Phishing with Office 365

AUSTRALIAN CATHOLIC UNIVERSITY

*Minecraft, also a Microsoft product

Our users? →

Keep an eye out for a zombie villager, you might win something!

Like this guy, but not this one ->

Phishing with O365

- Environment Pre-migration – what we had
- Post-migration – what we lost
- Fun and games (well… not really) or bad timing?
- Review current processes
- Rasomware Mitigation strategies?
- Lessons learned – zombie proof your village

What we had…

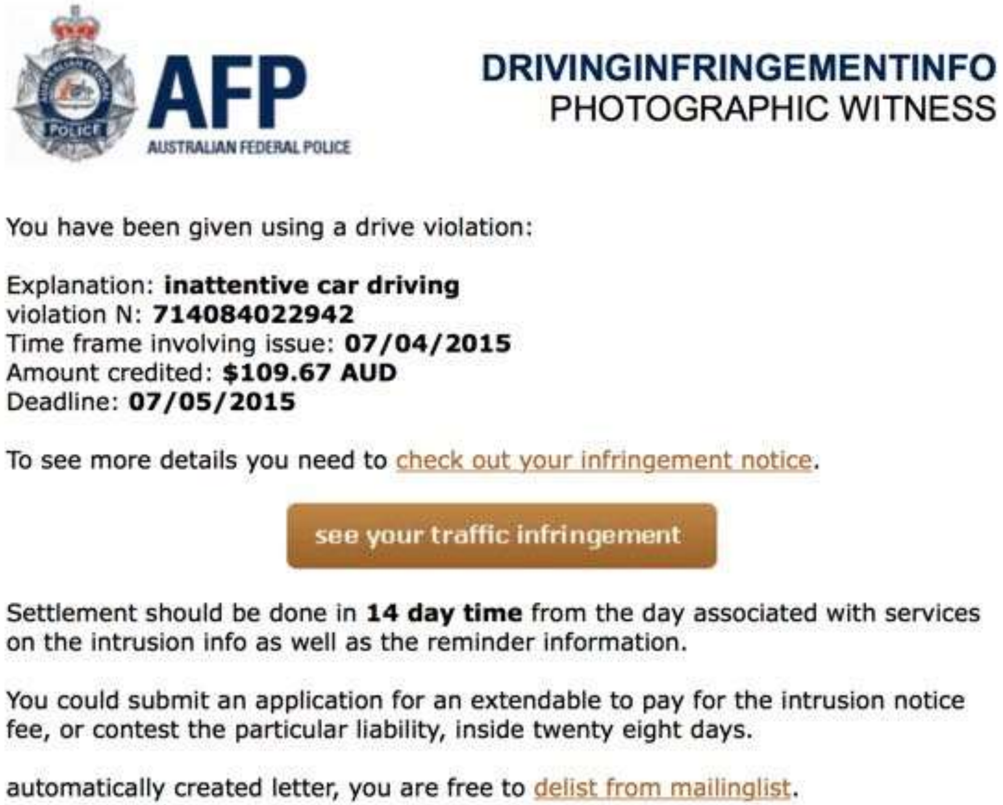
- 2014 - On-prem Exchange 2010
  - Exchange servers just about all virtualised
- Mail filtering using Symantec Cloud (messagelabs)
  - Pretty good protection

What we lost…

- April 2015 – migration complete
- Symantec Cloud turned off
  - Spam and phishing increased
  - Mail flowing directly into O365 basic protection (ATP filters not released to Education yet and expensive)
- Limited mail-queue visibility!

Fun and games?

More staff getting phishing emails, like…



AFP
AUSTRALIAN FEDERAL POLICE

DRIVINGINFRINGEMENTINFO
PHOTOGRAPHIC WITNESS

You have been given using a drive violation:

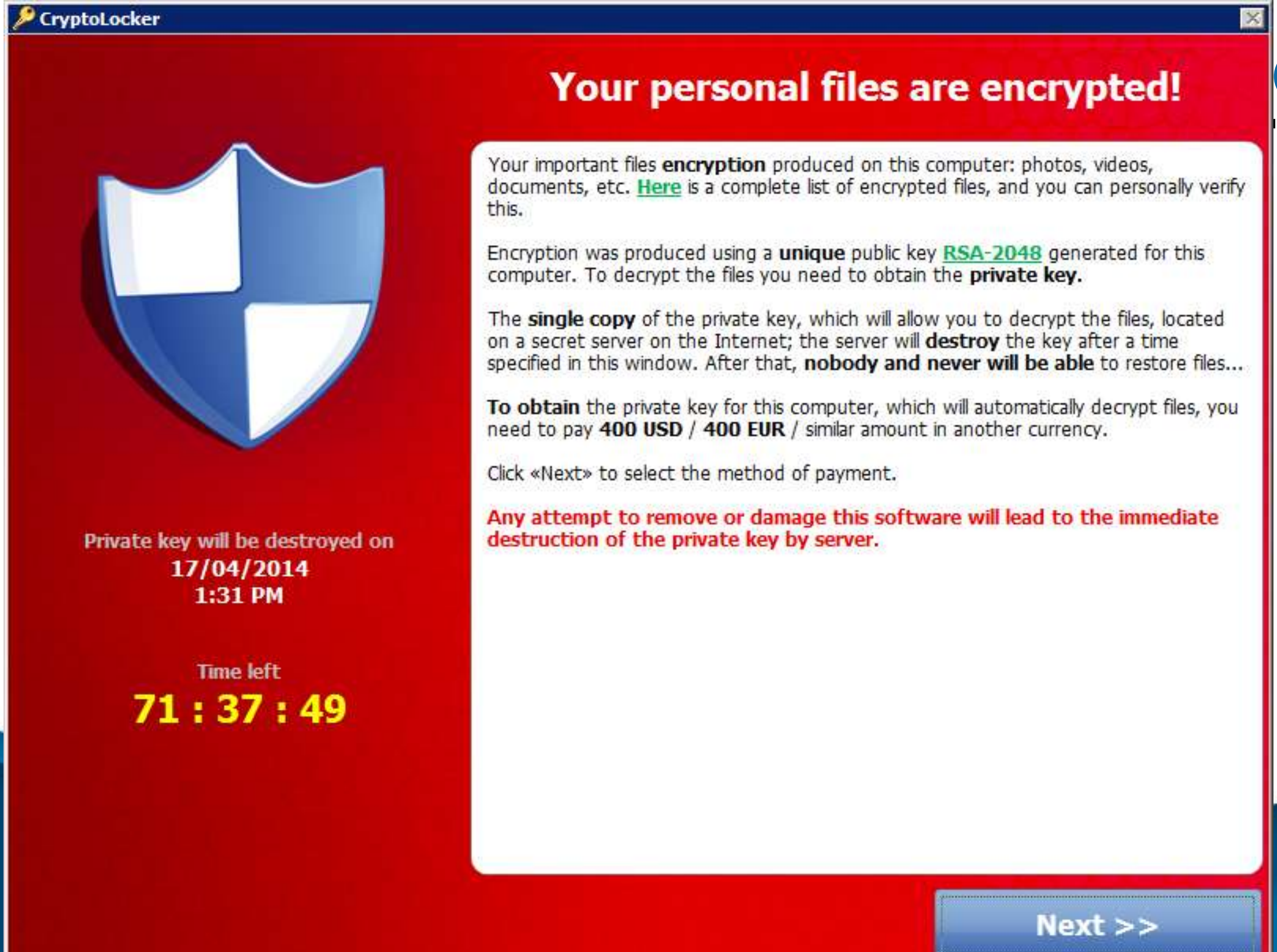
Explanation: **inattentive car driving**
violation N: **714084022942**
Time frame involving issue: **07/04/2015**
Amount credited: **$109.67 AUD**
Deadline: **07/05/2015**

To see more details you need to check out your infringement notice.

Settlement should be done in **14 day time** from the day associated with services on the intrusion info as well as the reminder information.

You could submit an application for an extendable to pay for the intrusion notice fee, or contest the particular liability, inside twenty eight days.

automatically created letter, you are free to delist from mailinglist.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **400 USD** / **400 EUR** / similar amount in another currency.

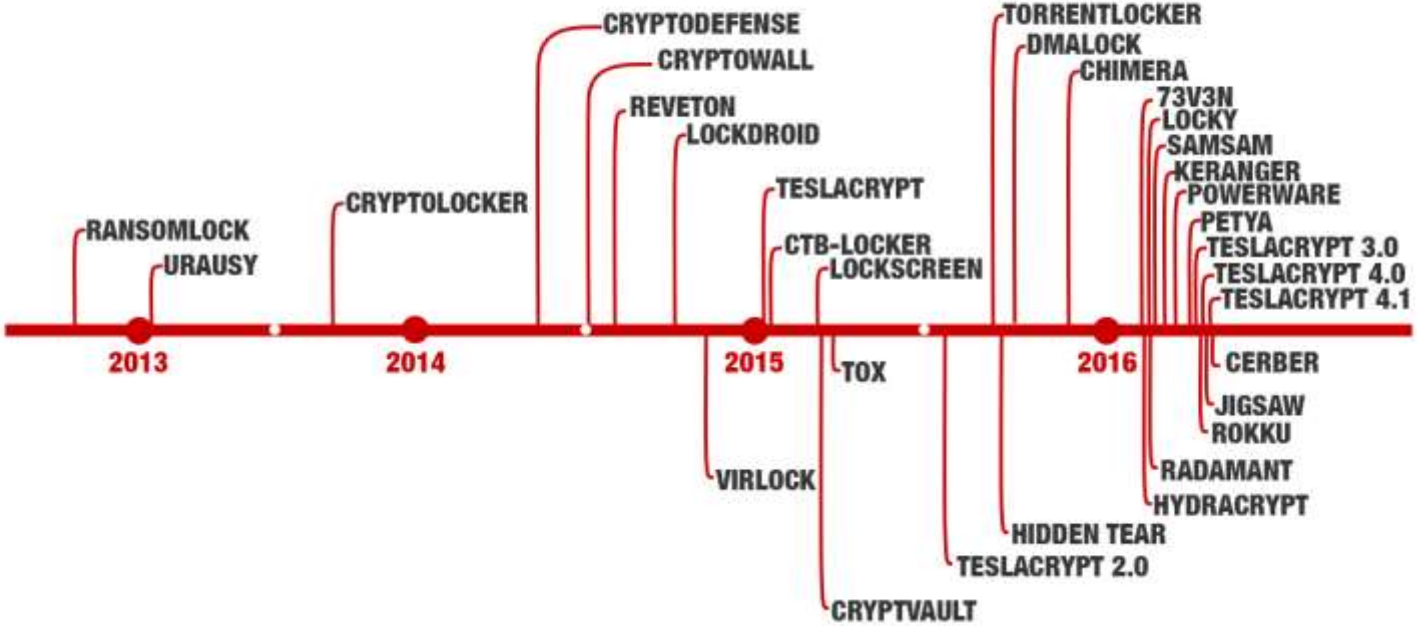
Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
17/04/2014
1:31 PM

