Into the Darkness: Dissecting Targeted Attacks

Rodrigo Rubira Branco (@bsdaemon)
Director Vulnerability & Malware Research
Qualys, Inc.
Troopers – March/2012

- Adobe Reader X Code Execution
- 13 Adobe Shockwave Code Execution
- 2 Microsoft Office Excel Code Execution
- Microsoft Word Code Execution
- Internet Explorer Code Execution
- 2 Solaris 10 Remote Code Execution
- 3 AIX 5 Remote Code Execution
- 3 HP-UX 11.11 Remote Code Execution
- CUPS Remote Code Execution (All *BSD/Linux)
- Apple Quicktime Remote Code Execution
- 4 Vulnerabilities in MacOS X (Remote and Local)

Since three years ago in Troopers…

I start from the end ;)

wmic OS Get DataExecutionPrevention_Available
wmic OS Get DataExecutionPrevention_Drivers

6685-8924-9131-1651-931… the last digit is in the last slide…

APT

APT

Advanced Persistent Threat

APT

~~Advanced Persistent~~ Threats

ASIAN Pacific

Sony: Data breach is sophisticated attack

May 05, 2011 | By Joelle Tessler, Associated Press

Kazuo Hirai defended Sony's handling of breach. (Associated Press)

WASHINGTON - The data breach of Sony's PlayStation Network resulted from a "very carefully planned, very professional, highly sophisticated criminal cyber attack designed to steal personal and credit-card information for illegal purposes," a Sony executive says.

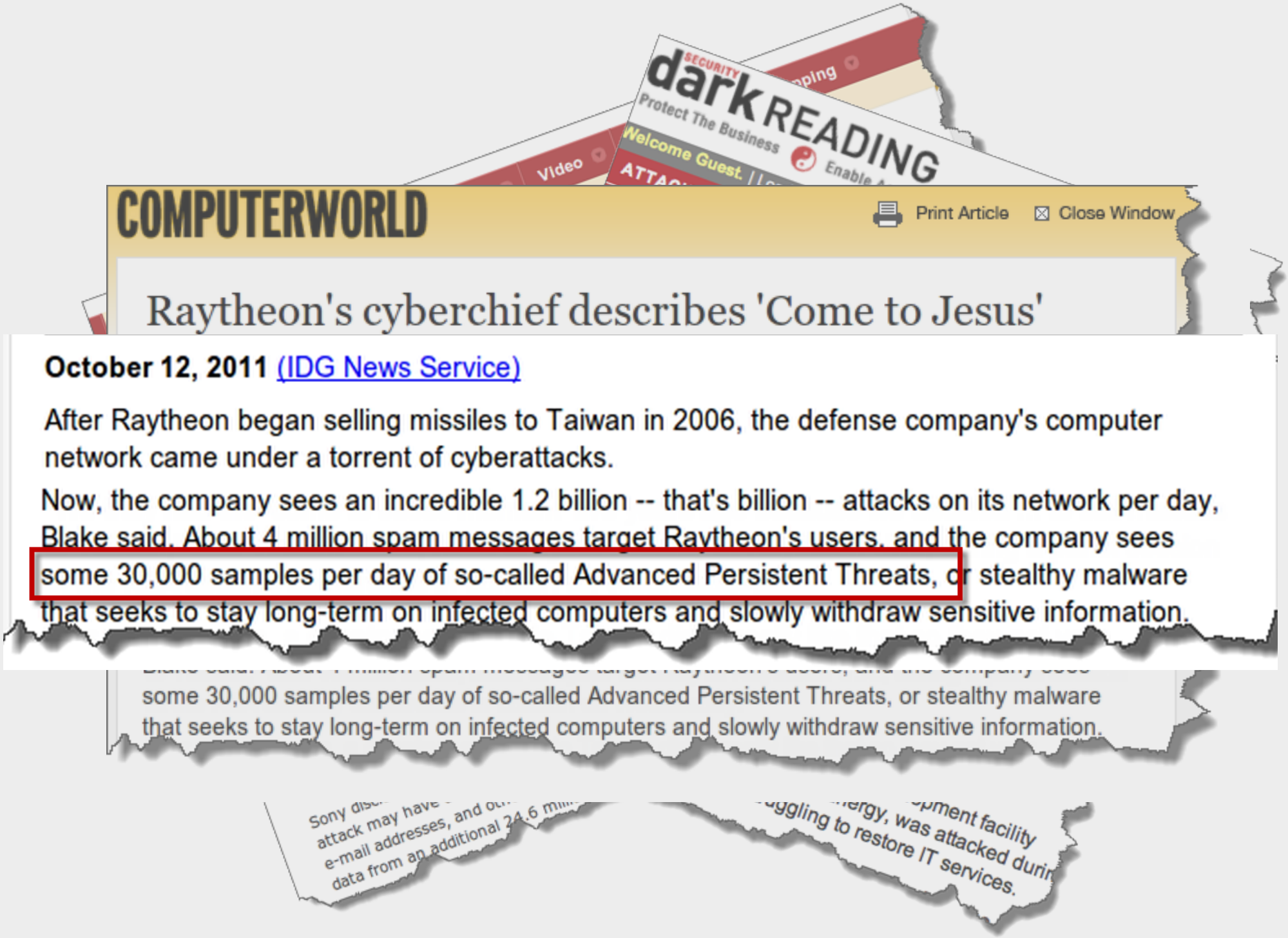
In a letter to members of the House Commerce Committee released Wednesday, Kazuo Hirai, chairman of Sony Computer Entertainment America L.L.C., defended the company's handling of the breach.

Sony disclosed the problem last week. It said the attack may have compromised credit-card data, e-mail addresses, and other personal information from 77 million user accounts. On Monday, Sony said data from an additional 24.6 million online gaming accounts also may have been stolen.


Business
Business Wires
Restaurants & Food
Highest-Paid CEOs
Living
Top Workplaces
Video
Sony: Data breach is sophi
attack
May 05, 2011 | By Joelle Tessler, Associated Pr
WASHINGTON - The data breach of So
PlayStation Network resulted from a
carefully planned, very professiona
sophisticated criminal cyber atta
steal personal and credit-card
illegal purposes," a Sony ex
In a letter to members
Committee released
chairman of Sony
America L.L.C., defend
of the breach.
Sony disclosed the problem las
attack may have compromised cred
e-mail addresses, and other personal
data from an additional 24.6 million online
SECURITY
darkREADING
Protect The Business
Enable Access
Welcome Guest. | Log In | Register | Membership Benefits
ATTACKS / BREACHES
VULNERABILITIES
APPLICATION
SECURITY MANAGEMENT
STORAGE SECURITY
ENCRYPTION
E-mail this page | Print this page |
BOOKMARK
'Sophisticated Cyberattack' Hits Pacific Northwest National Lab
Energy Department research facility's website down; employees still unable to access email
Jul 06, 2011 | 10:18 PM | 0 Comments
By Tim Wilson
Pacific Northwest National Labs, a research and development facility operated under contract to the Department of Energy, was attacked durin the long holiday weekend and is still struggling to restore IT services.


SECURITY
dark READING
Protect The Business
Welcome Guest.
Enable
Video
COMPUTERWORLD
Print Article
Close Window
Raytheon's cyberchief describes 'Come to Jesus' moment
A rash of attacks following missile sales to Taiwan prompted a major cybersecurity review
Jeremy Kirk
October 12, 2011 (IDG News Service)
After Raytheon began selling missiles to Taiwan in 2006, the defense company's computer network came under a torrent of cyberattacks.
Now, the company sees an incredible 1.2 billion -- that's billion -- attacks on its network per day, Blake said. About 4 million spam messages target Raytheon's users, and the company sees some 30,000 samples per day of so-called Advanced Persistent Threats, or stealthy malware that seeks to stay long-term on infected computers and slowly withdraw sensitive information.
attack may have
e-mail addresses, and
data from an additional
facility
was attacked
to restore IT services.


SECURITY
dark READING
Protect The Business
Welcome Guest.
Video
COMPUTERWORLD
Print Article
Close Window
Raytheon's cyberchief describes 'Come to Jesus' moment
A rash of attacks following missile sales to Taiwan prompted a major cybersecurity review
Jeremy Kirk
October 12, 2011 (IDG News Service)
After Raytheon began selling missiles to Taiwan in 2006, the defense company's computer network came under a torrent of cyberattacks.
Now, the company sees an incredible 1.2 billion -- that's billion -- attacks on its network per day, Blake said. About 4 million spam messages target Raytheon's users, and the company sees some 30,000 samples per day of so-called Advanced Persistent Threats, or stealthy malware that seeks to stay long-term on infected computers and slowly withdraw sensitive information.
attack may have
e-mail addresses, and
data from an additional
facility
was attacked
to restore IT services.


dark READING
Protect The Business
Welcome Guest.
Video
COMPUTERWORLD
Print Article
Close Window
Raytheon's cyberchief describes 'Come to Jesus'
October 12, 2011 (IDG News Service)
After Raytheon began selling missiles to Taiwan in 2006, the defense company's computer network came under a torrent of cyberattacks.
Now, the company sees an incredible 1.2 billion -- that's billion -- attacks on its network per day, Blake said. About 4 million spam messages target Raytheon's users, and the company sees some 30,000 samples per day of so-called Advanced Persistent Threats, or stealthy malware that seeks to stay long-term on infected computers and slowly withdraw sensitive information.
some 30,000 samples per day of so-called Advanced Persistent Threats, or stealthy malware that seeks to stay long-term on infected computers and slowly withdraw sensitive information.
attack may have
e-mail addresses, and
data from an additional
facility
was attacked
IT services.

