CyberSecurity MALAYSIA

MOSTI
Ministry of Science,
Technology & Innovation

Handling Incidents from Honeypot data

Adli Wahid
Head, Malaysia CERT (MyCERT)
CyberSecurity Malaysia

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009

Securing Our Cyberspace

Agenda

- MyCERT Honeynet Project
- Handling Data
- Numbers
- Issues

Sharing is Caring

Honeynet @ MyCERT

Phases

1

Deployment

2

Research / Information Sharing

3

~~World Domination~~ Incident Response

1

Deployment

- Distributed
- Components
  - Malware Collection
  - Remote File Inclusion
  - Generic attacks

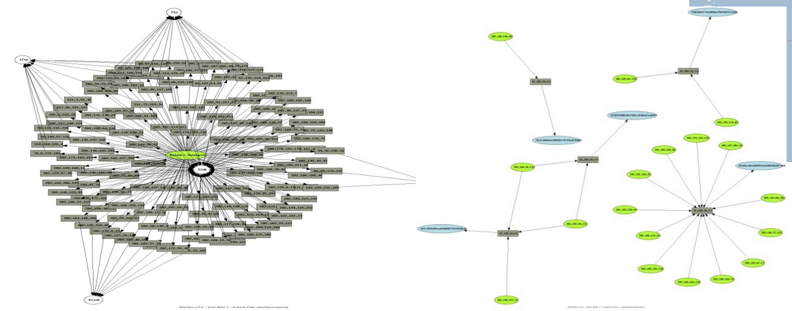
2

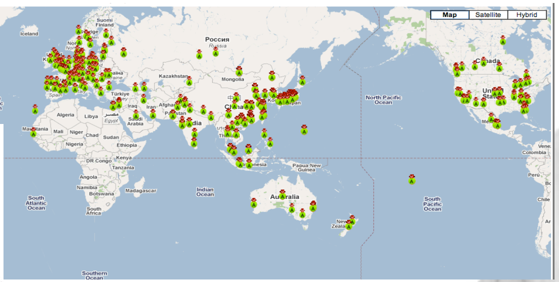
Research / Information Sharing

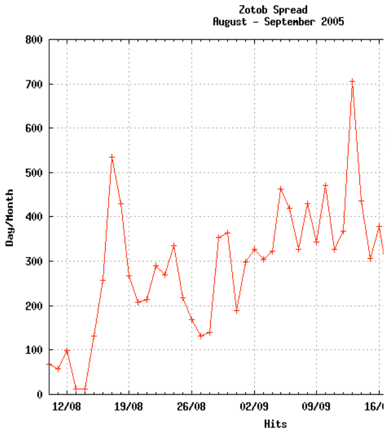
- Threat analysis
- ‘Early Warning’
- Collaboration & Information Sharing