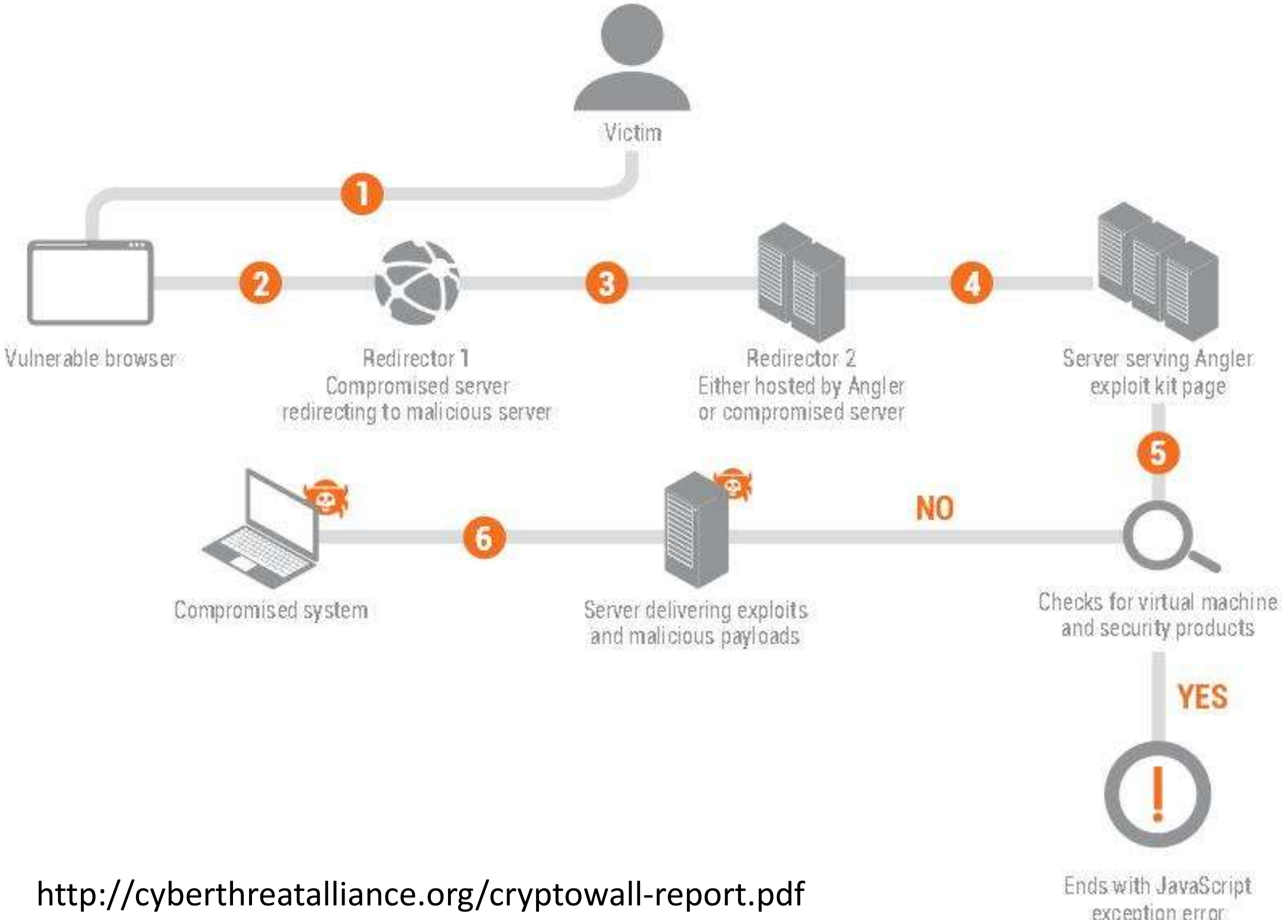
Time left
71 : 37 : 49

Here be zombies!


RANSOMLOCK
URAUSY
2013
CRYPTOLOCKER
2014
CRYPTODEFENSE
CRYPTOWALL
REVETON
LOCKDROID
VIRLOCK
TESLACRYPT
CTB-LOCKER
2015
LOCKSCREEN
TOX
CRYPTVAULT
TESLACRYPT 2.0
TORRENTLOCKER
DMALOCK
HIDDEN TEAR
CHIMERA
2016
73V3N
LOCKY
SAMSAM
KERANGER
POWERWARE
PETYA
TESLACRYPT 3.0
TESLACRYPT 4.0
TESLACRYPT 4.1
CERBER
JIGSAW
ROKKU
RADAMANT
HYDRACRYPT

How Ransomware works

AUSTRALIAN CATHOLIC UNIVERSITY

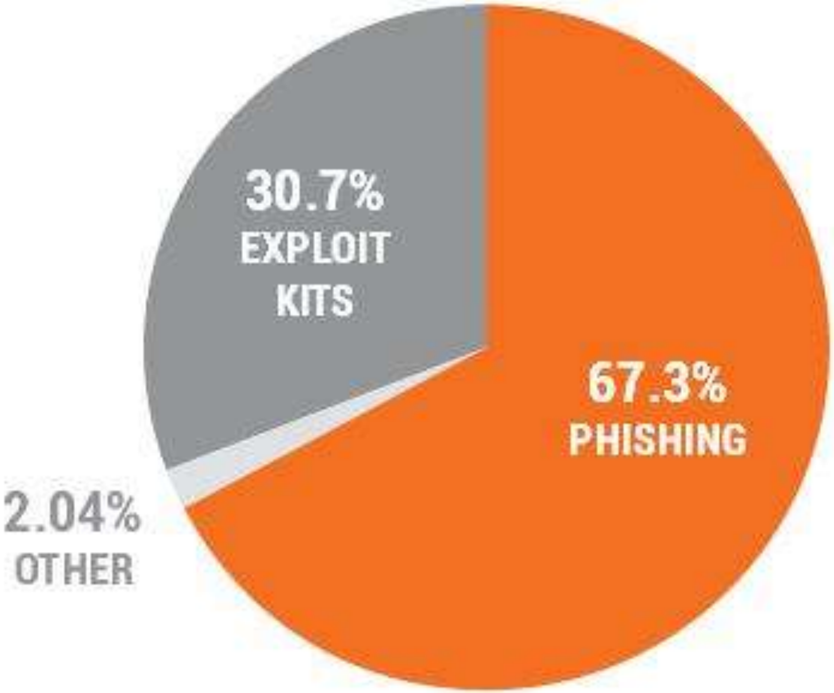


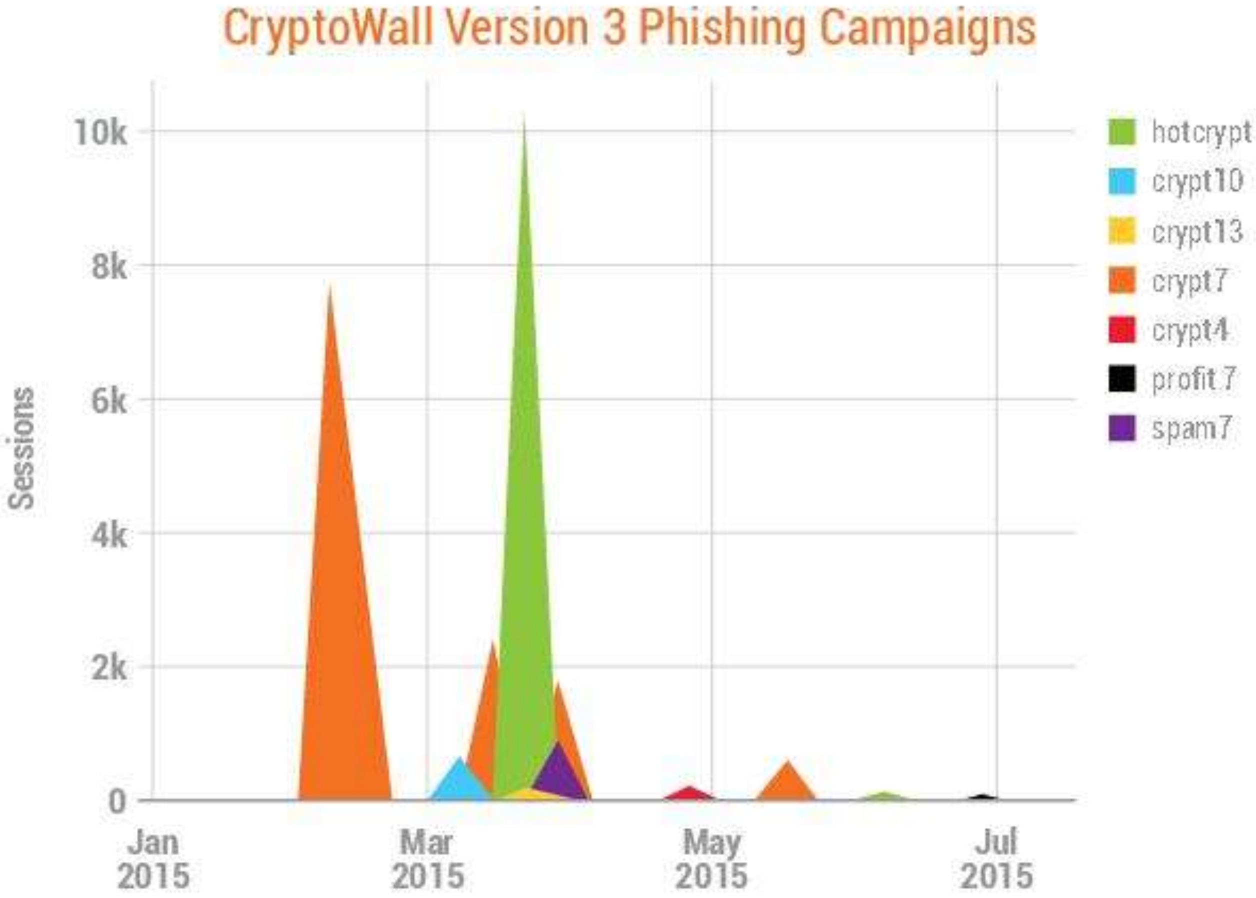
http://cyberthreatalliance.org/cryptowall-report.pdf

The Angler exploit kit performs several steps to successfully infect systems:

- Victim accesses a compromised web server through a vulnerable browser.
- Compromised web server redirects to an intermediate server.
- Intermediate server redirects to a malicious web server hosting the exploit kit’s landing page.
- Landing page checks for the presence of vulnerable plug-ins (e.g., Java®, Flash®, Silverlight®) and their version information.
- When a vulnerable browser or plug-in is found, the exploit kit delivers the proper payload and infects the machine.

Propogation of CryptoWall Version 3

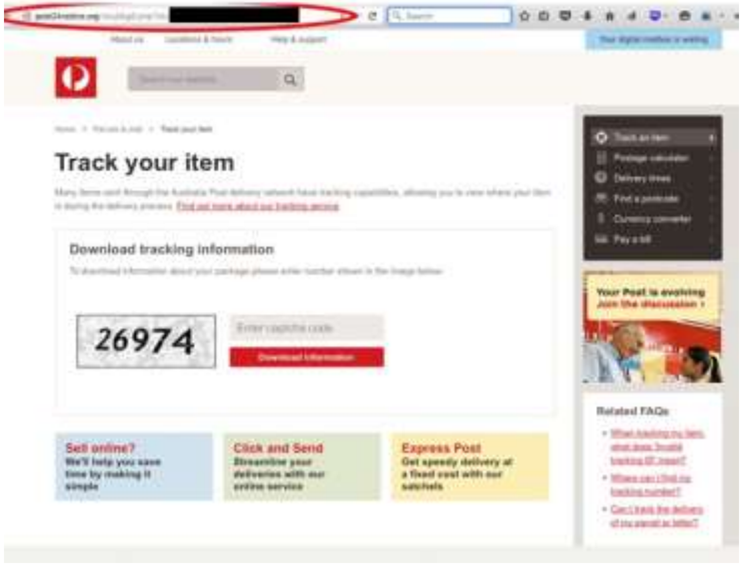




Really bad timing to turn off our filters during April!

Some links from the Auspost/AFP phishing scam had a very interesting URL

How deep is the rabbit hole…



[illegible] [redacted]

Search
About us
Locations & hours
Help & support
Your digital mailbox is waiting
Search our website
Home > Parcels & mail > Track your item

Track your item

Many items sent through the Australia Post delivery network have tracking capabilities, allowing you to view where your item is during the delivery process. Find out more about our tracking service

Download tracking information

To download information about your package please enter number shown in the image below

26974

Enter captcha code

Related FAQs

- When tracking my item, what does 'Invalid tracking ID' mean?
- Where can I find my tracking number?
- Can I track the delivery of my parcel or letter?