To APT or not to APT?

Infection

Case Study

Case Study
RSA

Between the Lines

Larry Dignan, Andrew Nusca and Rachel King

EMC: RSA was hit with sophisticated attack, SecurID data lifted

By Larry Dignan | March 18, 2011, 5:03am PDT

EMC said that its RSA unit was hit with a "sophisticated cyber attack" that swiped information related to

Attack Vector

Attack Vector
E-Mail

Target

Target

APT?

The Attack

E-Mail

Anatomy of an Attack

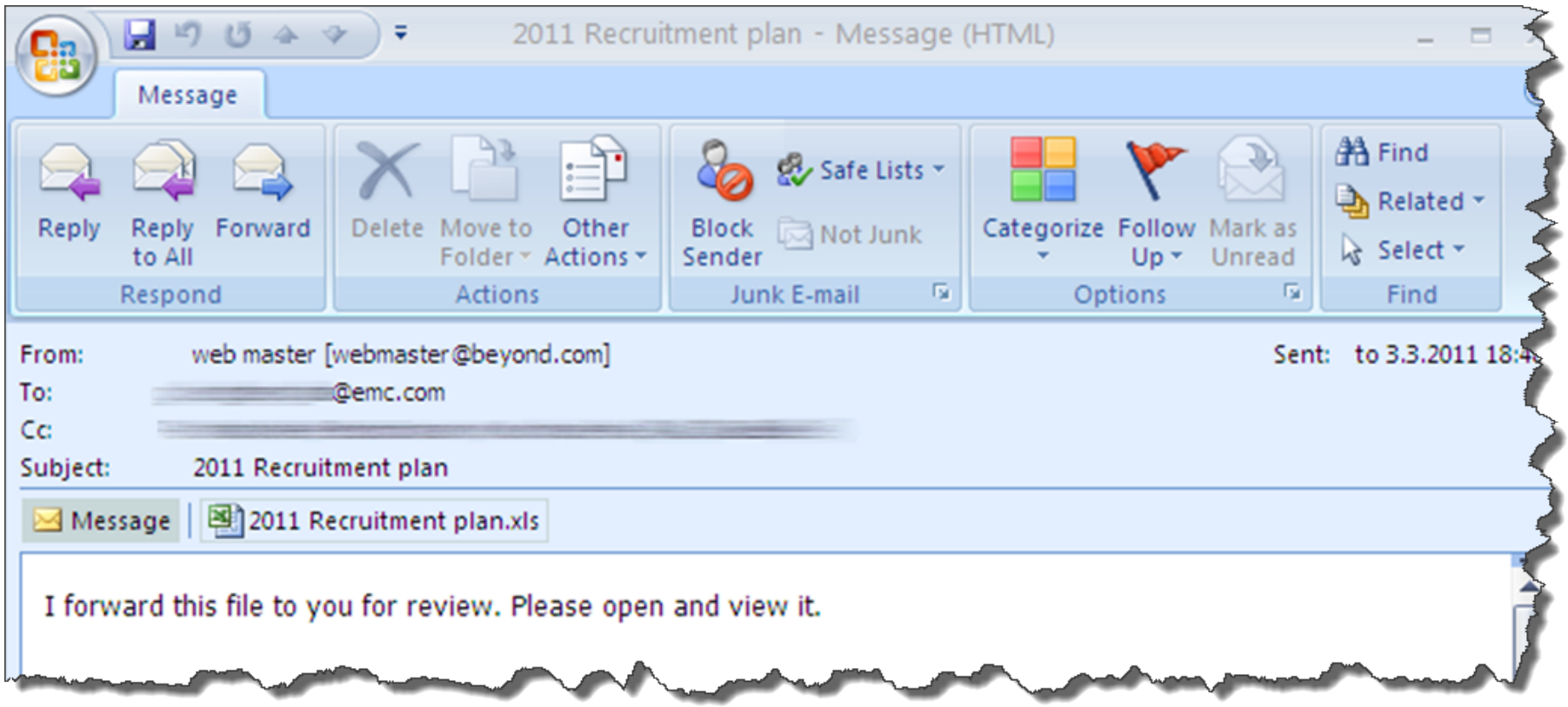
Written on April 1, 2011 by Uri Rivner Comments (40)

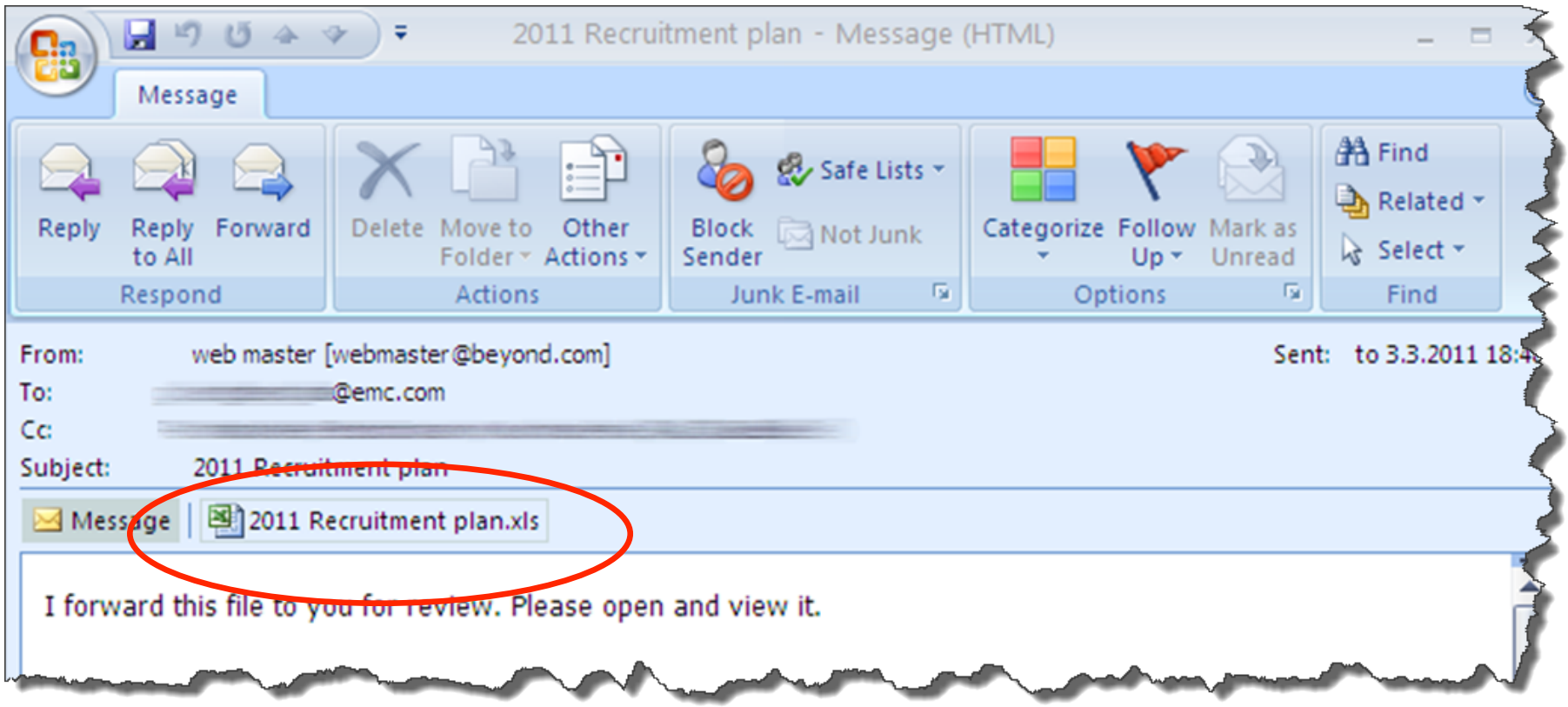
I was on a tour in Asia Pacific when I first heard the **news** about the attack. The investigation into this attack continues but I'm eager to share some information with you about it.

The attacker in this case sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan."

