No-Holds Barred Penetration Testing

By Jarrod Loidl

Senior Security Consultant

Dimension Data

No-Holds Barred Penetration Testing

- Who Am I? / Why Am I Presenting?
- Problem Definition
- The Client’s Dilemma
- The Consultant’s Dilemma
- Crossroads
- Solutions

Who Am I?

- Been working in IT security industry since ~2004 (+10 years IT)
- Responsible for conducting and/or co-ordinating penetration testing in various roles since early 2007
- Moved from working in-house to consulting in late 2009

Why Am I Presenting?

Two Reasons:

- I've been the client
- I've been the consultant

I've Been The Client

- Hired (lots of) penetration testers
- Dealt with reports and remediation of findings
- Juggled multiple projects + operational tasks
- Dealt with business stakeholders:
  - delay projects
  - give me money (for security initiatives, features, testing)
  - accept risk

I've Been The Consultant

- The pentests we've done for clients
- Involved in pre-sales
- Discussed service offerings
- Seen what often happens with a typical pentest...

Problem Definition

Problem Definition

- Client side penetration testing means testing the “end user”
- Most people assume perimeter protects them
- Client side penetration testing **shatters** the myth
- Get the users, you get the lot

Problem Definition

- How do we perform client-side penetration testing?
- “Non-conventional methods”
- Information harvesting (who do we want to target to get the access we require?)
- Targeted users, tailored attacks (‘social engineering’)

Problem Definition

How would we perform client-side penetration testing?

- Data mining (e.g. Maltego, LinkedIn, Facebook)
- Browser exploits (via. compromised sites, XSS)
- Desktop applications and plugins:
  - Adobe Acrobat, Java, Flash
- Social Engineering/Phishing (via. email, social networks, USB devices, etc)
- Would you like some 0-day with that?

Problem Definition

How do we do we perform penetration testing today?

- —Use methodologies aiming at identifying
- —configuration weakness,
- —information leakage,
- —poor coding

- We don’t test clients
- We test servers and applications

So why is this a problem?

Problem Definition

Taken from 'Verizon Data Bre

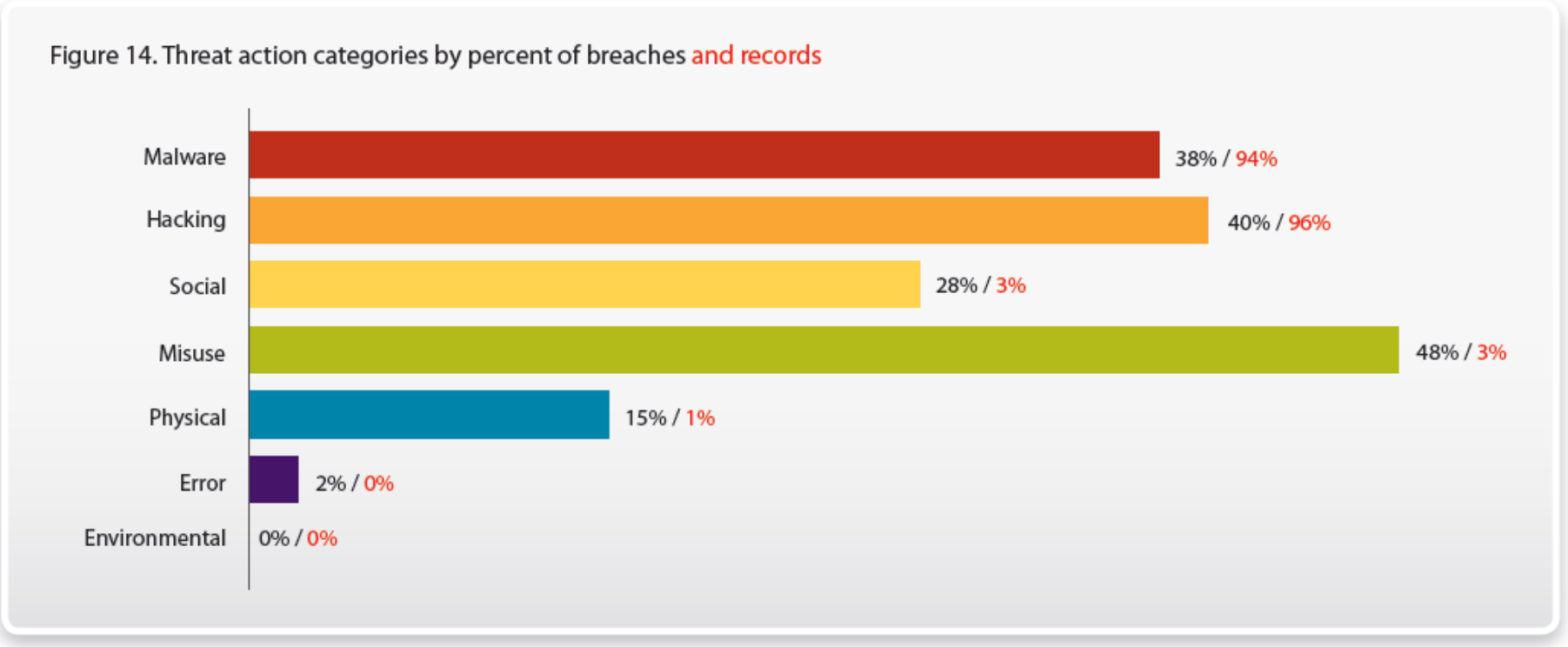
WHO IS BEHIND DATA BREACHES?