Sell online?
We'll help you save time by making it simple
Click and Send
Streamline your deliveries with our online service
Express Post
Get speedy delivery at a fixed cost with our satchels

Several things happening here:

URL link in email:

http://xxxxxxxx.xxx/system/logs/bfPYcul7XAGszr.php?id=example@example.com
(Redirect)

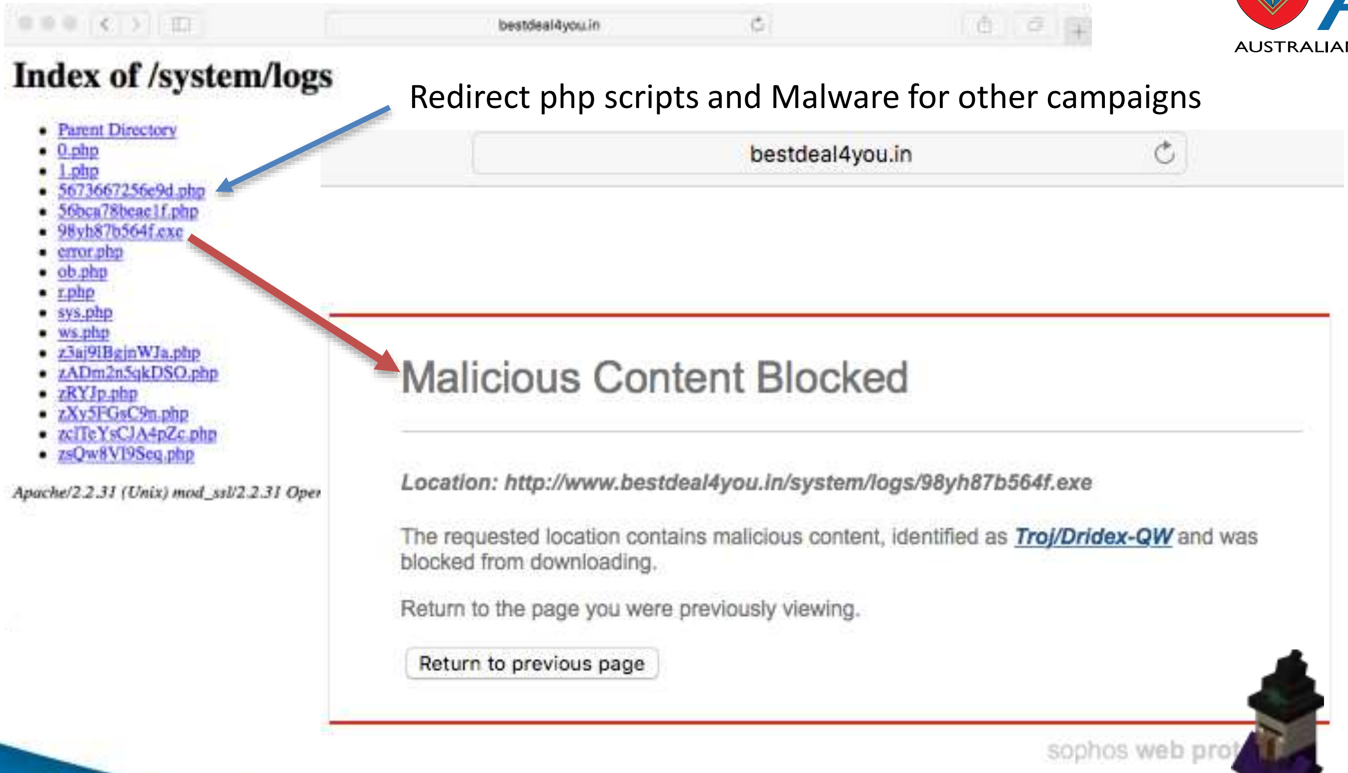
http://post24-notice.net/ug22ectc.php?id=ZXhhbXBsZUBleGFtcGxlLmNvbQ==
(AusPost Page with Captcha Challenge)

http://post24-notice.net/ug22ectc.php?id=ZXhhbXBsZUBleGFtcGxlLmNvbQ==
(POST captcha_code=26974, Redirect)

Malware download from yandex share:

https://downloader.disk.yandex.com/disk/32b75c3ce244c43768c9b145dfb2999382cff4c20c1d4e6436bc973f5d6f2c2c/55dfdd3b/h2wvLwF-bQZ1j6SxcVCNR3-dtkMMzVoL32Hfz5PiWv9UfSrJ9Eg2byl0A0GbbKEwDiKC7Ch0Z4q7naihNm3ZWA%3D%3D?uid=0&filename=notice_139691.zip&disposition=attachment&hash=bxVXwD%2BXezq9/mNrxNK%2BoVrgHqUuGuUhr/Vzer%2Bsmbg%3D&limit=0&content_type=application%2Fx-zip-compressed&fsize=479629&hid=300b6c914d713e384b1d63950315e9d0&media_type=compressed&tknv=v2

File saved as notice_139691.zip



bestdeal4you.in

Index of /system/logs

- Parent Directory
- 0.php
- 1.php
- 5673667256e9d.php
- 56bca78beae1f.php
- 98yh87b564f.exe
- error.php
- ob.php
- r.php
- sys.php
- ws.php
- z3aj9lBgjnWJa.php
- zADm2n5qkDSO.php
- zRYJp.php
- zXy5FGsC9n.php
- zcITeYsCJA4pZc.php
- zsQw8VI9Seq.php

Apache/2.2.31 (Unix) mod_ssl/2.2.31 Oper

Redirect php scripts and Malware for other campaigns

bestdeal4you.in

Malicious Content Blocked

Location: http://www.bestdeal4you.in/system/logs/98yh87b564f.exe

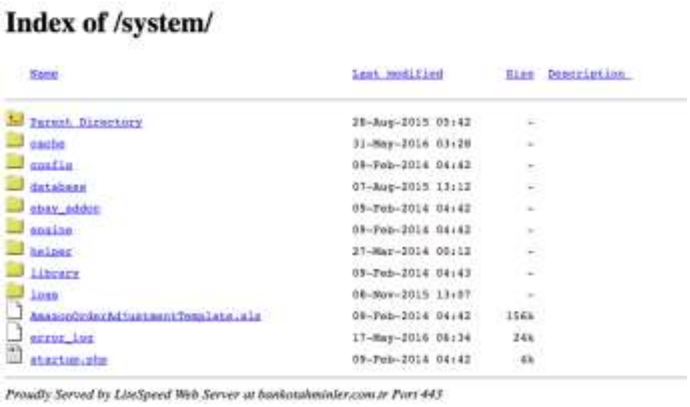
The requested location contains malicious content, identified as ***Troj/Dridex-QW*** and was blocked from downloading.

Return to the page you were previously viewing.

Return to previous page

sophos web prot

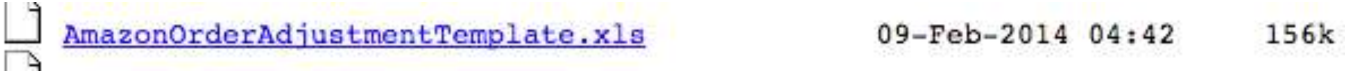
What web application uses /system/logs??? Lets go back a folder…



Index of /system/

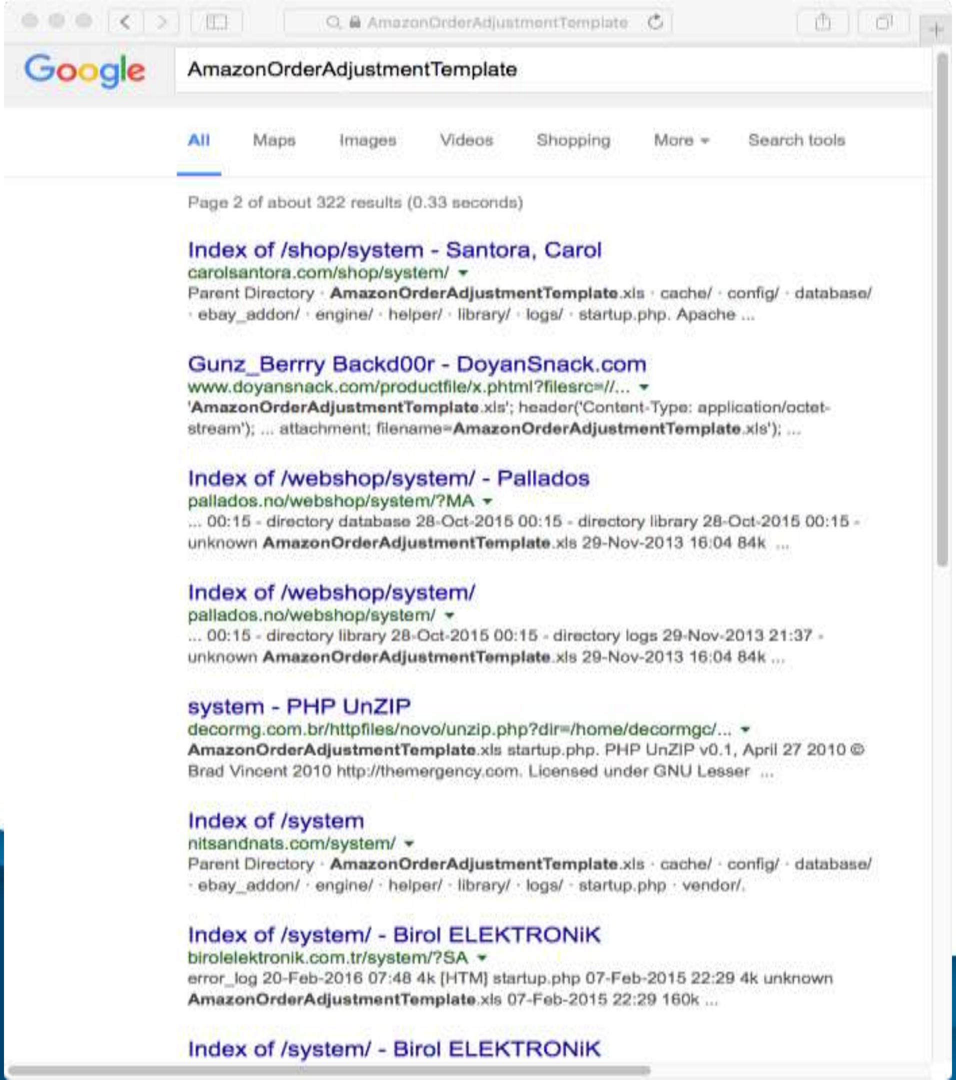
```
     Name                                          Last modified      Size  Description

     Parent Directory                              28-Aug-2015 03:42    -
     cache                                         31-May-2016 03:28    -
     config                                        09-Feb-2014 04:42    -
     database                                      07-Aug-2015 13:12    -
     ebay_addon                                    09-Feb-2014 04:42    -
     engine                                        09-Feb-2014 04:42    -
     helper                                        27-Mar-2014 00:12    -
     library                                       09-Feb-2014 04:43    -
     logs                                          08-Nov-2015 13:07    -
     AmazonOrderAdjustmentTemplate.xls             09-Feb-2014 04:42  156k
     error_log                                     17-May-2016 08:34   24k
     startup.php                                   09-Feb-2014 04:42    4k
```

Proudly Served by LiteSpeed Web Server at bankotahminler.com.tr Port 443



```
AmazonOrderAdjustmentTemplate.xls                 09-Feb-2014 04:42      156k
```

Huh? I can browse the file structure??
wow…



AmazonOrderAdjustmentTemplate

Page 2 of about 322 results (0.33 seconds)

Index of /shop/system - Santora, Carol
carolsantora.com/shop/system/
Parent Directory · **AmazonOrderAdjustmentTemplate**.xls · cache/ · config/ · database/ · ebay_addon/ · engine/ · helper/ · library/ · logs/ · startup.php. Apache ...