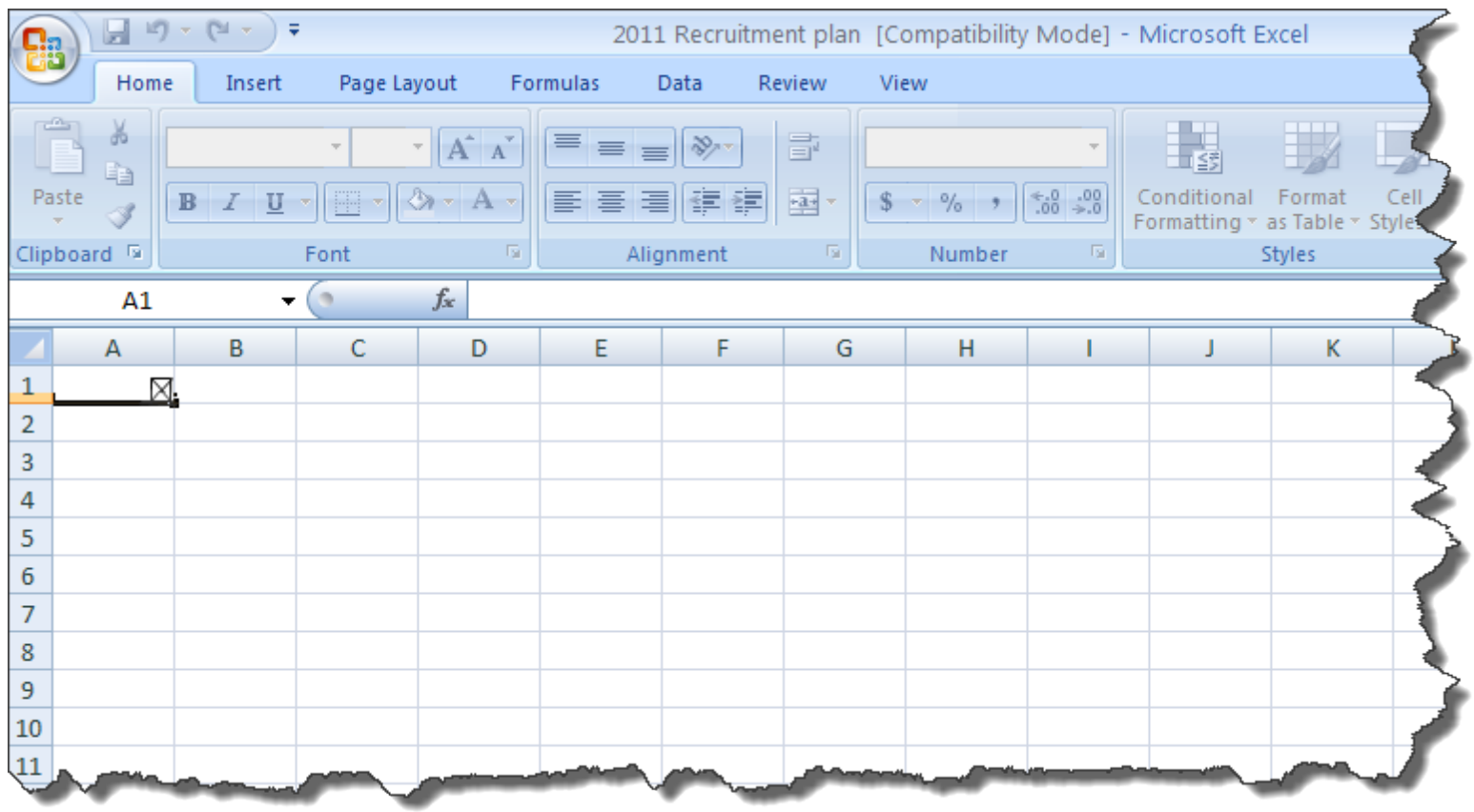
The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls.

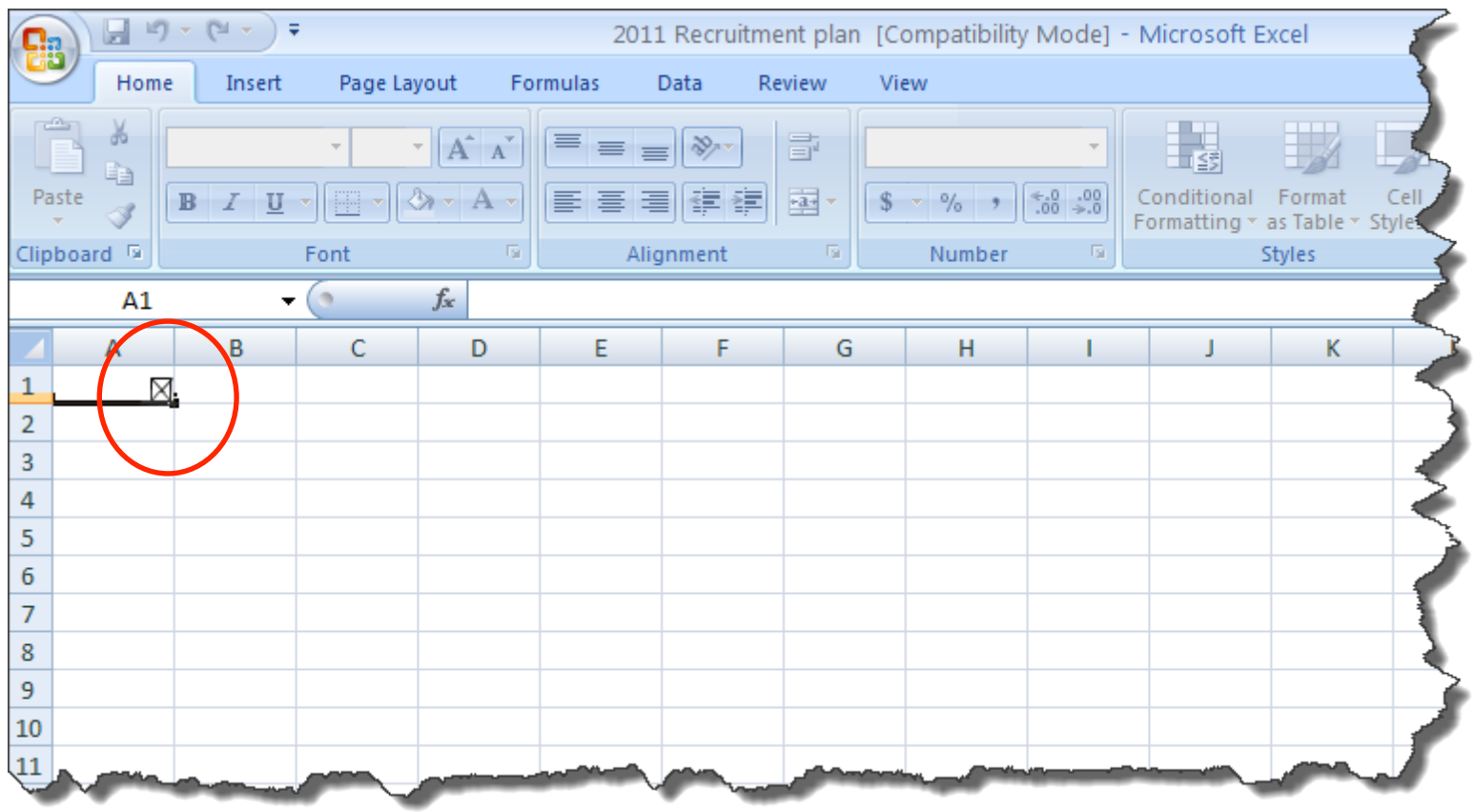
The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609). As a side note, by now Adobe has released a **patch** for the zero-day, so it can no longer be used to inject malware onto patched machines.

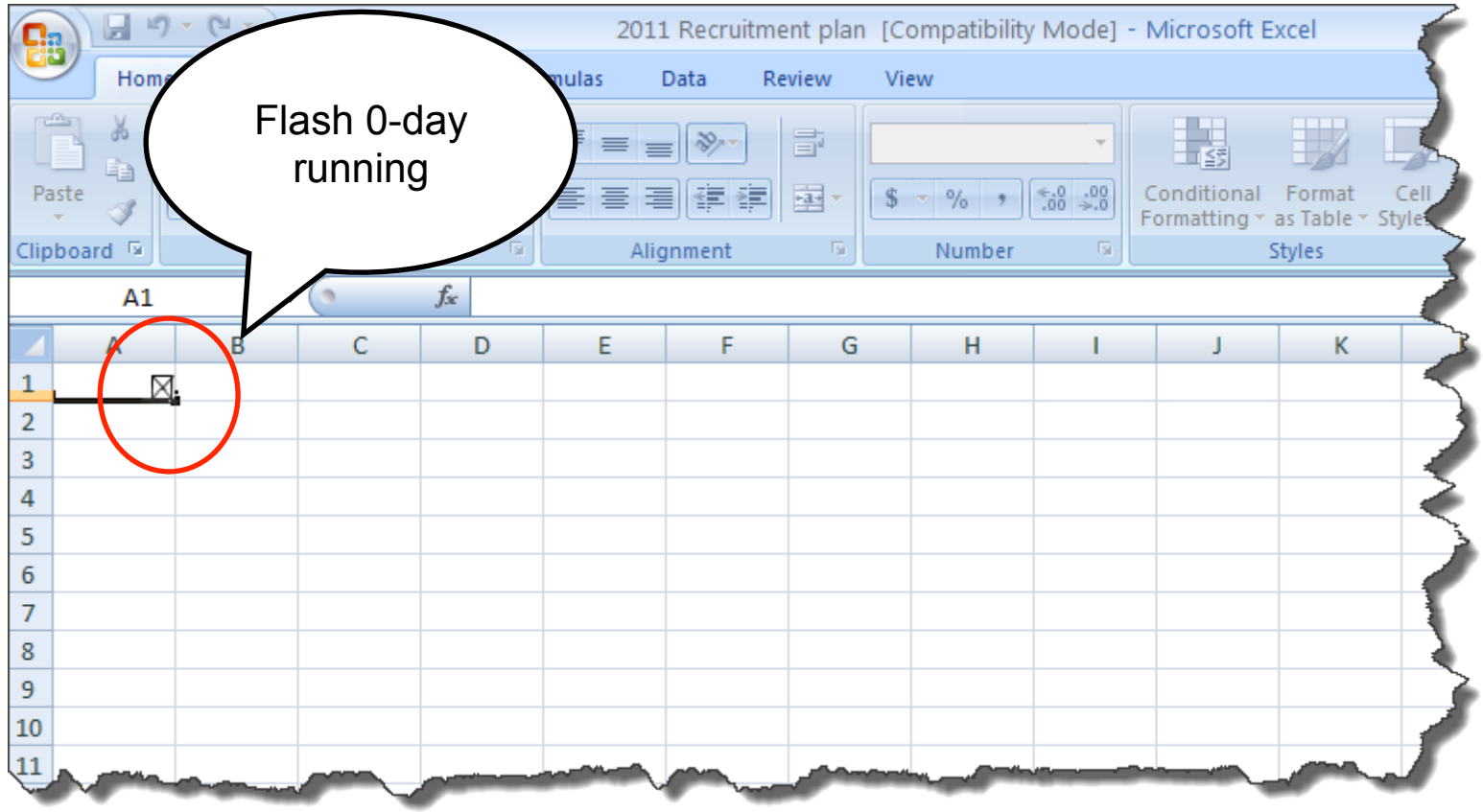

2011 Recruitment plan - Message (HTML)
Message
Reply
Reply to All
Forward
Respond
Delete
Move to Folder
Other Actions
Actions
Block Sender
Safe Lists
Not Junk
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
Related
Select
Find
From: web master [webmaster@beyond.com]
Sent: to 3.3.2011 18:4
To: @emc.com
Cc:
Subject: 2011 Recruitment plan
Message
2011 Recruitment plan.xls
I forward this file to you for review. Please open and view it.