- **70%** resulted from external agents (-9%)
- **48%** were caused by insiders (+26%)
- **11%** implicated business partners (-23%)
- **27%** involved multiple parties (-12%)

HOW DO BREACHES OCCUR?

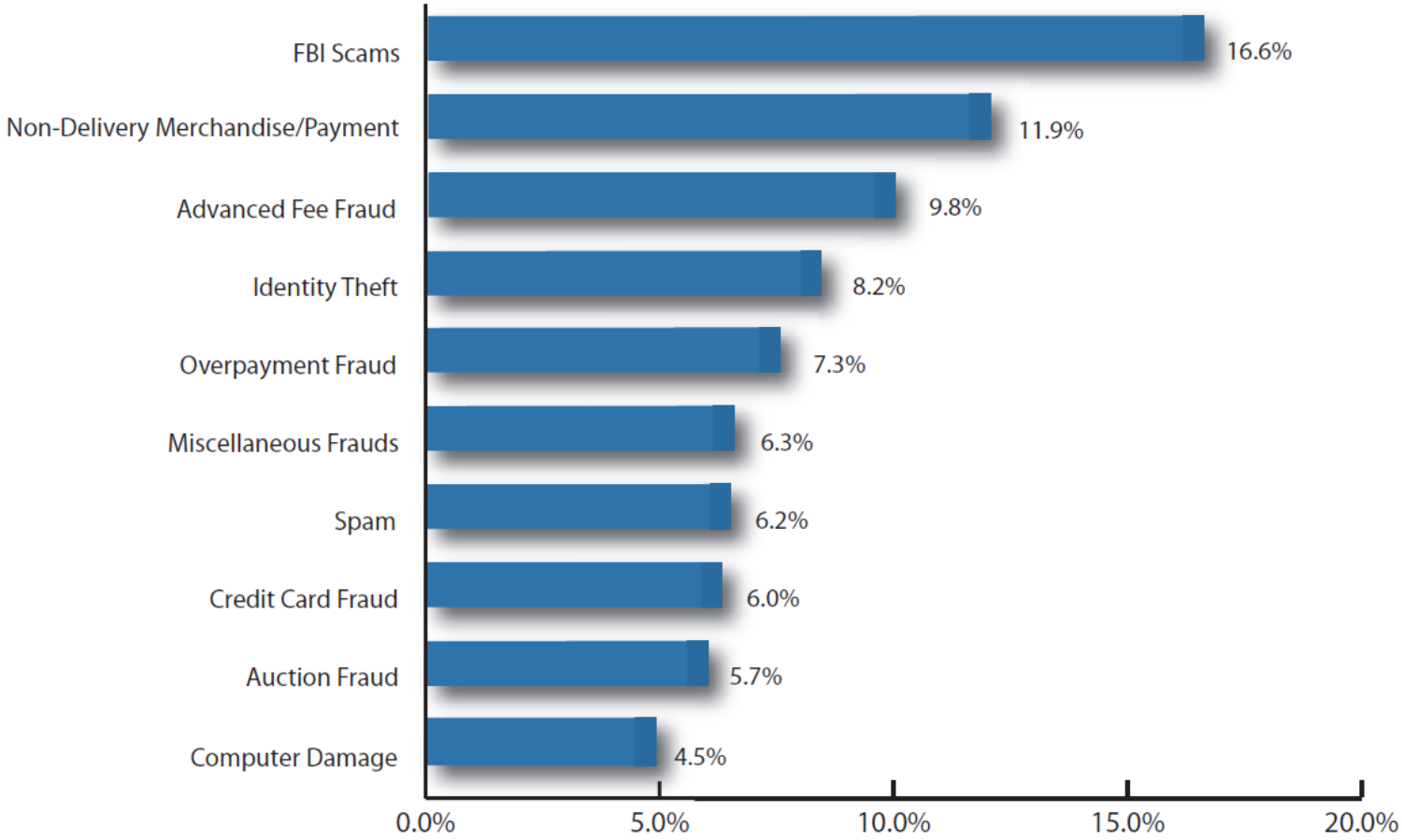
- **48%** involved privilege misuse (+26%)
- **40%** resulted from hacking (-24%)
- **38%** utilized malware (<>)
- **28%** employed social tactics (+16%)
- **15%** comprised physical attacks (+6%)