Gunz_Berrry Backd00r - DoyanSnack.com
www.doyansnack.com/productfile/x.phtml?filesrc=//...
'**AmazonOrderAdjustmentTemplate**.xls'; header('Content-Type: application/octet-stream'); ... attachment; filename=**AmazonOrderAdjustmentTemplate**.xls'); ...

Index of /webshop/system/ - Pallados
pallados.no/webshop/system/?MA
... 00:15 - directory database 28-Oct-2015 00:15 - directory library 28-Oct-2015 00:15 - unknown **AmazonOrderAdjustmentTemplate**.xls 29-Nov-2013 16:04 84k ...

Index of /webshop/system/
pallados.no/webshop/system/
... 00:15 - directory library 28-Oct-2015 00:15 - directory logs 29-Nov-2013 21:37 - unknown **AmazonOrderAdjustmentTemplate**.xls 29-Nov-2013 16:04 84k ...

system - PHP UnZIP
decormg.com.br/httpfiles/novo/unzip.php?dir=/home/decormgc/...
AmazonOrderAdjustmentTemplate.xls startup.php. PHP UnZIP v0.1, April 27 2010 © Brad Vincent 2010 http://themergency.com. Licensed under GNU Lesser ...

Index of /system
nitsandnats.com/system/
Parent Directory · **AmazonOrderAdjustmentTemplate**.xls · cache/ · config/ · database/ · ebay_addon/ · engine/ · helper/ · library/ · logs/ · startup.php · vendor/.

Index of /system/ - Birol ELEKTRONiK
birolelektronik.com.tr/system/?SA
error_log 20-Feb-2016 07:48 4k [HTM] startup.php 07-Feb-2015 22:29 4k unknown **AmazonOrderAdjustmentTemplate**.xls 07-Feb-2015 22:29 160k ...

Index of /system/ - Birol ELEKTRONiK

Lots of sites with the
Same file....

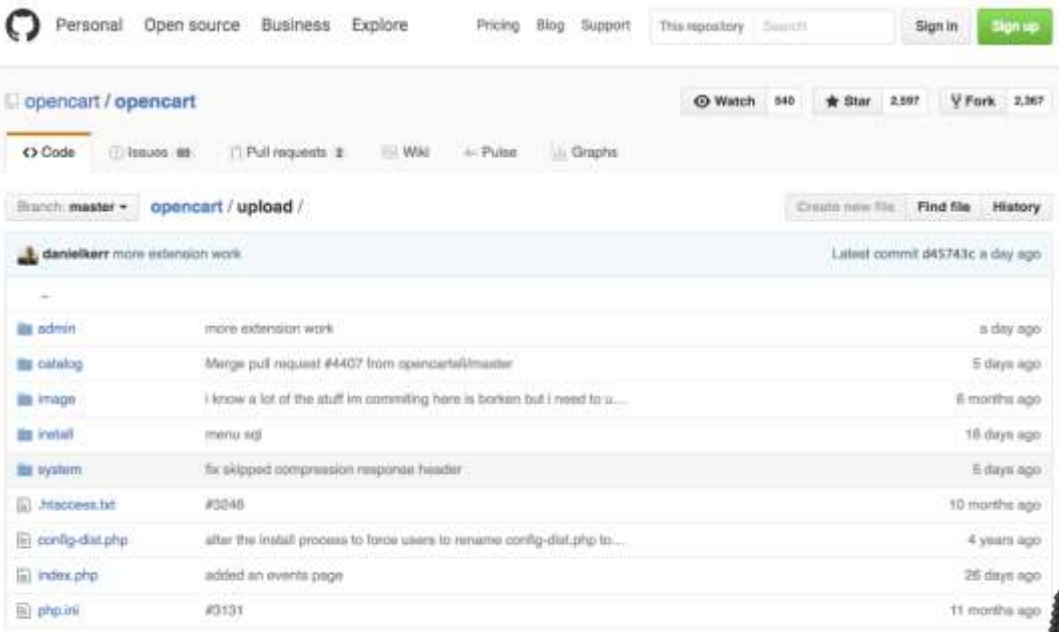
... All shopping sites...

All world readable....

Some kind of
Shopping cart?

Lots of these
Hosting malware

Yup…. Opencart

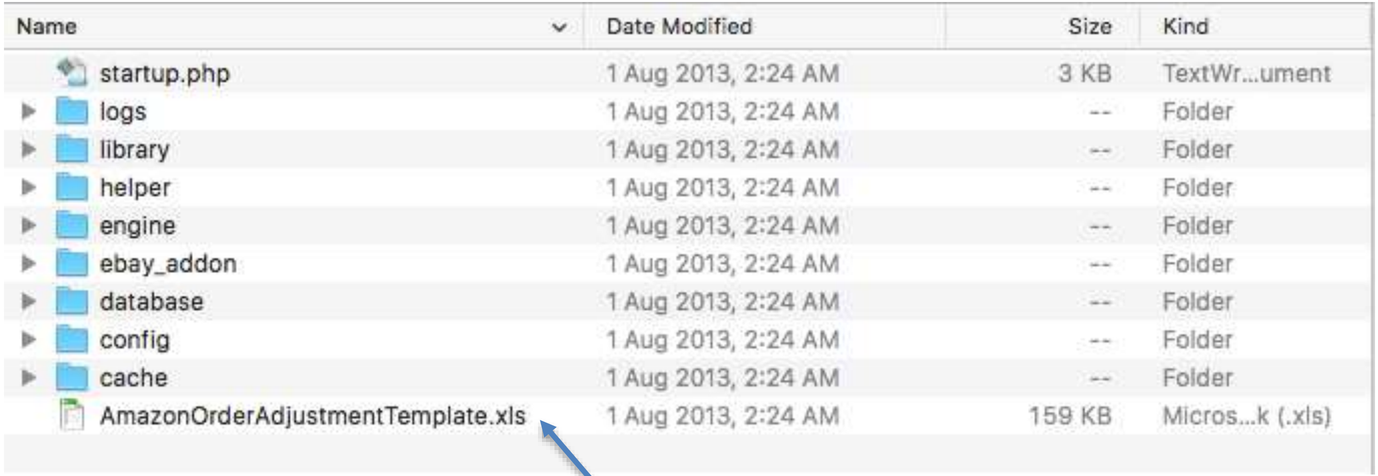


opencart / opencart

opencart / upload /

danielkerr more extension work — Latest commit d45743c a day ago

..		
admin	more extension work	a day ago
catalog	Merge pull request #4407 from opencart/master	5 days ago
image	i know a lot of the stuff im commiting here is borken but i need to u…	6 months ago
install	menu sql	18 days ago
system	fix skipped compression response header	5 days ago
.htaccess.txt	#3248	10 months ago
config-dist.php	alter the install process to force users to rename config-dist.php to…	4 years ago
index.php	added an events page	26 days ago
php.ini	#3131	11 months ago

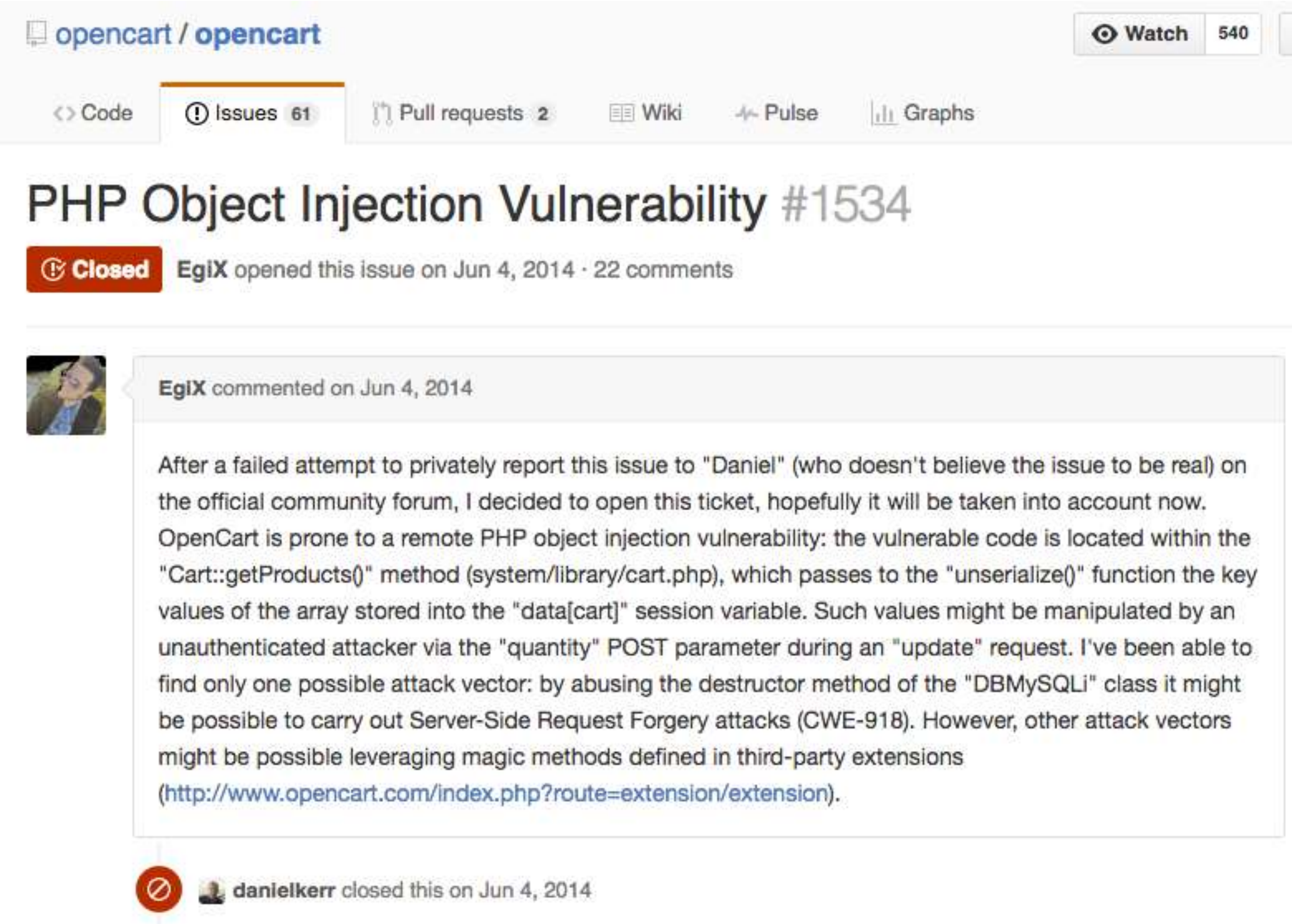


Name	Date Modified	Size	Kind
startup.php	1 Aug 2013, 2:24 AM	3 KB	TextWr...ument
logs	1 Aug 2013, 2:24 AM	--	Folder
library	1 Aug 2013, 2:24 AM	--	Folder
helper	1 Aug 2013, 2:24 AM	--	Folder
engine	1 Aug 2013, 2:24 AM	--	Folder
ebay_addon	1 Aug 2013, 2:24 AM	--	Folder
database	1 Aug 2013, 2:24 AM	--	Folder
config	1 Aug 2013, 2:24 AM	--	Folder
cache	1 Aug 2013, 2:24 AM	--	Folder
AmazonOrderAdjustmentTemplate.xls	1 Aug 2013, 2:24 AM	159 KB	Micros...k (.xls)

Opencart v 1.5.6 …. 1st Aug 2013!!