2011 Recruitment plan - Message (HTML)
Message
Reply
Reply to All
Forward
Respond
Delete
Move to Folder
Other Actions
Actions
Block Sender
Safe Lists
Not Junk
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
Related
Select
Find
From: web master [webmaster@beyond.com]
Sent: to 3.3.2011 18:4
To: @emc.com
Cc:
Subject: 2011 Recruitment plan
Message
2011 Recruitment plan.xls
I forward this file to you for review. Please open and view it.

The Attachment


2011 Recruitment plan [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Clipboard
Font
Alignment
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
A1
A B C D E F G H I J K
1 2 3 4 5 6 7 8 9 10 11


2011 Recruitment plan [Compatibility Mode] - Microsoft Excel
Home
Insert
Page Layout
Formulas
Data
Review
View
Paste
Clipboard
Font
Alignment
Number
Conditional Formatting
Format as Table
Cell Styles
Styles
A1
A
B
C
D
E
F
G
H
I
J
K
1
2
3
4
5
6
7
8
9
10
11


2011 Recruitment plan [Compatibility Mode] - Microsoft Excel
Data
Review
View
Paste
Clipboard
Alignment
Number
Conditional Formatting
Format as Table
Styles
Flash 0-day running
A1
A
B
C
D
E
F
G
H
I
J
K
1
2
3
4
5
6
7
8
9
10
11

RSA Exploit Just Crashes Excel…

The Malware

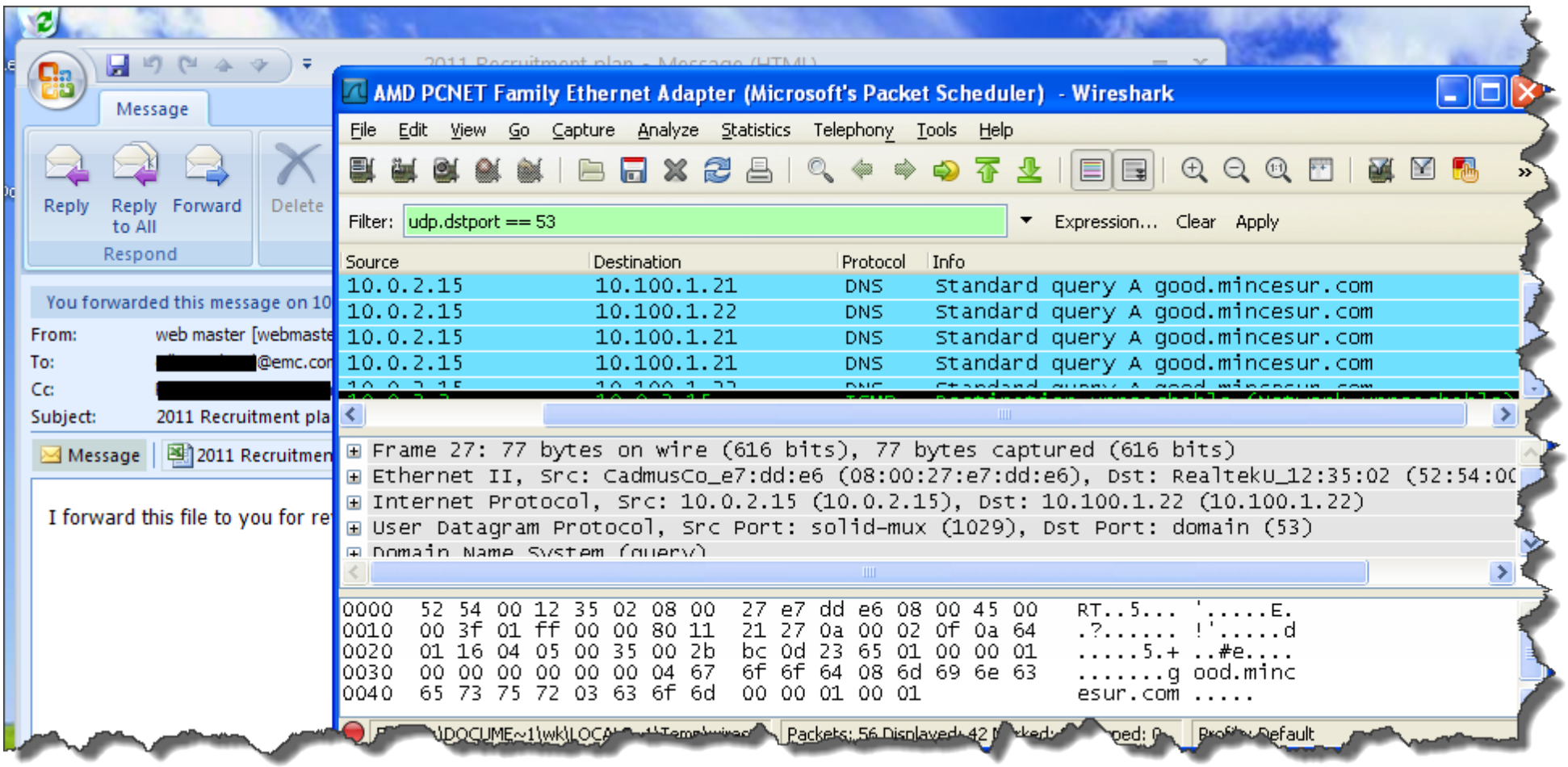
Poison Ivy

Poison Ivy
2006

Poison Ivy

2006

→ mincesur.com


Message
Reply
Reply to All
Forward
Delete
Respond
You forwarded this message on 10
From: web master [webmaste
To: @emc.com
Cc:
Subject: 2011 Recruitment pla
Message
2011 Recruitmen
I forward this file to you for re
AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: udp.dstport == 53
Expression... Clear Apply
Source Destination Protocol Info
10.0.2.15 10.100.1.21 DNS Standard query A good.mincesur.com
10.0.2.15 10.100.1.22 DNS Standard query A good.mincesur.com
10.0.2.15 10.100.1.21 DNS Standard query A good.mincesur.com
10.0.2.15 10.100.1.21 DNS Standard query A good.mincesur.com
Frame 27: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: CadmusCo_e7:dd:e6 (08:00:27:e7:dd:e6), Dst: RealtekU_12:35:02 (52:54:00
Internet Protocol, Src: 10.0.2.15 (10.0.2.15), Dst: 10.100.1.22 (10.100.1.22)
User Datagram Protocol, Src Port: solid-mux (1029), Dst Port: domain (53)
Domain Name System (query)
0000 52 54 00 12 35 02 08 00 27 e7 dd e6 08 00 45 00 RT..5... '.....E.
0010 00 3f 01 ff 00 00 80 11 21 27 0a 00 02 0f 0a 64 .?..... !'.....d
0020 01 16 04 05 00 35 00 2b bc 0d 23 65 01 00 00 01 .....5.+ ..#e....
0030 00 00 00 00 00 00 04 67 6f 6f 64 08 6d 69 6e 63 .....g ood.minc
0040 65 73 75 72 03 63 6f 6d 00 00 01 00 01 esur.com .....
Packets: 56 Displayed: 42
Profile: Default