Problem Definition



Problem Definition

Figure 4: 2009 Top 10 Most Common IC3 Complaint Categories (Percent of Total Complaints Received)



Problem Definition

InSecurity Complex

By Elinor Mills

Starting Nmap 4.76 (htt
Initiating Ping Scan at
Scanning 192.169.1.1 [2
Completed Ping Scan at 1
Read data files from: /u

January 14, 2010 12:37 PM PST

New IE hole exploited in attacks on U.S. firms

by Elinor Mills

Font size Print E-mail Share 92 comments

Tweet

Attackers targeting Google and a host of other U.S. companies recently used software that exploits a new hole in Internet Explorer, Microsoft said Thursday.

"Internet Explorer was one of the vectors" used in the attacks that Google disclosed earlier this week, Microsoft said in a statement. "To date, Microsoft has not seen widespread customer impact, rather only targeted and limited attacks exploiting IE 6," the statement said.

The vulnerability affects Internet Explorer 6, IE 7, and **IE 8** on **Windows 7**, Vista, Windows XP, Server 2003, Server 2008 R2, as well as IE 6 Service Pack 1 on Windows 2000 Service Pack 4, Microsoft said in **an advisory** on Thursday afternoon.

Google disclosed the attacks targeting it and other U.S. companies **on Tuesday** and said the attacks originated in China. Human rights activists who use Gmail also were targeted, Google said.

Problem Definition

- Black Hats are not constrained
  - They have no limitations!
  - Attacks are going on in the wild already
  - See “Why Black Hats Always Win” by Val Smith & Chris
- Also, consultants in other countries do this testing too
- Times are changing and our methods must change with it.

Who *is* doing this **today**?

Problem Definition

Reported by SANS (via. Qualys) - Patchable Application Level Bugs in 2009

- WordPad and Office Text Converters Remote Code Execution Vulnerability (MS09-010)
- Sun Java Multiple Vulnerabilities (244988 and others)
- Sun Java Web Start Multiple Vulnerabilities May Allow Elevation of Privileges(238905)
- Java Runtime Environment Virtual Machine May Allow Elevation of Privileges (238967)
- Adobe Acrobat and Adobe Reader Buffer Overflow (APSA09-01)
- Microsoft SMB Remote Code Execution Vulnerability (MS09-001)
- Sun Java Runtime Environment GIF Images Buffer Overflow Vulnerability
- Microsoft Excel Remote Code Execution Vulnerability (MS09-009)
- Adobe Flash Player Update Available to Address Security Vulnerabilities (APSB09-01)
- Sun Java JDK JRE Multiple Vulnerabilities (254569)
- Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067)
- .... And more.... !!!