About the only version with this file

So we assume that this old version is
Vulnerable and being used to host malware



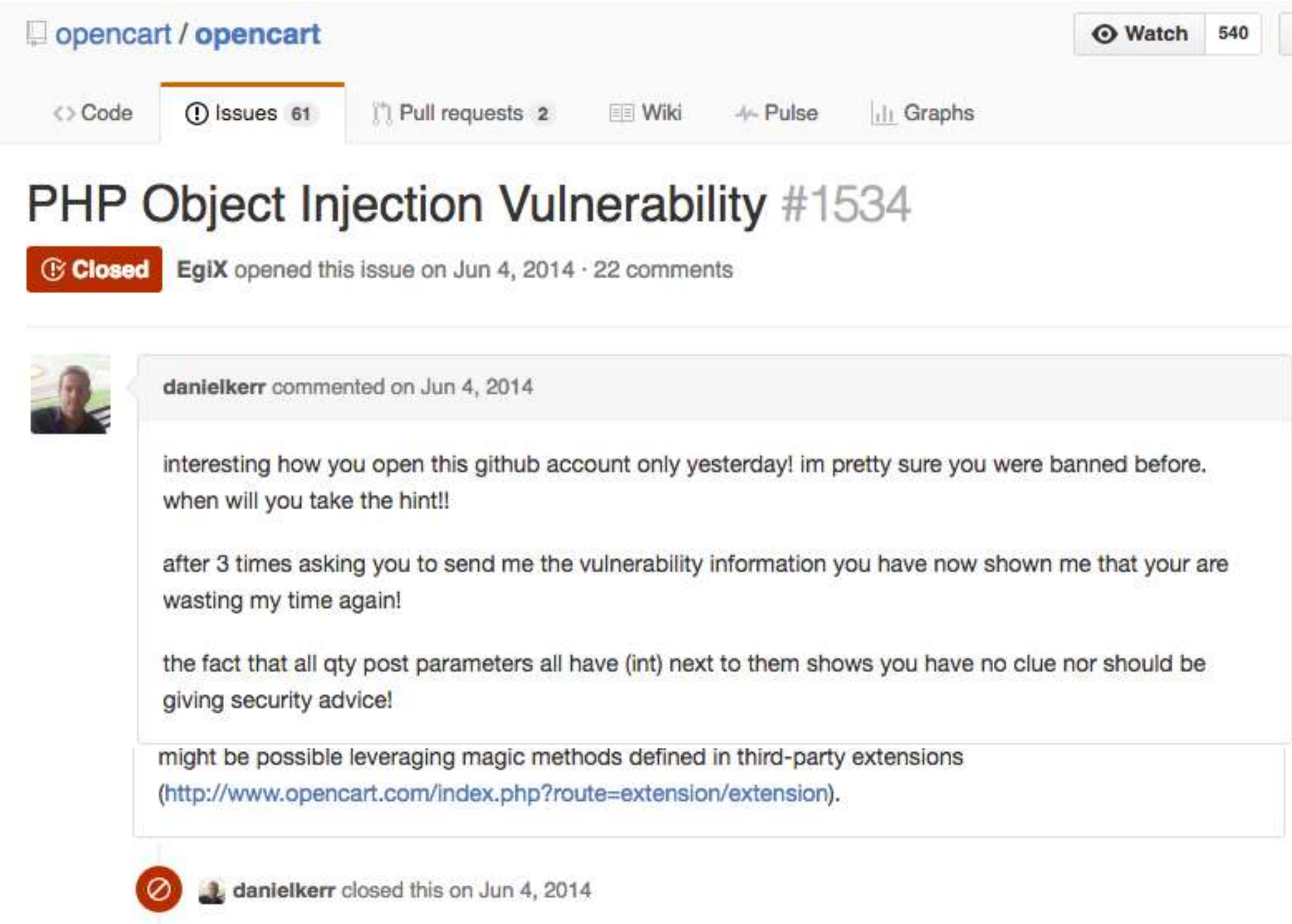
PHP Object Injection Vulnerability #1534

EgiX opened this issue on Jun 4, 2014 · 22 comments

EgiX commented on Jun 4, 2014

After a failed attempt to privately report this issue to "Daniel" (who doesn't believe the issue to be real) on the official community forum, I decided to open this ticket, hopefully it will be taken into account now. OpenCart is prone to a remote PHP object injection vulnerability: the vulnerable code is located within the "Cart::getProducts()" method (system/library/cart.php), which passes to the "unserialize()" function the key values of the array stored into the "data[cart]" session variable. Such values might be manipulated by an unauthenticated attacker via the "quantity" POST parameter during an "update" request. I've been able to find only one possible attack vector: by abusing the destructor method of the "DBMySQLi" class it might be possible to carry out Server-Side Request Forgery attacks (CWE-918). However, other attack vectors might be possible leveraging magic methods defined in third-party extensions (http://www.opencart.com/index.php?route=extension/extension).

danielkerr closed this on Jun 4, 2014



PHP Object Injection Vulnerability #1534

EgiX opened this issue on Jun 4, 2014 · 22 comments

danielkerr commented on Jun 4, 2014

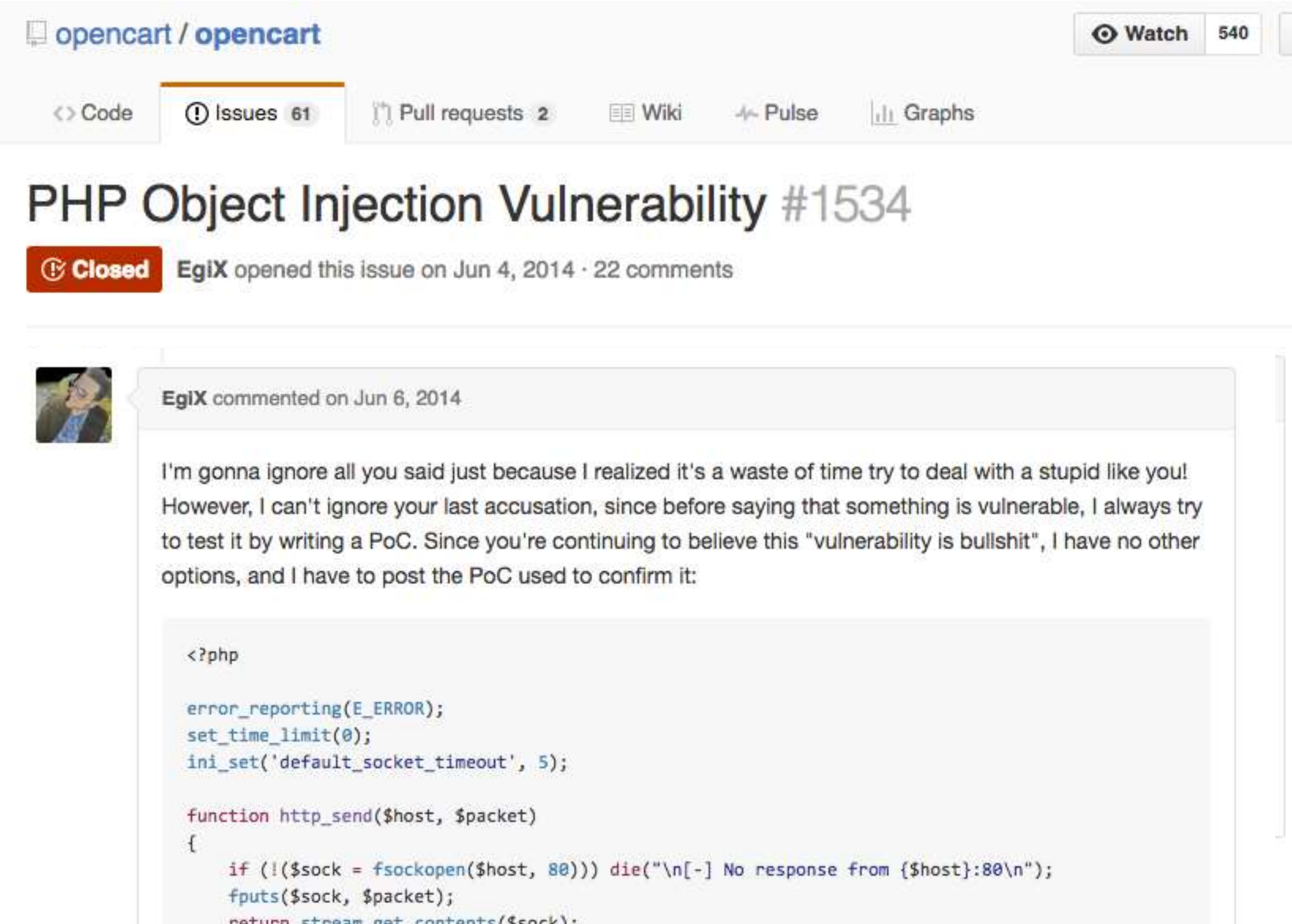
interesting how you open this github account only yesterday! im pretty sure you were banned before. when will you take the hint!!

after 3 times asking you to send me the vulnerability information you have now shown me that your are wasting my time again!

the fact that all qty post parameters all have (int) next to them shows you have no clue nor should be giving security advice!

might be possible leveraging magic methods defined in third-party extensions (http://www.opencart.com/index.php?route=extension/extension).

danielkerr closed this on Jun 4, 2014



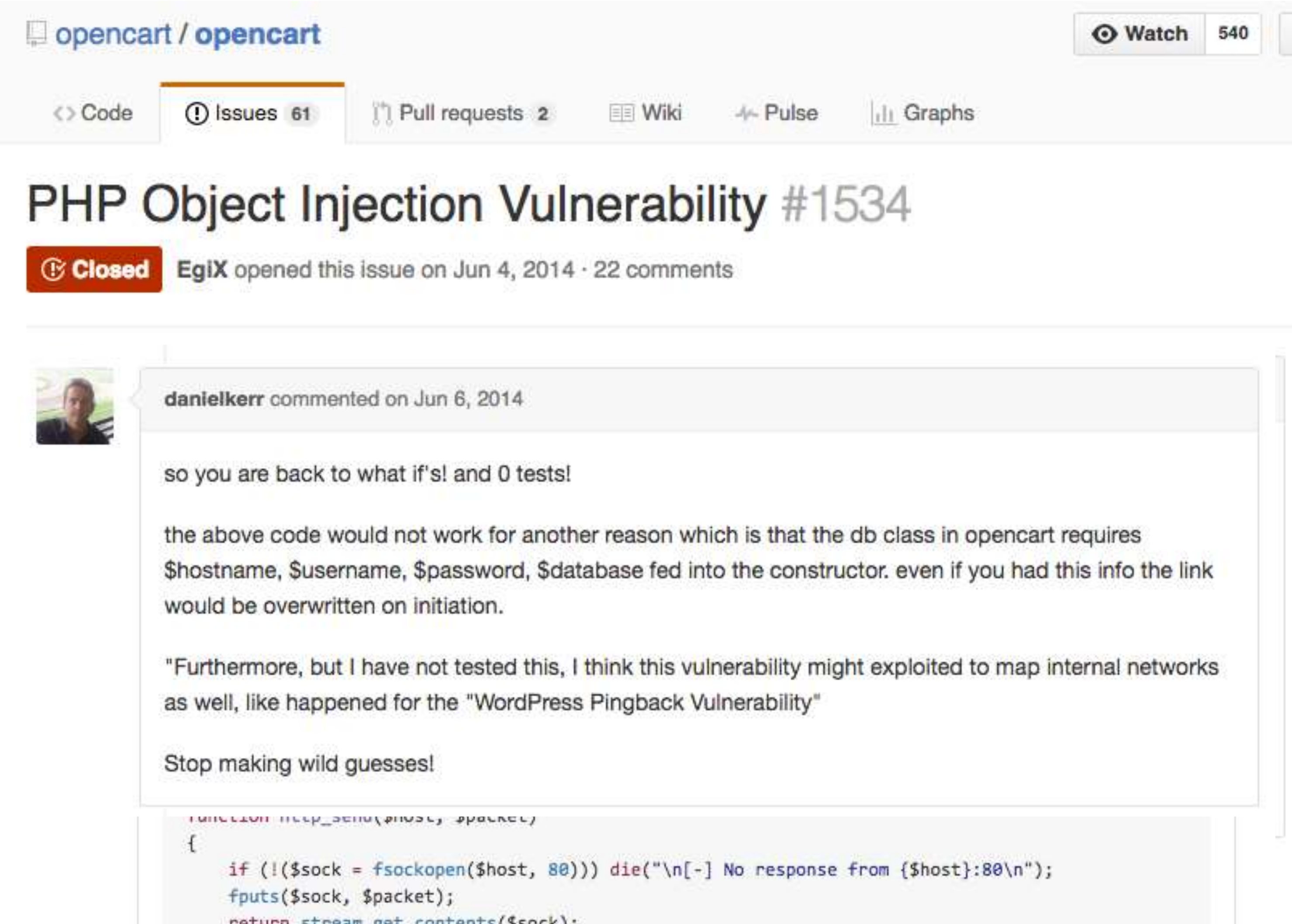
PHP Object Injection Vulnerability #1534