Poison Ivy

2006

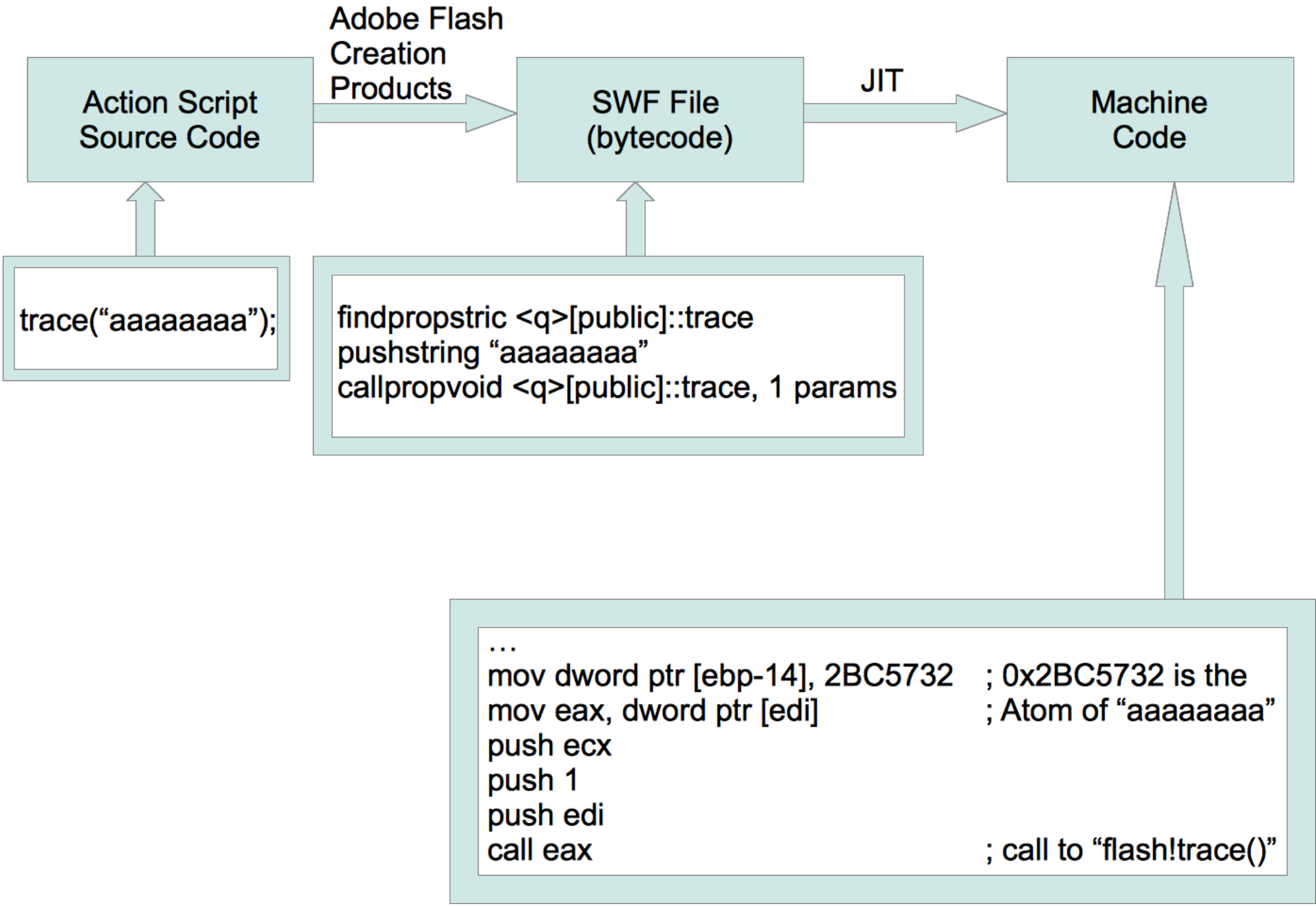
→mincesur.com

== known bad domain

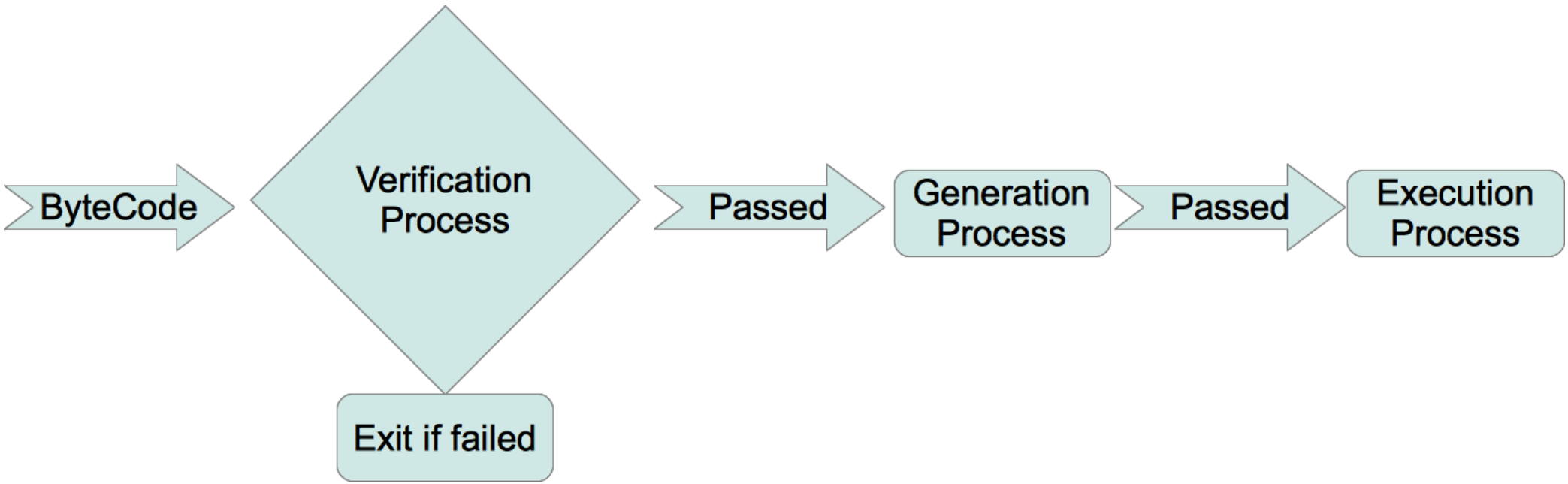
Going deeper…

SWF File divided in ABC Segments:

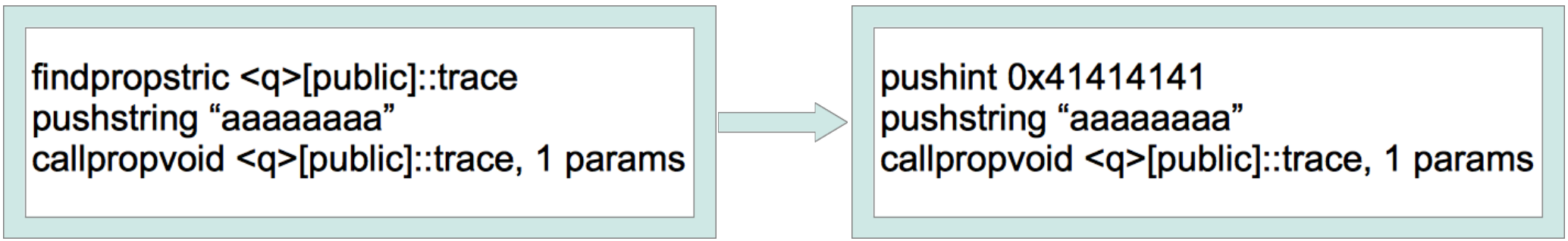
```
abcFile {
    u16 minor_version
    u16 major_version
    cpool_info constant_pool
    u30 method_count
    method_info method[method_count]
    u30 metadata_count
    metadata_info metadata[metadata_count]
    u30 class_count
    instance_info instance[class_count]
    u30 script_count
    script_info script[script_count]
    u30 method_body_count
    methody_body_info method_body[method_body_count]
}
```



Source: Understanding and Exploiting Flash ActionScript Vulnerabilities, Haifei Li, CansecWest2011



Source: Understanding and Exploiting Flash ActionScript Vulnerabilities, Haifei Li, CansecWest2011


findpropstric <q>[public]::trace
pushstring “aaaaaaaa”
callpropvoid <q>[public]::trace, 1 params
pushint 0x41414141
pushstring “aaaaaaaa”
callpropvoid <q>[public]::trace, 1 params

Inconsistent stack state after a jump to the incorrect position
Instructions write to the wrong object in the ActiveScript Stack, overwriting memory:

```
mov ecx, dword ptr ds:[edx+70] -> Program fails here
lea edx, dword ptr ss:[ebp-70]
mov dword ptr ss:[ebp-70], eax
mov eax, dword ptr ds:[ecx]
push edx
push 0
push ecx
call eax
```