Vulnerability Research Trends

Microsoft

Sign in

Security Research & Defense

Information from Microsoft about vulnerabilities, mitigations and workarounds, active attacks, security research, tools and guidance

TechNet Blogs > Security Research & Defense

Posts

Assessing the risk of the October security updates

Tue, Oct 12 2010 by swiblog

Today we released sixteen security bulletins. Four have a maximum severity rating of Critical, ten have a maximum severity rating of Important, and two have a maximum severity rating of Moderate. We hope that the table below helps you prioritize the deployment of the updates appropriately for your environment.

Bulletin	Most likely attack vector	Max Bulletin Severity	Max exploit-ability	Likely first 30 days impact	Platform mitigations and key notes
MS10-071 (IE)	Victim browses to a malicious webpage.	Critical	1	Likely to see a code execution exploit developed for memory corruption vulnerabilities.	Neither IE7 nor IE8 vulnerable to CVE-2010-3326, one of the two Critical issues addressed by this security bulletin.
MS10-076 (EOT)	Victim browses to a malicious webpage.	Critical	1	Likely to see an exploit released for older platforms	ASLR on Windows Vista and later operating systems makes building a successful exploit for code execution much more difficult.
	Victim running 64-bit				

Options

- About
- Email Blog Author
- RSS for Posts
- Subscribe w/ Email Adc OK

Search

Loading...

Archive

October 2010 (3)
September 2010 (7)
August 2010 (7)
July 2010 (3)
June 2010 (5)
May 2010 (2)
April 2010 (4)
March 2010 (1)
February 2010 (5)
January 2010 (4)
December 2009 (2)
November 2009 (4)
October 2009 (8)
September 2009 (7)
August 2009 (4)
July 2009 (10)
June 2009 (9)

Problem Definition

More trends (not just Microsoft to blame)

UBM CRN NEWS, ANALYSIS, AND PERSPECTIV
FOR VARS AND TECHNOLOGY INTEG

HOME | NEWS | SLIDE SHOWS | VIDEO | BLOGS & OP
NETWORKING | SECURITY | CLOUD | STORAGE | APPLICA

Oracle Repairs Flaws In Java, S With 85-Fix Patch

By Stefanie Hoffman, CRN

RELATED: VIDEOS | SLIDE SHOWS | CHANNELCASTS | COMMENTS

Page 1 of 2

Oracle (NSDQ:ORCL) issued 85 fixes in a massive Critical Patch Update, repairing a slew of vulnerabilities in both its Sun and Java product lines, many of which could enable malicious hackers to launch remote code execution attacks on users' systems.

Thirty-one of the 85 fixes were for Oracle's newly acquired Sun products, which included OpenSolaris, Open Office, Sun Convergence, Sun Directory Server and Enterprise Edition. Of the Sun patches, 16 repaired vulnerabilities that could be exploited remotely by hackers, while some of the most critical vulnerabilities fixed by the patch affected OpenOffice, Solaris and OpenSolaris.

Specifically, the CPU included five new fixes for OpenOffice, repairing serious vulnerabilities that received at least a 9.3 on Oracle's Common Vulnerability Scoring System, which indicate that

Adobe | Products | Industries | Learning | Help | Downloads | Company | Store

Home / Support / Security advisories /

Security bulletin

Security updates available for Adobe Reader and Acrobat

Release date: October 5, 2010

Vulnerability identifier: APSB10-21

CVE Numbers: CVE-2010-2883, CVE-2010-2884, CVE-2010-2887, CVE-2010-2888, CVE-2010-2889, CVE-2010-2890, CVE-2010-3619, CVE-2010-3620, CVE-2010-3621, CVE-2010-3622, CVE-2010-3623, CVE-2010-3624, CVE-2010-3625, CVE-2010-3626, CVE-2010-3627, CVE-2010-3628, CVE-2010-3629, CVE-2010-3630, CVE-2010-3631, CVE-2010-3632, CVE-2010-3656, CVE-2010-3657, CVE-2010-3658