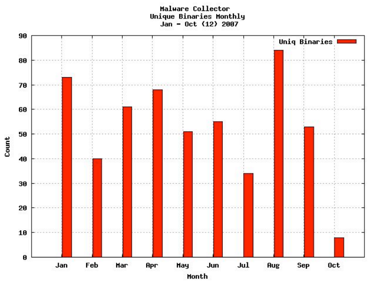
Lebahnet

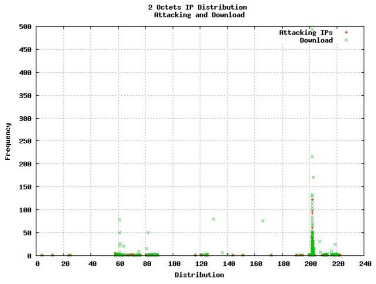
CyberSecurity Malaysia Honeynet Project

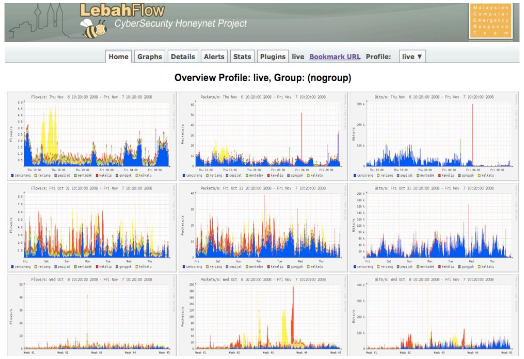




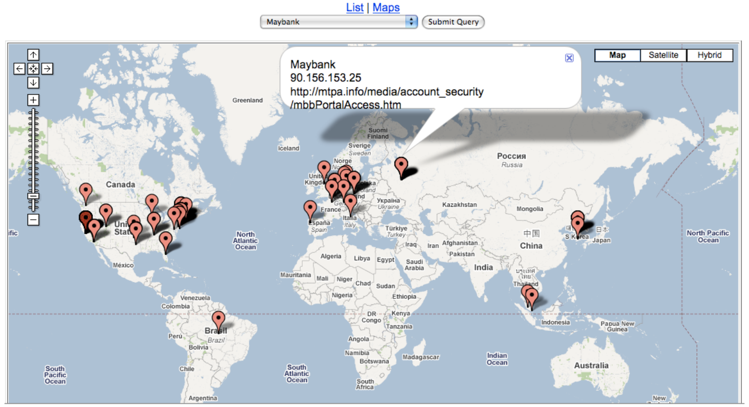




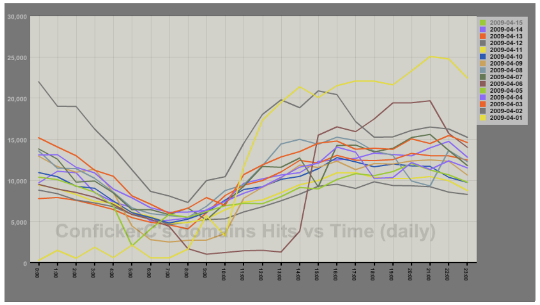




Overview Profile: live, Group: (nogroup)



Maybank
90.156.153.25
http://mtpa.info/media/account_security/mbbPortalAccess.htm



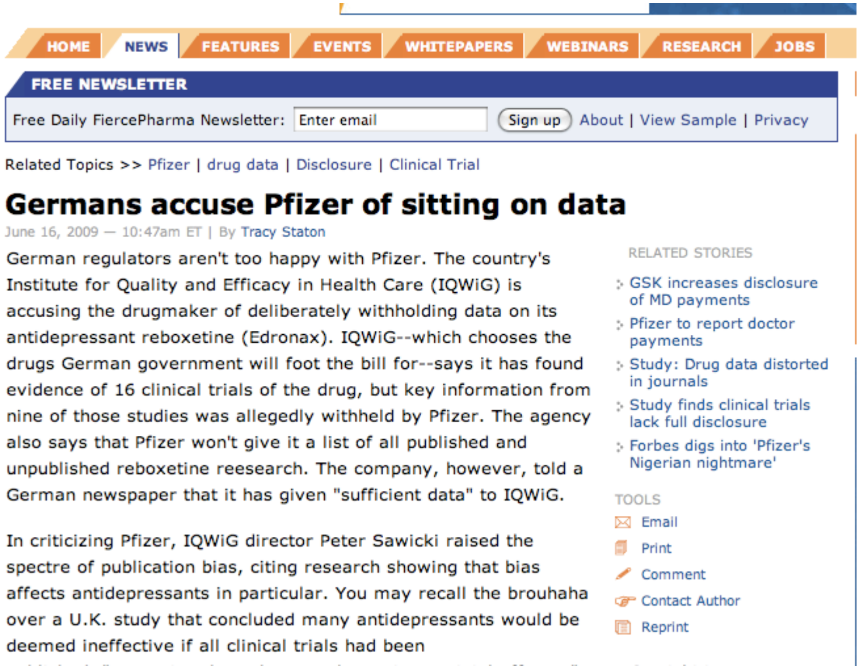
* http://images8.cafepress.com/product/15114178v1_350x350_Front.jpg

Securing Our Cyberspace

- Incident Response Service a.k.a Cyber999
- Atomated Notification

3

Incident Response



Free Daily FiercePharma Newsletter: Enter email Sign up About | View Sample | Privacy

Related Topics >> Pfizer | drug data | Disclosure | Clinical Trial

Germans accuse Pfizer of sitting on data

June 16, 2009 — 10:47am ET | By Tracy Staton

German regulators aren't too happy with Pfizer. The country's Institute for Quality and Efficacy in Health Care (IQWiG) is accusing the drugmaker of deliberately withholding data on its antidepressant reboxetine (Edronax). IQWiG--which chooses the drugs German government will foot the bill for--says it has found evidence of 16 clinical trials of the drug, but key information from nine of those studies was allegedly withheld by Pfizer. The agency also says that Pfizer won't give it a list of all published and unpublished reboxetine reesearch. The company, however, told a German newspaper that it has given "sufficient data" to IQWiG.