Countermeasures

DEP

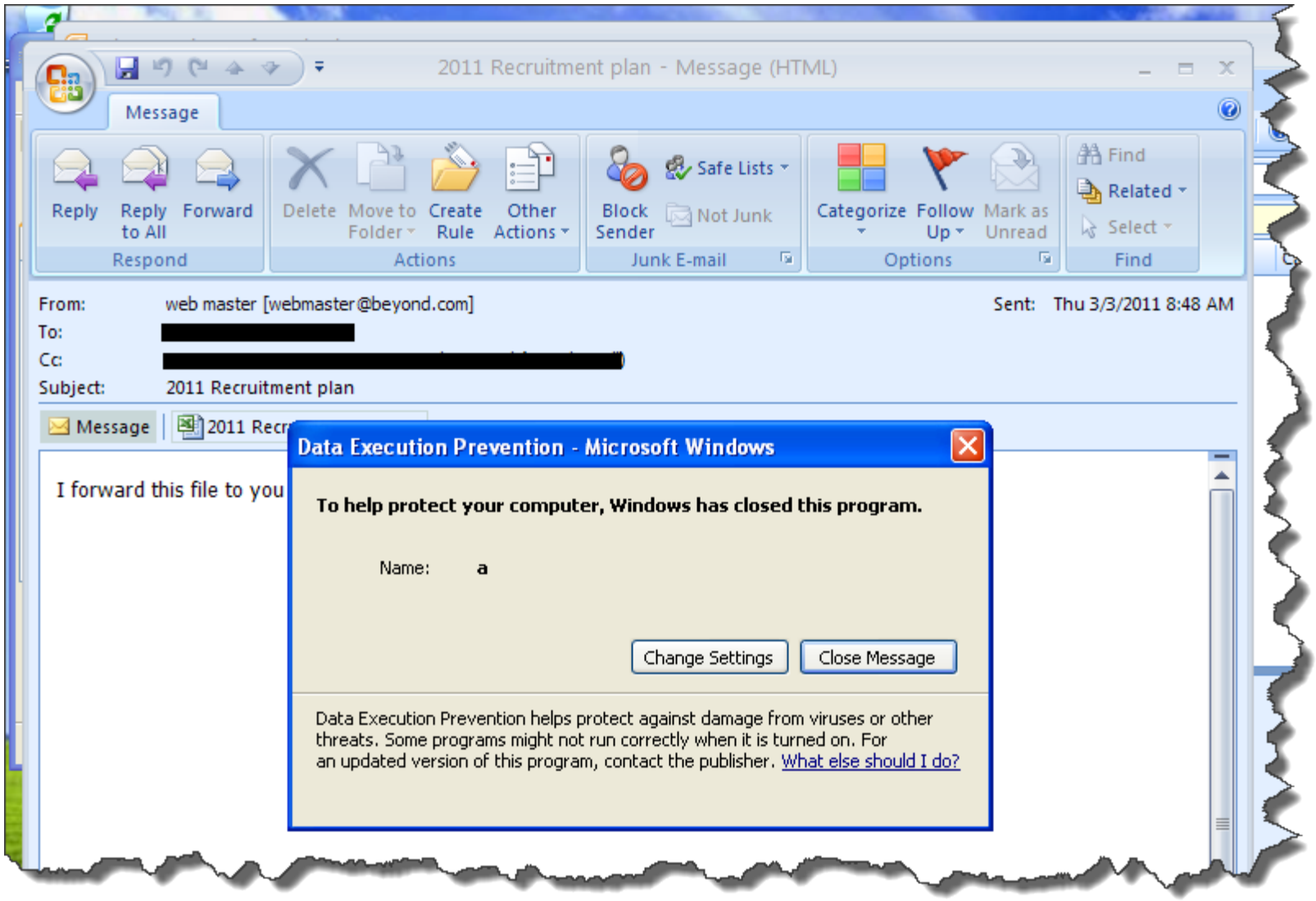
DEP

Data Execution Protection

DEP

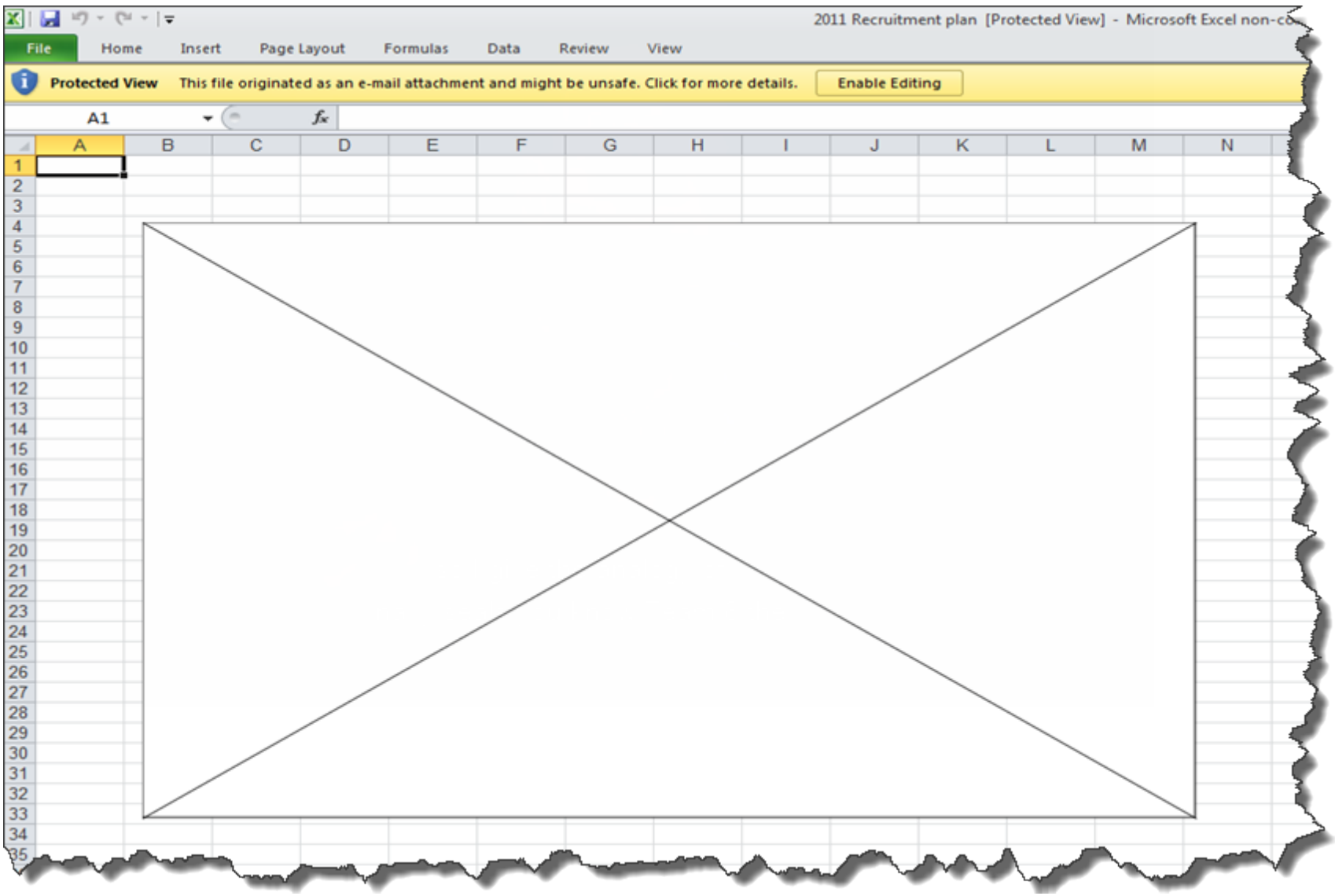
Data Execution Protection

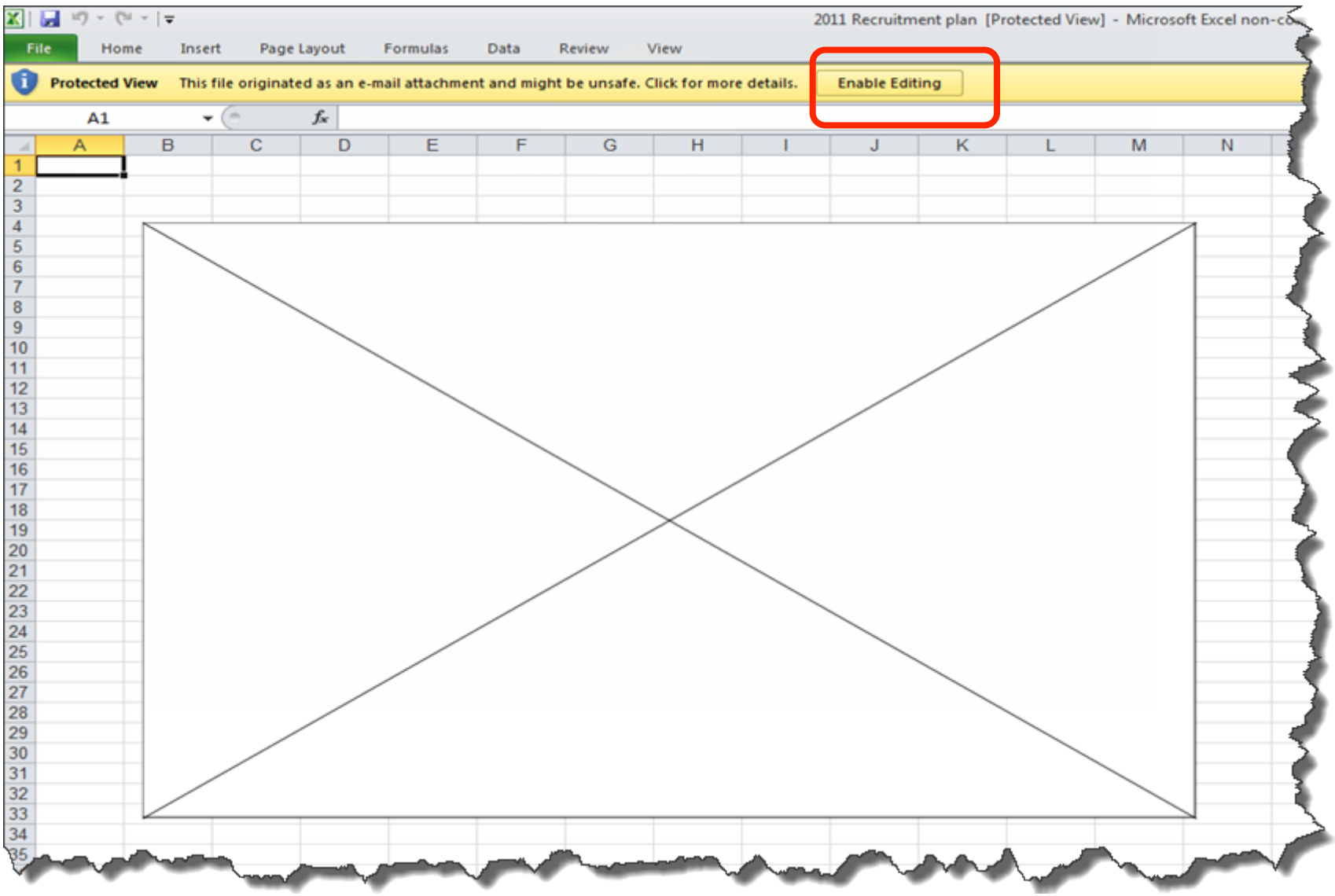
XP SP2 (2006)