Closed EgiX opened this issue on Jun 4, 2014 · 22 comments

EgiX commented on Jun 6, 2014

I'm gonna ignore all you said just because I realized it's a waste of time try to deal with a stupid like you! However, I can't ignore your last accusation, since before saying that something is vulnerable, I always try to test it by writing a PoC. Since you're continuing to believe this "vulnerability is bullshit", I have no other options, and I have to post the PoC used to confirm it:

```
<?php

error_reporting(E_ERROR);
set_time_limit(0);
ini_set('default_socket_timeout', 5);

function http_send($host, $packet)
{
    if (!($sock = fsockopen($host, 80))) die("\n[-] No response from {$host}:80\n");
    fputs($sock, $packet);
    return stream_get_contents($sock);
```



PHP Object Injection Vulnerability #1534

Closed EgiX opened this issue on Jun 4, 2014 · 22 comments

danielkerr commented on Jun 6, 2014

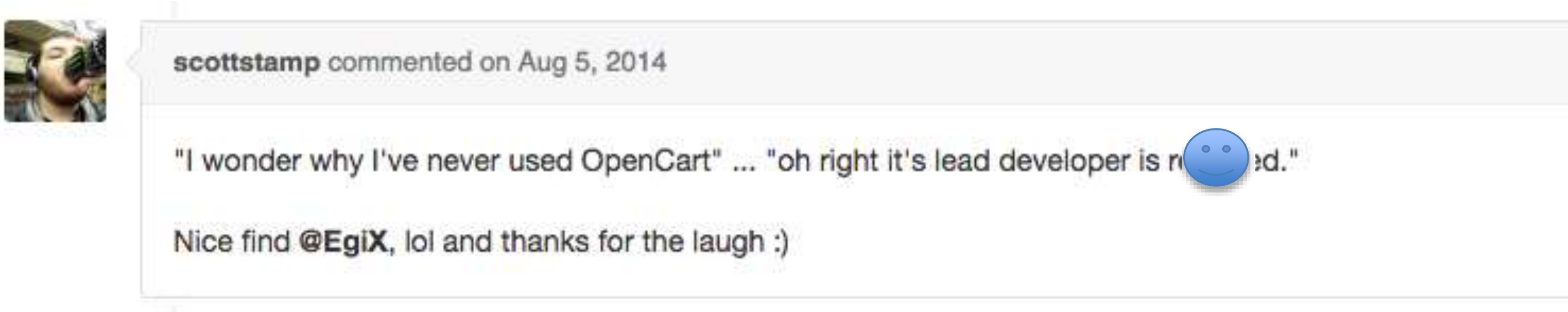
so you are back to what if's! and 0 tests!

the above code would not work for another reason which is that the db class in opencart requires $hostname, $username, $password, $database fed into the constructor. even if you had this info the link would be overwritten on initiation.

"Furthermore, but I have not tested this, I think this vulnerability might exploited to map internal networks as well, like happened for the "WordPress Pingback Vulnerability"

Stop making wild guesses!

```
function http_send($host, $packet)
{
    if (!($sock = fsockopen($host, 80))) die("\n[-] No response from {$host}:80\n");
    fputs($sock, $packet);
    return stream_get_contents($sock);
```



scottstamp commented on Aug 5, 2014

"I wonder why I've never used OpenCart" ... "oh right it's lead developer is r[redacted]ed."

Nice find **@EgiX**, lol and thanks for the laugh :)

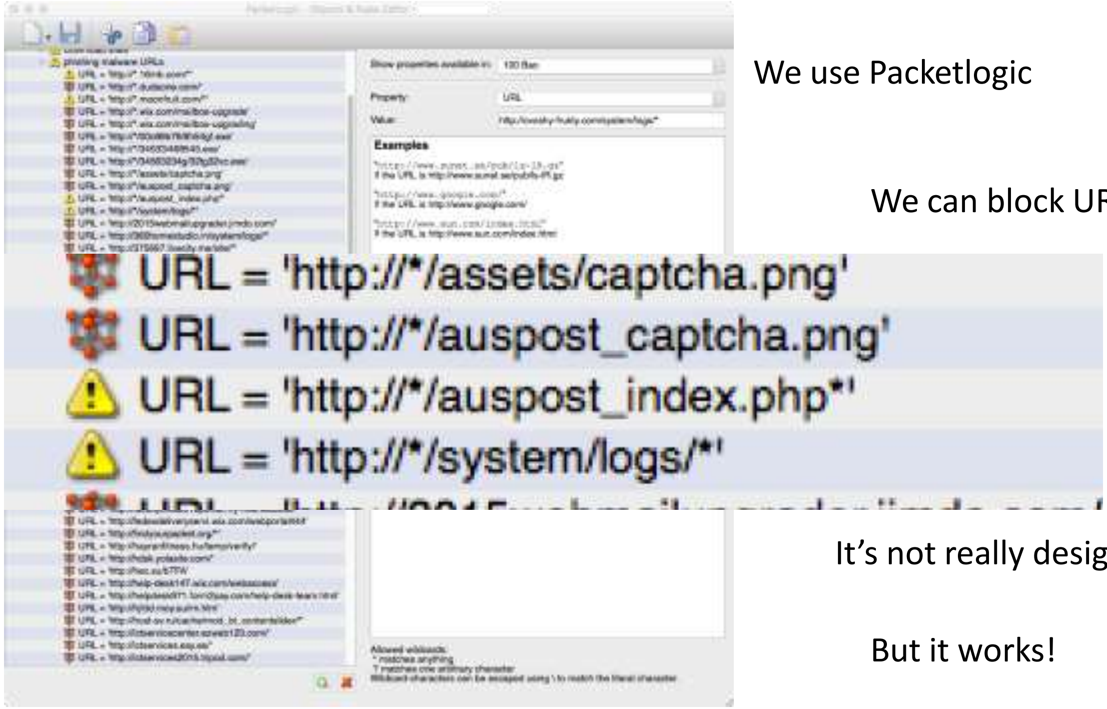
Anyway…

How do we block these sites?
And protect our Staff (or village)

Grrrrr
Help!
51

We use Packetlogic

We can block URL's



phishing malware URLs

```
URL = 'http://*.tknk.com/*'
URL = 'http://*.dudaone.com/*'
URL = 'http://*.macrofuk.com/*'
URL = 'http://*.wix.com/mailbox-upgrade/'
URL = 'http://*.wix.com/mailbox-upgrading/'
URL = 'http://*/[illegible].exe/'
URL = 'http://*/[illegible].exe/'
URL = 'http://*/[illegible].exe/'
URL = 'http://*/assets/captcha.png'
URL = 'http://*/auspost_captcha.png'
URL = 'http://*/auspost_index.php*'
URL = 'http://*/system/logs/*'
URL = 'http://2015webmailupgrader.jimdo.com/'
URL = 'http://[illegible]/system/logs/*'
URL = 'http://[illegible]'
```

```
URL = 'http://*/assets/captcha.png'
URL = 'http://*/auspost_captcha.png'
URL = 'http://*/auspost_index.php*'
URL = 'http://*/system/logs/*'
```

```
URL = 'http://fedexdeliverypanel.wix.com/webportal###'
URL = 'http://findyourpacket.org/*'
URL = 'http://hopranfitness.hu/temp/verify/'
URL = 'http://hdsk.yolasite.com/'
URL = 'http://hec.su/b7FW'
URL = 'http://help-desk147.wix.com/webaccess/'
URL = 'http://helpdesk0971.[illegible].com/help-desk-team.html'
URL = 'http://hyfdd.moy.su/m.html'
URL = 'http://host-sv.ru/[illegible]'
URL = 'http://itservicecenter.[illegible].com/'
URL = 'http://itservices.[illegible]'
URL = 'http://itservices2015.[illegible].com/'
```

Show properties available in: 100 [illegible]

Property: URL

Value: http://[illegible]/system/logs/*

Examples

"http://www.*.sunet.se/pub/[illegible]"
if the URL is http://www.sunet.se/pub/[illegible]

"http://www.*.google.com/*"
if the URL is http://www.google.com/

"http://www.*.sun.com/index.html"
if the URL is http://www.sun.com/index.html

Allowed wildcards:
* matches anything
? matches one arbitrary character
Wildcard characters can be escaped using \ to match the literal character

It's not really designed for this

But it works!

Lets change some processes

- Block some URL's (http://*/system/logs/*)
- Block captcha image (users couldn't see it)
- Report websites to Netcraft, AusCERT
- Try to get websites taken down (AusCERT)
- Educate users
- Clean-up processes (several Cryptowall infections)

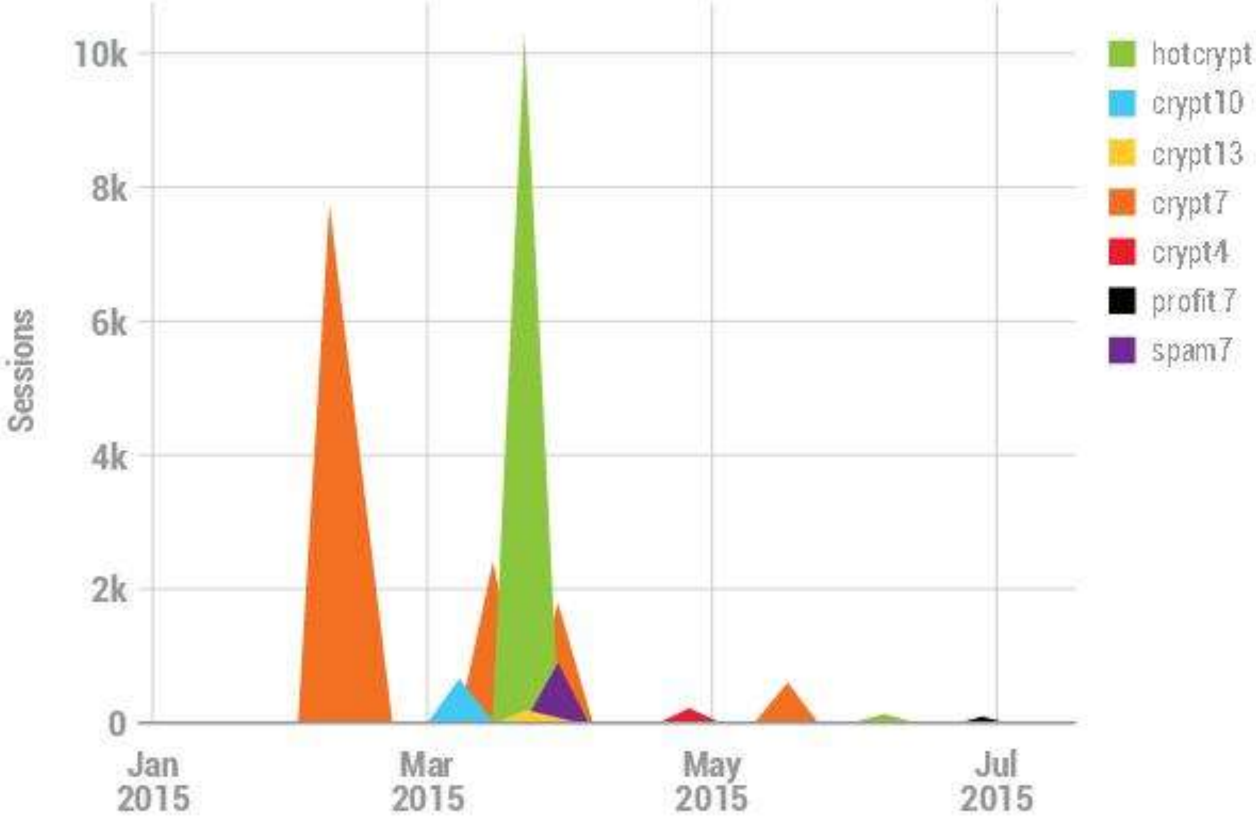
Ransomware Mitigation strategies?