Platform: All Platforms

SUMMARY

Critical vulnerabilities have been identified in Adobe Reader 9.3.4 (and earlier versions) for Windows, Macintosh and UNIX, Adobe Acrobat 9.3.4 (and earlier versions) for Windows and Macintosh, and Adobe Reader 8.2.4 (and earlier versions) and Adobe Acrobat 8.2.4 (and earlier versions) for Windows and Macintosh. These vulnerabilities, including CVE-2010-2883, referenced in Security Advisory APSA10-02, and CVE-2010-2884 referenced in the Adobe Flash Player Security Bulletin APSB10-22, could cause the application to crash and could potentially allow an attacker to take control of the affected system

Problem Definition

Symantec Internet Security Threat Report 2009 :

"The top Web-based attack in 2009 was associated with ***malicious PDF activity****, which accounted for* ***49 percent of the total****."*

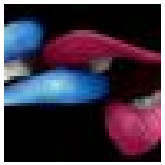
Problem Definition

Plenty of ways to trick end users…

Latest: take your free movie star porn in facebook http://www.free s/facebook.html

1 day ago via web

Taker



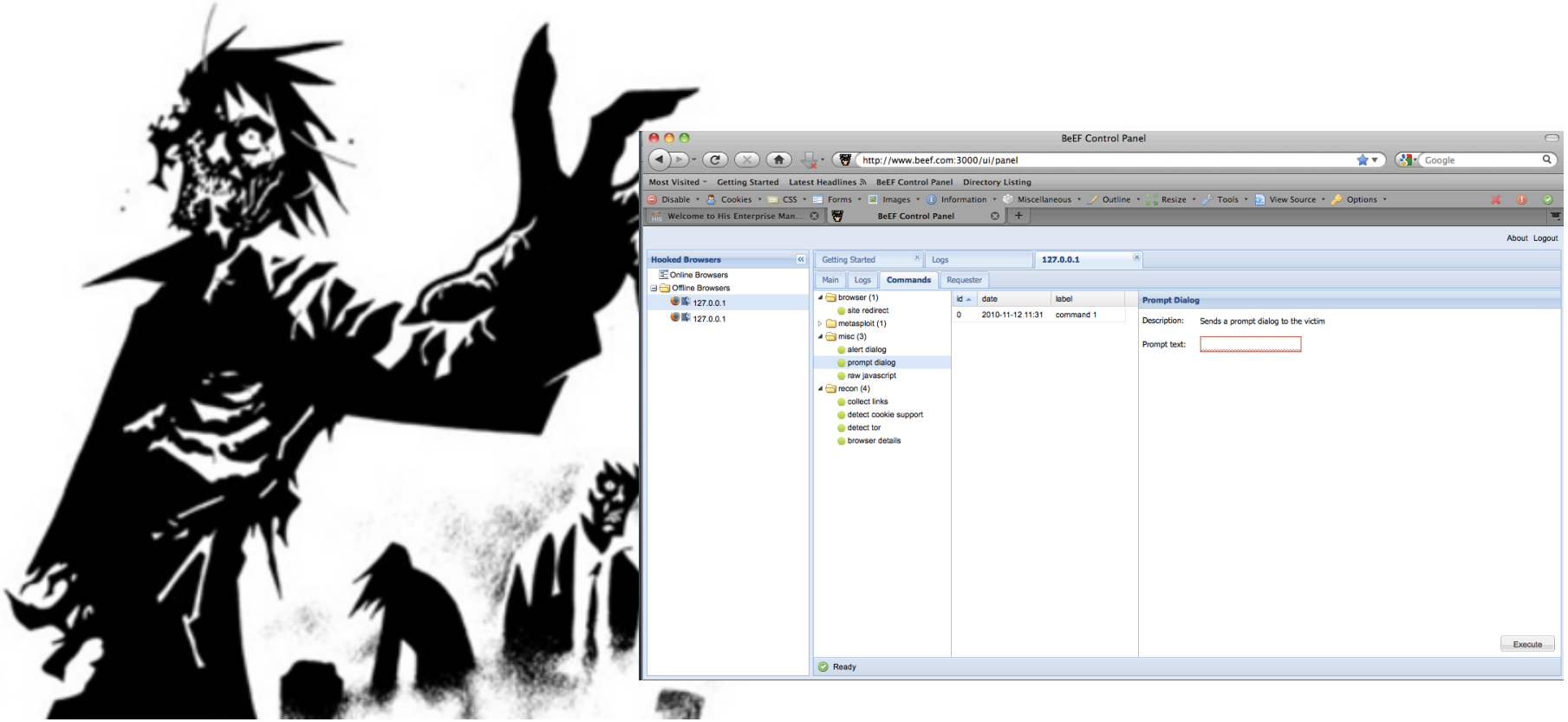
: http://www.free 2010/Proxybreaker.exe

4 days ago via web

: best proxi http://www.free 007/proxi.exe

4 days ago via web

Browser Attacks! The Day of the Zombie



Problem Definition

Security = *people* + *process* + technology

Problem Definition

Why do we perform penetration tests?

- *Provide assurance*
- Validate security (design/requirements/model)
- Satisfy legal/regulatory/governance requirements
- Know whats “unknown”
  - (e.g. Common-Off-The-Shelf software or old legacy applications)

Problem Definition

Why is client-side penetration testing out of scope? (Reasons/excuses)

- Client doesn’t want to test clients
- Consultant doesn’t want to test clients

Problem Definition

Why is client-side penetration testing out of scope? (cont.)

- Don’t need client side exploits to pwn:
  - Weak passwords,
  - Configuration errors,
  - Patching,
  - Insecure coding
- Risky to both parties

Problem Definition

Result?

- Clients gets detailed report of *exactly* what they're after
- Consultant gets paid and develops good rapport with the client
- Findings *may* get fixed....