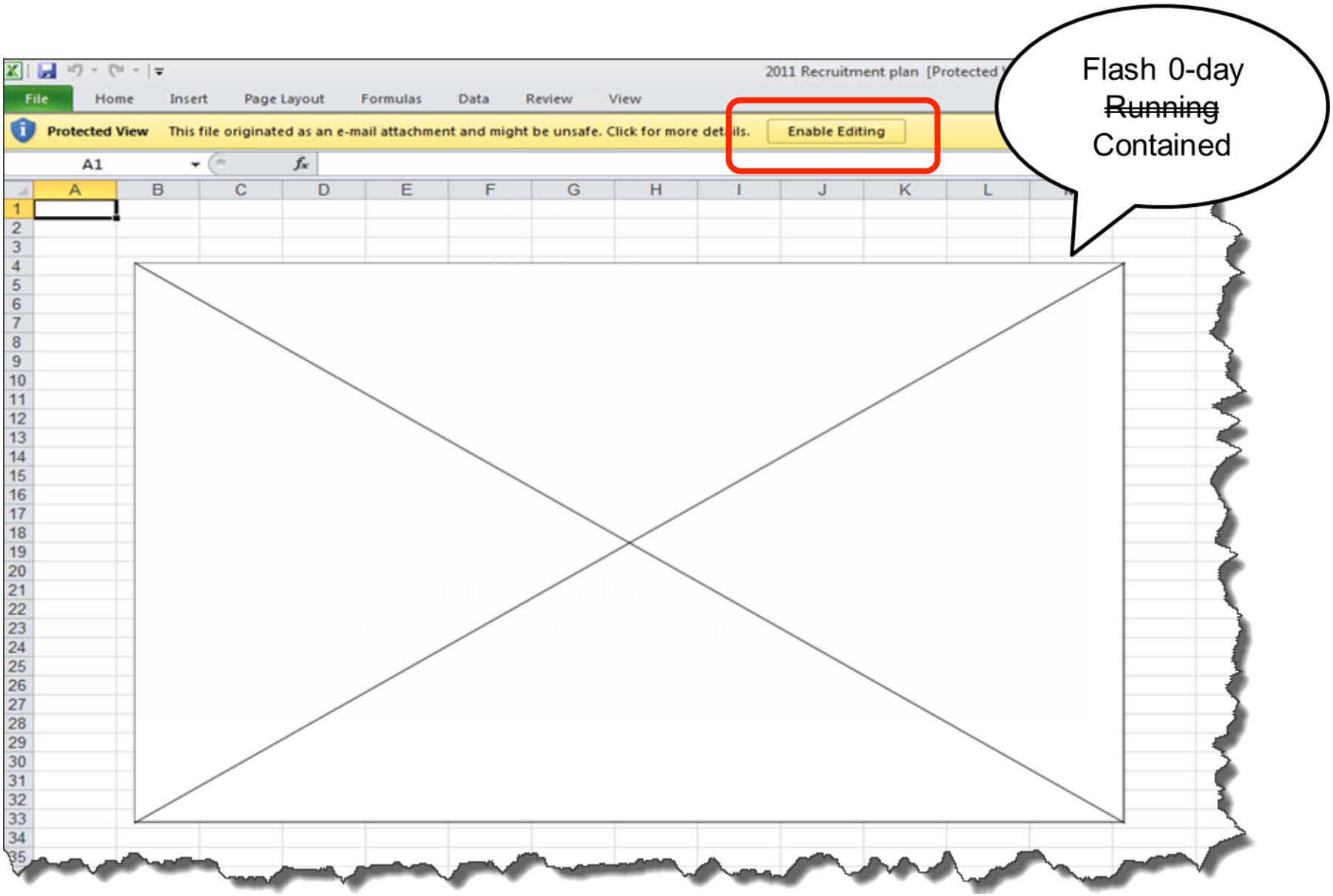

2011 Recruitment plan - Message (HTML)
Message
Reply
Reply to All
Forward
Respond
Delete
Move to Folder
Create Rule
Other Actions
Actions
Block Sender
Safe Lists
Not Junk
Junk E-mail
Categorize
Follow Up
Mark as Unread
Options
Find
Related
Select
Find
From: web master [webmaster@beyond.com]
Sent: Thu 3/3/2011 8:48 AM
To:
Cc:
Subject: 2011 Recruitment plan
Message
2011 Recr
I forward this file to you
Data Execution Prevention - Microsoft Windows
To help protect your computer, Windows has closed this program.
Name: a
Change Settings
Close Message
Data Execution Prevention helps protect against damage from viruses or other threats. Some programs might not run correctly when it is turned on. For an updated version of this program, contact the publisher. What else should I do?

Microsoft Office 2010

Microsoft Office 2010 Protected View Sandbox

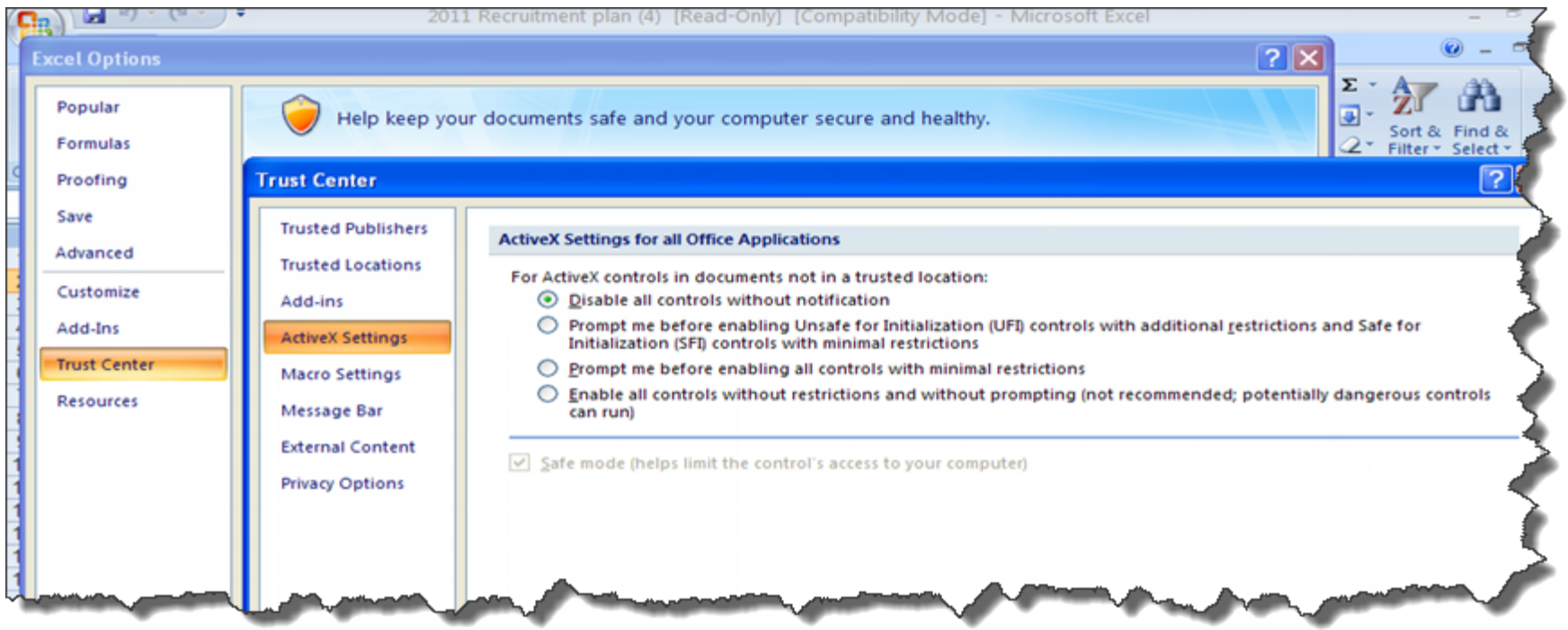

2011 Recruitment plan [Protected View] - Microsoft Excel non-co
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Protected View
This file originated as an e-mail attachment and might be unsafe. Click for more details.
Enable Editing
A1
A
B
C
D
E
F
G
H
I
J
K
L
M
N