- Considered restricting local Admin rights
- Use IDS alerts to detect users clicking on links
- Block executables running in Appdata/temp folders?
  - Application restrictions in GPO’s
- Scanning fileshares for Cryptolocker files?
- Removed Domain admin rights from every-day login accounts (IT Staff) – provide alt login

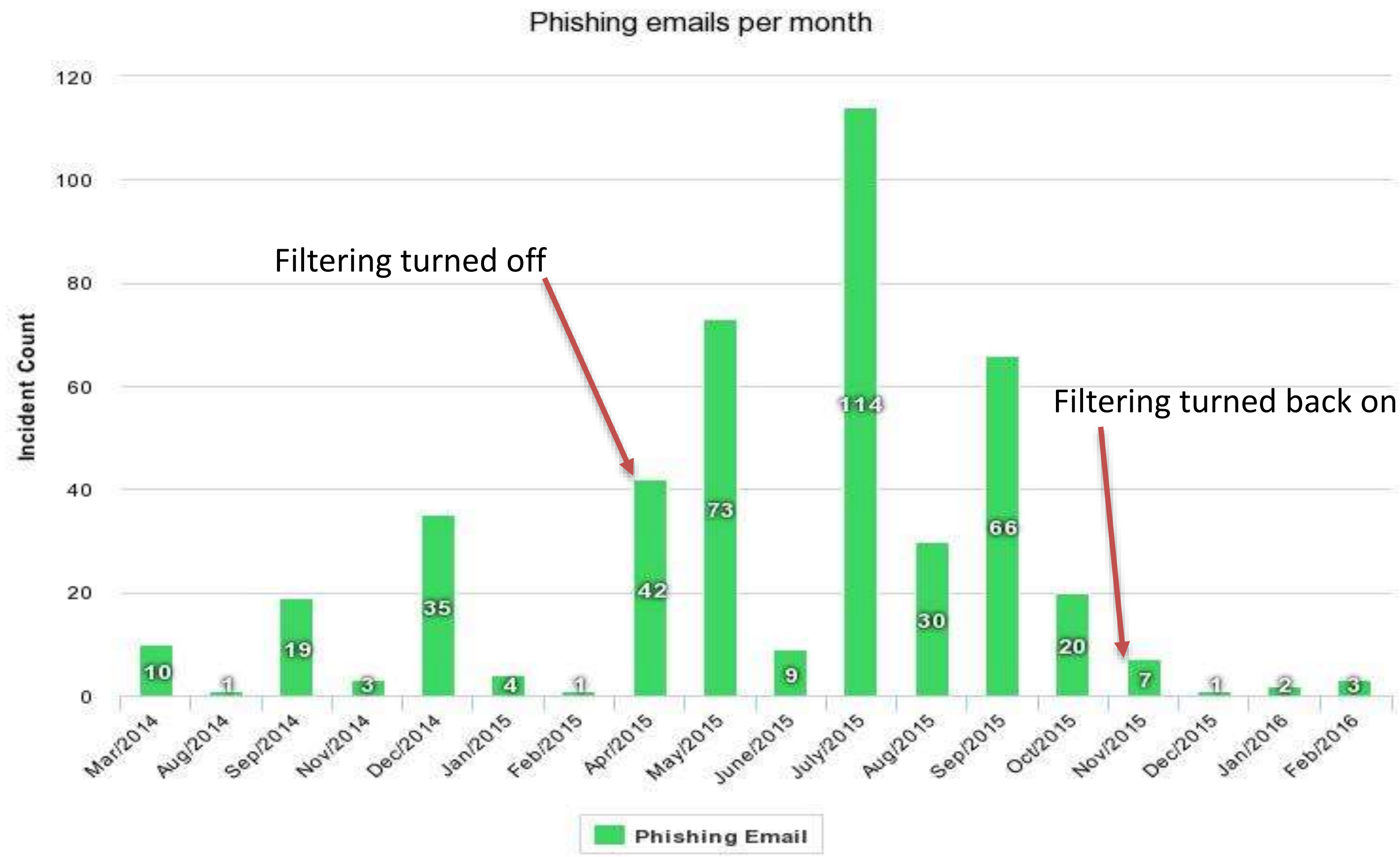
Conclusions

- Office 365 protection not working
- At the time, MS ATP services just released
  - Not available to Education yet, will cost more
- Really need to stop phishing emails
- Produce graphs!
- Campaign for reinstatement of email filter (Symantec.Cloud)

CryptoWall Version 3 Phishing Campaigns



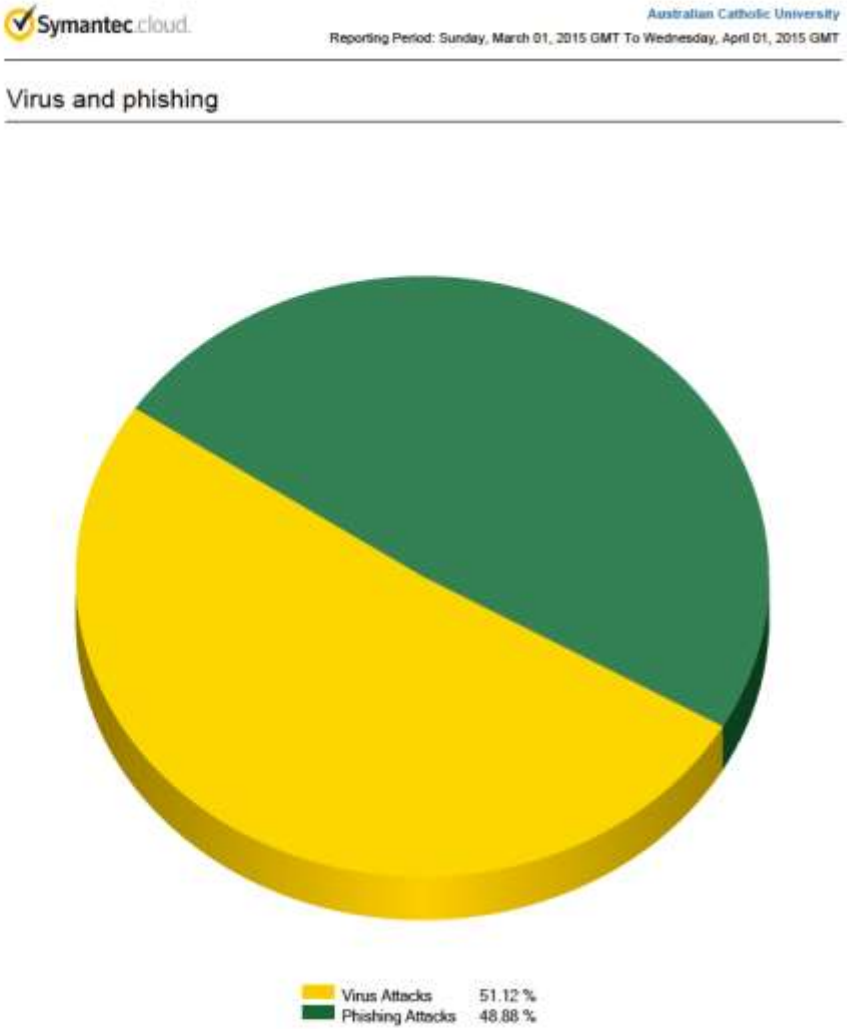
“Reported” phishing emails from Staff
there might have been a lot more!



Filtering turned off

Filtering turned back on

March 2015



Symantec.cloud

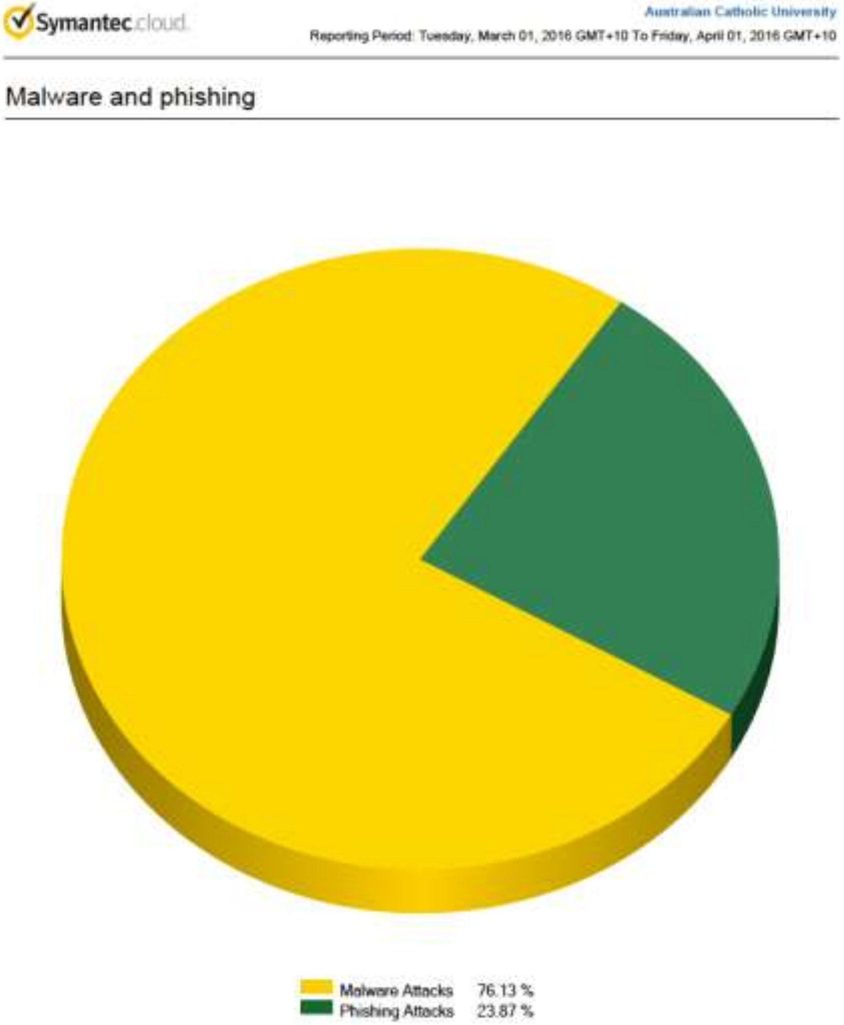
Australian Catholic University

Reporting Period: Sunday, March 01, 2015 GMT To Wednesday, April 01, 2015 GMT

Virus and phishing

🟨	Virus Attacks	51.12 %
🟩	Phishing Attacks	48.88 %

March 2016



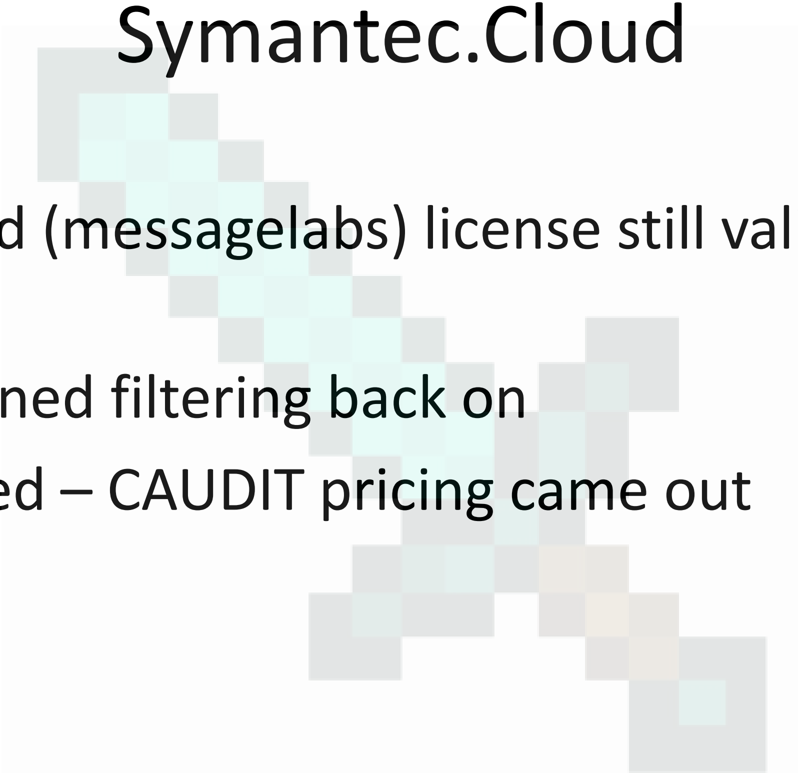
Symantec.cloud

Australian Catholic University

Reporting Period: Tuesday, March 01, 2016 GMT+10 To Friday, April 01, 2016 GMT+10