Problem Definition

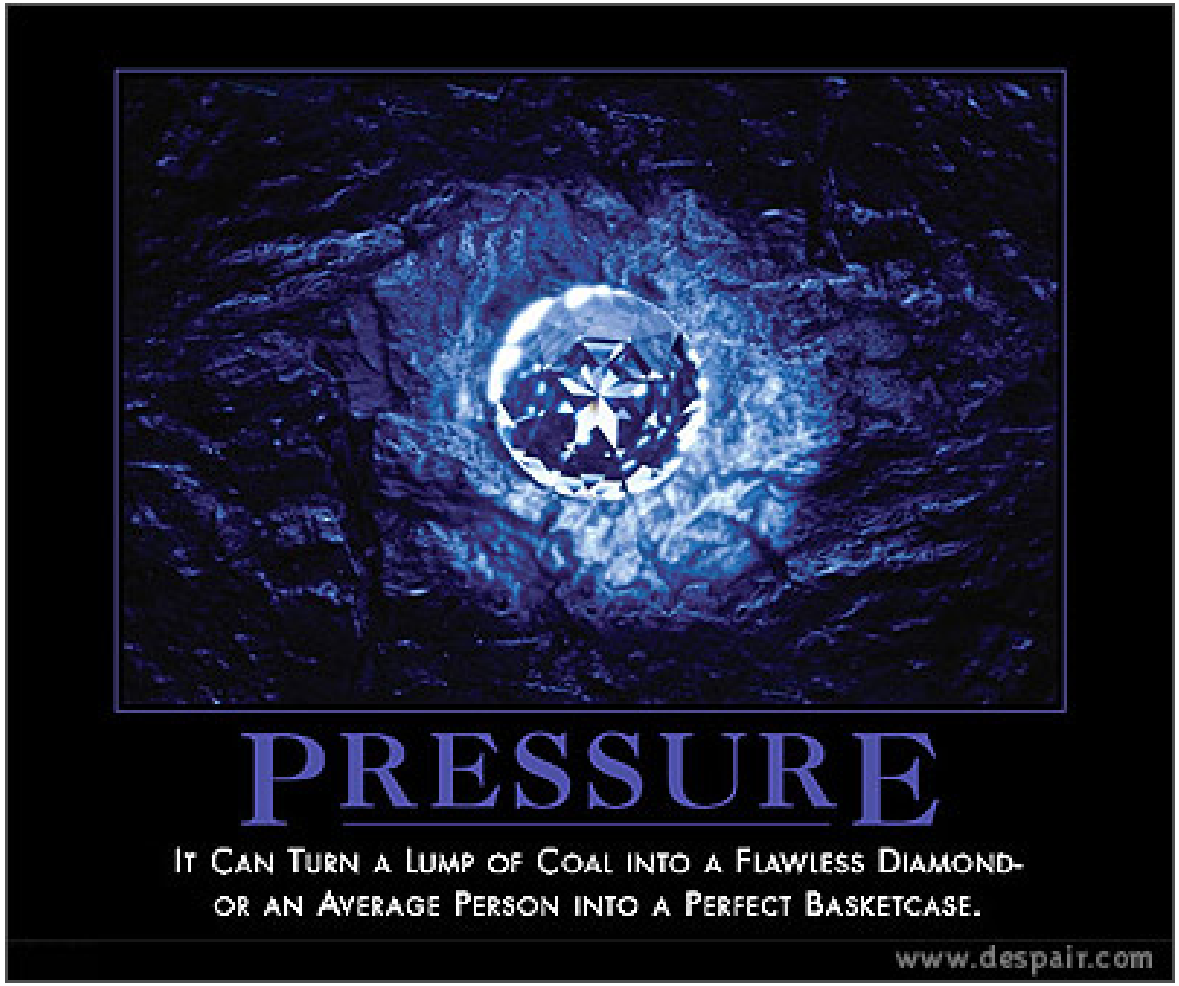
- Unfortunately, the end users (the other “clients”) are not being tested:
- Security model there is the weakest:
  - Many run with admin rights
  - Stored passwords in the browser
  - Non standard machines
  - Unfettered internet connectivity
  - Flat networks

To summarise….

Problem Definition

1. We know that client-side software vulnerabilities are the focus in research
2. We know that attack trends are focusing on exploiting these vulnerabilities
