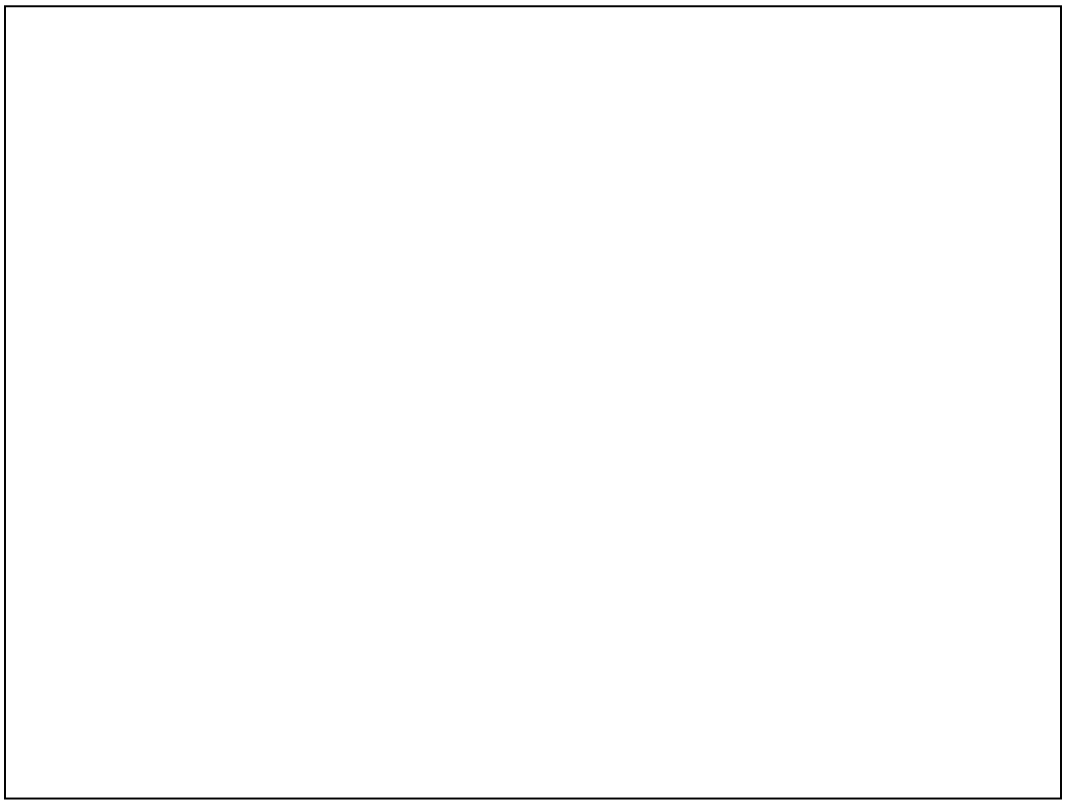






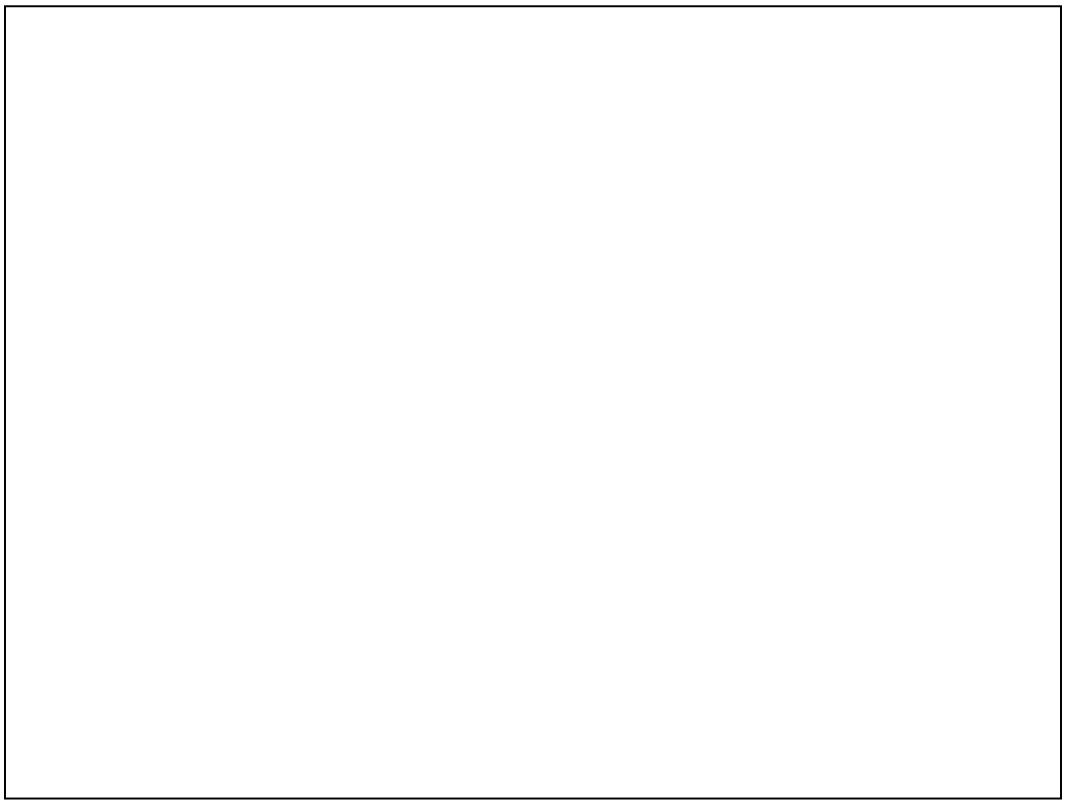


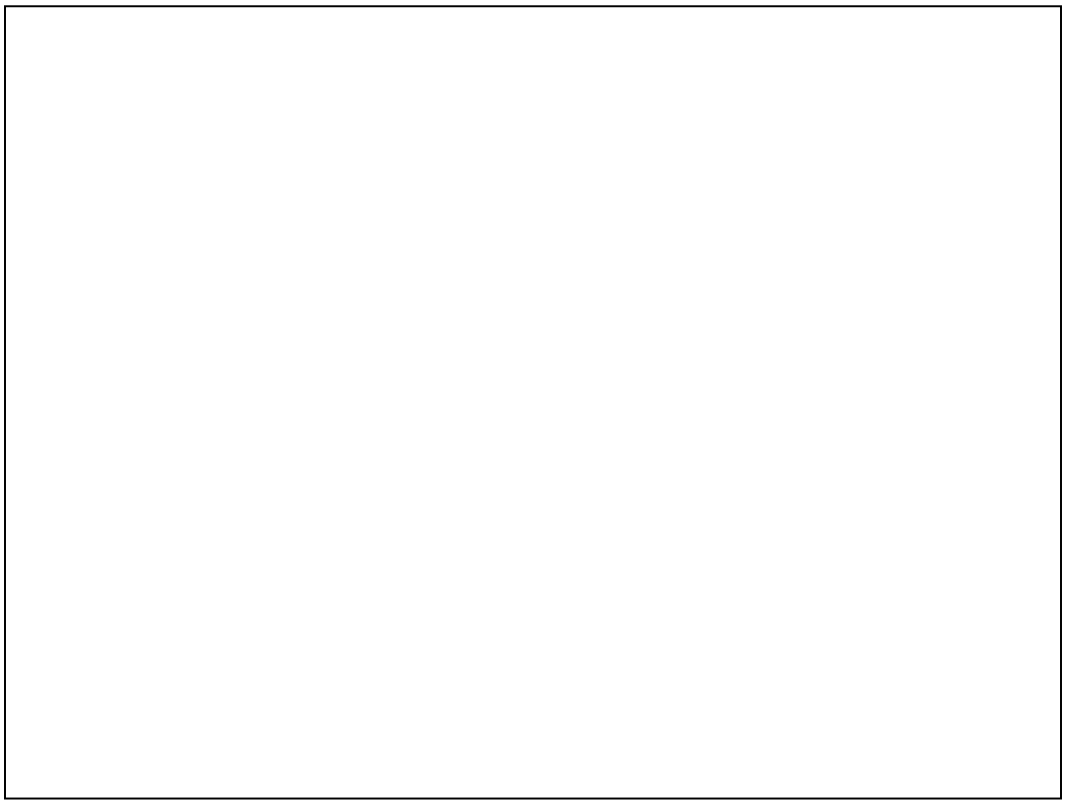




MS08-053: Windows Media Encoder wmex.dll ActiveX Control Buffer

9 Sept 2008





http://blogs.msdn.com/sdl/archive/2008/10/22/ms08-067

About MS08-067