Malware and phishing

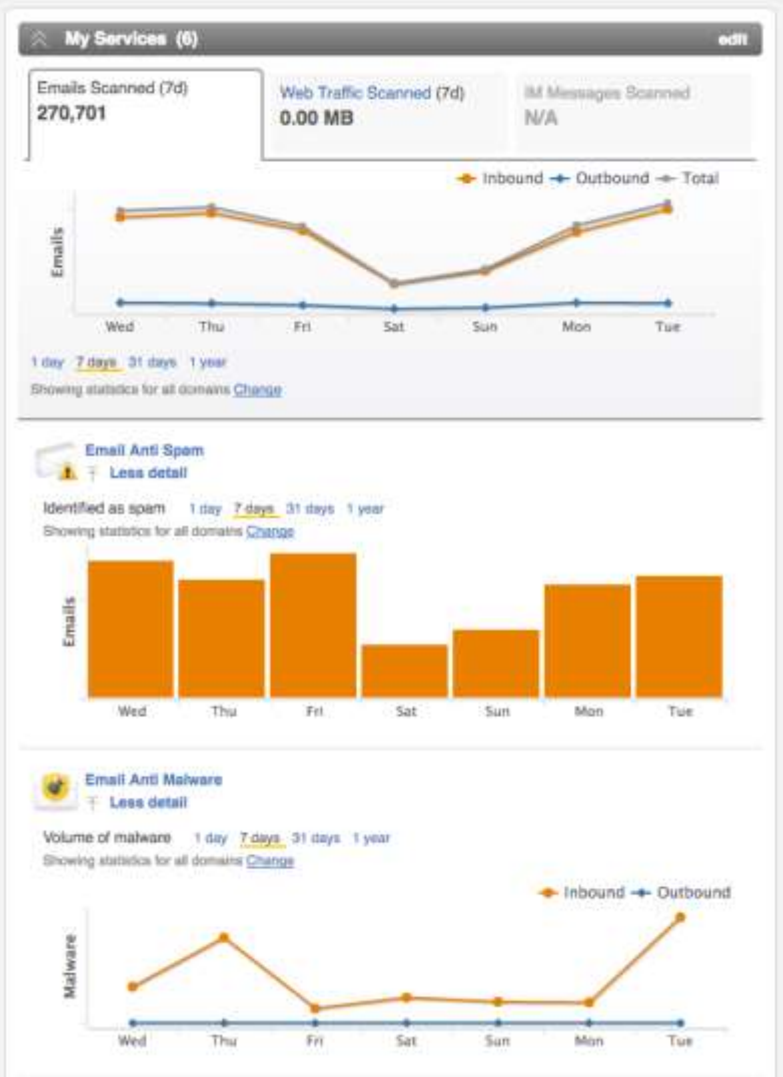
Symantec.Cloud



- Symantec Cloud (messagelabs) license still valid until the end of the year
- Nov 2015 – turned filtering back on
- License renewed – CAUDIT pricing came out
- New features!

Symantec.Cloud

- eMail filtering – includes:
  - Malware
  - Anti-Spam
  - Data protection policies
- MSS – Managed Security Service
- Web filter – agent or proxy
- Customisable reports & Dashboard



My Services (6)

Emails Scanned (7d)
270,701

Web Traffic Scanned (7d)
0.00 MB

IM Messages Scanned
N/A

Showing statistics for all domains Change

Email Anti Spam

Identified as spam

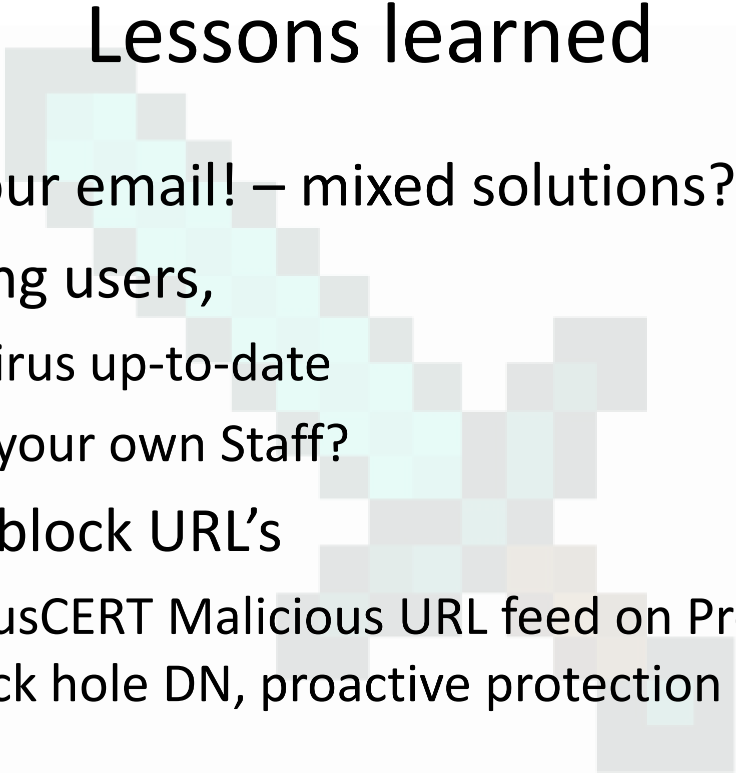
Showing statistics for all domains Change

Email Anti Malware

Volume of malware

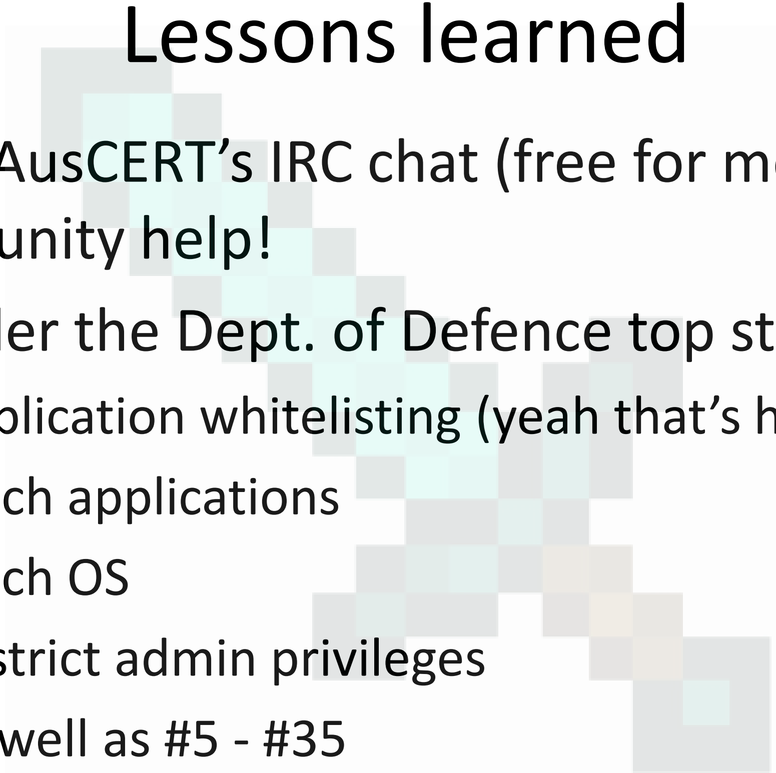
Showing statistics for all domains Change

Lessons learned



- Filter your email! – mixed solutions?
- Educating users,
  - Anti-virus up-to-date
  - Phish your own Staff?
- Able to block URL’s
  - Use AusCERT Malicious URL feed on Proxy servers or black hole DN, proactive protection

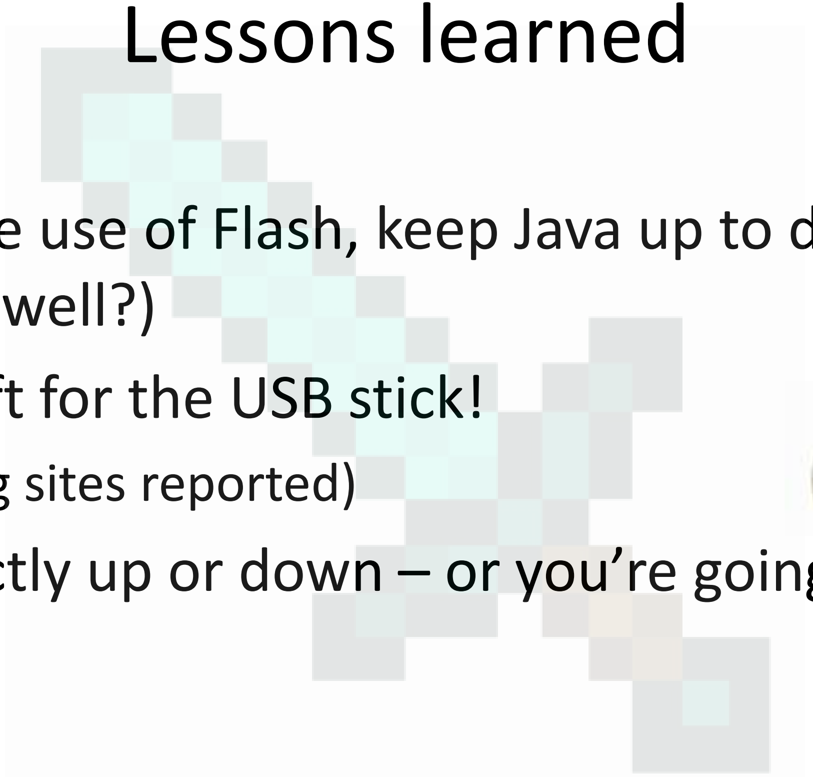
Lessons learned



- Using AusCERT’s IRC chat (free for members) – community help!
- Consider the Dept. of Defence top strategies:
  1. Application whitelisting (yeah that’s hard)
  2. Patch applications
  3. Patch OS
  4. Restrict admin privileges

  – As well as #5 - #35

Lessons learned



- Discontinue the use of Flash, keep Java up to date (or discontinue as well?)
- Thanks Netcraft for the USB stick!
  - (100+ phishing sites reported)
- Never dig directly up or down – or you're going to have a bad time!

Questions?