3. Despite knowing this… we don't test them.
4. We know our client's aren't defending themselves adequately.

The Client's Dilemma



The Client’s Dilemma

- Clients don’t want to test the end user tested:
- More interested in the new application/project/ service
- Less interested in the users - they know will fail
- Prefer not to know... (have enough unsolvable problems)

The Client's Dilemma

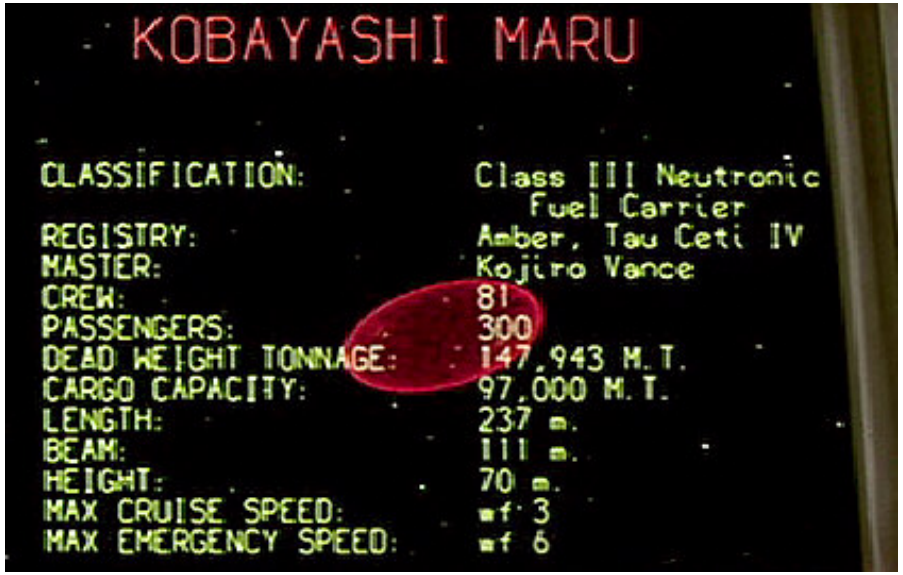
Client's know the recommendations will feature "impossible to implement" recommendations:

- Segment network
- Lock down desktops/ implement SOE / revoke admin rights
- Whitelist applications
- Restrict/proxy Internet connectivity
- Change password policy
- User Awareness Training

The Client's Dilemma

What is an "Impossible Recommendation" ?

1. *When the solution cannot be implemented by the client regardless of reason*
2. *When the solution creates a bigger problem*



The Client's Dilemma

Why can't the client implement them?

- "Our network is too complex to unflatten"
- "We only have budget to test this project"
- "This will application break if we upgrade IE6!"
- "Too many legacy applications rely on old password policy and its hardcoded"
- "CEO has accepted the risk"

The Consultant’s Dilemma

The Consultant's Dilemma

It's complicated:

- Reconnaisance time blows out significantly
  - Research company
  - Research staff
  - Pick your target
- Testing also takes longer
  - Tailor attack to the target
  - Known exploit vs 0-day?
  - Cleanup

The Consultant's Dilemma

It's complicated (cont.):

- By choosing to test the end-user, you risk reducing the time spent searching for other vulnerabilities

Methodology vs ad-hoc approaches

- This is a big trade-off and can greatly affect the end result for the client.

The Consultant's Dilemma

It's risky:

- There are laws against pre-texting
- Potential violations for the affected user
  - End user's machine *belongs to the end user* and not your client?
  - Did you just break the law if the end user didn't give his consent?
- Outcomes aren't always desirable....

The Consultant’s Dilemma

Result?

- Diminishing value/trade-off for the client
- Harder sell
- Risky business for the consultant
- Potentially costlier if the scoping is wrong.

The Crossroads

The Crossroads

Ok – so we need to change things. But HOW?

Solutions – For The Client

- Start requesting client side penetration tests from your consultants!
  - Consultants respond to client demand
- When to request them:
  - External Perimeter Testing
  - When you know the external perimeter is already locked down
  - Annual security review

Solutions – For The Client

- Pick a project and ride the wave
  - Find a project you can get the budget attached to
- Who are your business champions?
  - Who can give you money?
  - Will they give it to you?
  - If not, can you raise the risk profile to a higher level?

Solutions – For The Client

Learn to sell security!!!

- Why do you need money
- What is the business benefit

Authorisation for non-company owned machines

- Updated security policy to cover non-company owned assets connected to the network
- Third Party Agreements

Solutions – For The Consultant

Present client-side pentests as an “option”

- Doesn’t have to be all the time;
- Suggest them for annual pentests (did you learn from last year?);

Special clients

- “Nothing can hack us!” / “*Orly?*”
- Appeal to EGO!

Solutions – For The Consultant

Pre-empt the client's questions

- Deal with your internal legal team
- Service Agreements and Statements of Work

Be prepared!

- Have a methodology prepared for these sorts of tests

Solutions – For The Consultant

Learn to sell security better!

- Q: Why should I test the end user client?
- A: Recommendations will encourage your businesses to focus defense-in-depth strategies which deal with “real world” attacks

Check and DOUBLE CHECK you have the client machine

Final Thoughts

The take away message is:

- Start thinking of ***how*** we can perform client side penetration testing, rather than why we ***can't***.
- Intelligent solutions appear when we ask ourselves intelligent questions.

Questions?

Thanks to:

- Jaco Van Heerden, Wynand Viljoen, Ben Mosse, Andrew Dragatsikas.

Special Thanks to:

- The Security LOB @ DD,
- My family.