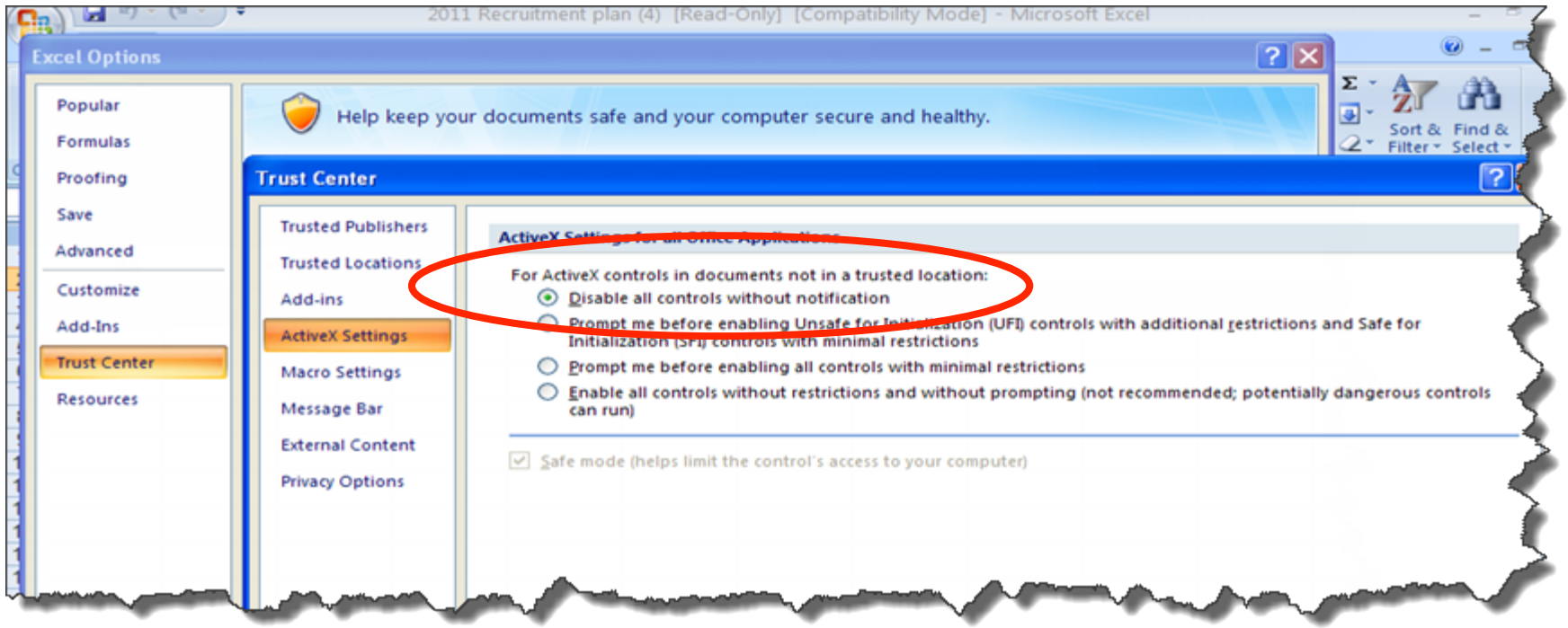

2011 Recruitment plan [Protected View] - Microsoft Excel non-co
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Protected View
This file originated as an e-mail attachment and might be unsafe. Click for more details.
Enable Editing
A1
A
B
C
D
E
F
G
H
I
J
K
L
M
N

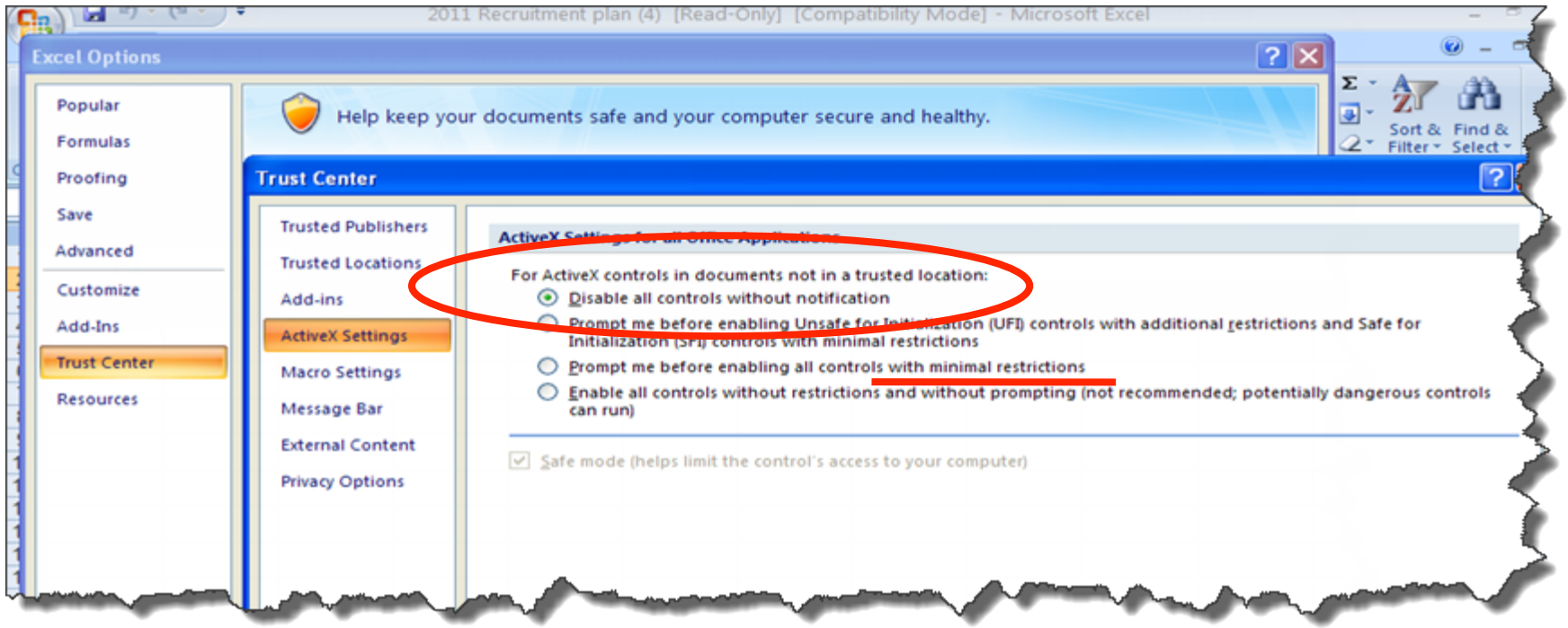

2011 Recruitment plan [Protected
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Protected View
This file originated as an e-mail attachment and might be unsafe. Click for more details.
Enable Editing
A1
Flash 0-day
~~Running~~
Contained

Microsoft Office 2007

Microsoft Office 2007
Limit Active Content


2011 Recruitment plan (4) [Read-Only] [Compatibility Mode] - Microsoft Excel
Excel Options
Popular
Formulas
Proofing
Save
Advanced
Customize
Add-Ins
Trust Center
Resources
Help keep your documents safe and your computer secure and healthy.
Sort & Filter
Find & Select
Trust Center
Trusted Publishers
Trusted Locations
Add-ins
ActiveX Settings
Macro Settings
Message Bar
External Content
Privacy Options
ActiveX Settings for all Office Applications
For ActiveX controls in documents not in a trusted location:
Disable all controls without notification
Prompt me before enabling Unsafe for Initialization (UFI) controls with additional restrictions and Safe for Initialization (SFI) controls with minimal restrictions
Prompt me before enabling all controls with minimal restrictions
Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run)
Safe mode (helps limit the control's access to your computer)


2011 Recruitment plan (4) [Read-Only] [Compatibility Mode] - Microsoft Excel
Excel Options
Popular
Formulas
Proofing
Save
Advanced
Customize
Add-Ins
Trust Center
Resources
Help keep your documents safe and your computer secure and healthy.
Sort & Filter
Find & Select
Trust Center
Trusted Publishers
Trusted Locations
Add-ins
ActiveX Settings
Macro Settings
Message Bar
External Content
Privacy Options
For ActiveX controls in documents not in a trusted location:
Disable all controls without notification
Prompt me before enabling Unsafe for Initialization (UFI) controls with additional restrictions and Safe for Initialization (SFI) controls with minimal restrictions
Prompt me before enabling all controls with minimal restrictions
Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run)
Safe mode (helps limit the control's access to your computer)


2011 Recruitment plan (4) [Read-Only] [Compatibility Mode] - Microsoft Excel
Excel Options
Popular
Formulas
Proofing
Save
Advanced
Customize
Add-Ins
Trust Center
Resources
Help keep your documents safe and your computer secure and healthy.
Sort & Filter
Find & Select
Trust Center
Trusted Publishers
Trusted Locations
Add-ins
ActiveX Settings
Macro Settings
Message Bar
External Content
Privacy Options
For ActiveX controls in documents not in a trusted location:
Disable all controls without notification
Prompt me before enabling Unsafe for Initialization (UFI) controls with additional restrictions and Safe for Initialization (SFI) controls with minimal restrictions
Prompt me before enabling all controls with minimal restrictions
Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run)
Safe mode (helps limit the control's access to your computer)

Blacklisting

Blacklisting
Known Malicious Domains

After this, Poison Ivy connects back to its server at **good.mincesur.com**. The domain **mincesur.com** has been used in similar espionage attacks over an extended period of time.

Found 6 RRs in 0.27 seconds.

download.mincesur.com.	A	119.70.119.30
good.mincesur.com.	A	119.70.119.30
hjkl.wekby.com.	A	119.70.119.30
man.mincesur.com.	A	119.70.119.30
qwer.wekby.com.	A	119.70.119.30
uiop.wekby.com.	A	119.70.119.30

After this, Poison Ivy connects back to its server at **good.mincesur.com**. The domain **mincesur.com** has been used in similar espionage attacks over an extended period of time.

Found 6 RRs in 0.27 seconds.

download.mincesur.com.	A	119.70.119.30
good.mincesur.com.	A	119.70.119.30
hjkl.wekby.com.	A	119.70.119.30
man.mincesur.com.	A	119.70.119.30
qwer.wekby.com.	A	119.70.119.30
uiop.wekby.com.	A	119.70.119.30

Windows 7

Windows 7
No Active X Flash

Windows 7
No Active X Flash
Alternative OS

To APT or not to APT?

Advanced?

Persistent?

Threat?

Information Asymmetry

~~Information Asymmetry~~

Community Knowledge

6

Thank you

rbranco@qualys.com

@bsdaemon