In criticizing Pfizer, IQWiG director Peter Sawicki raised the spectre of publication bias, citing research showing that bias affects antidepressants in particular. You may recall the brouhaha over a U.K. study that concluded many antidepressants would be deemed ineffective if all clinical trials had been

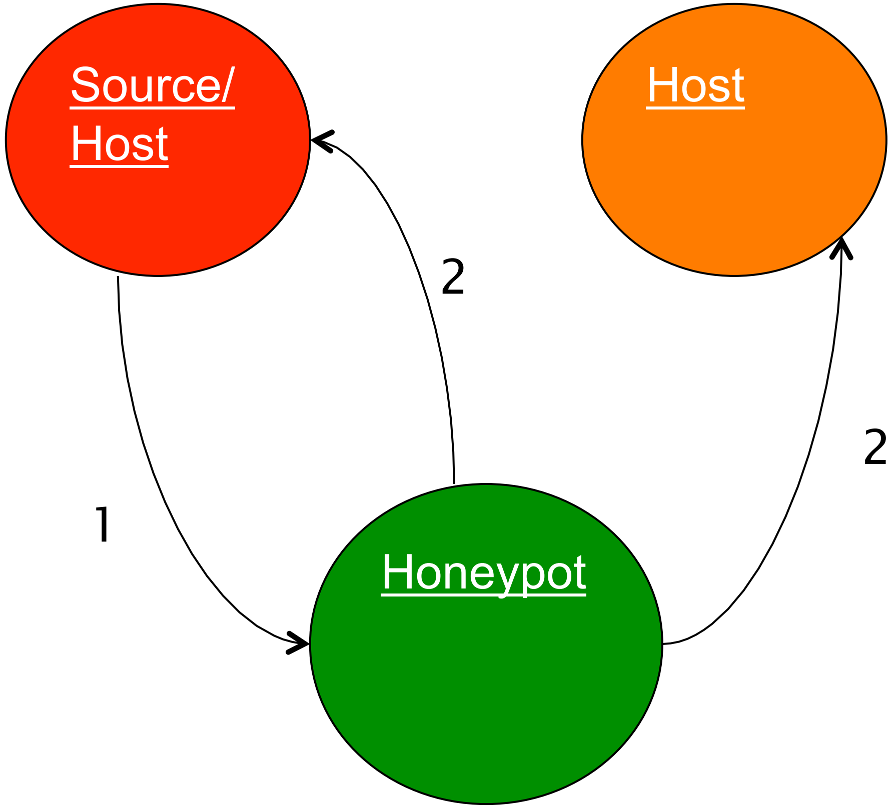
RELATED STORIES

- GSK increases disclosure of MD payments
- Pfizer to report doctor payments
- Study: Drug data distorted in journals
- Study finds clinical trials lack full disclosure
- Forbes digs into 'Pfizer's Nigerian nightmare'

TOOLS

- Email
- Print
- Comment
- Contact Author
- Reprint

Pattern



Generic

1. Source of attack

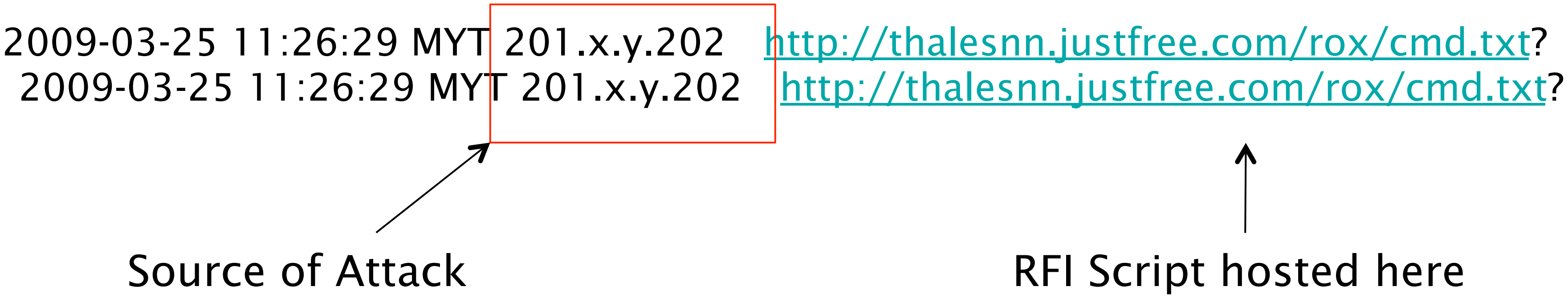
Malware

1. Source of Attack
2. Host hosting the payload / dropper

RFI

1. Source of attack
2. Host hosting the RFI script

Sample RFIpot log

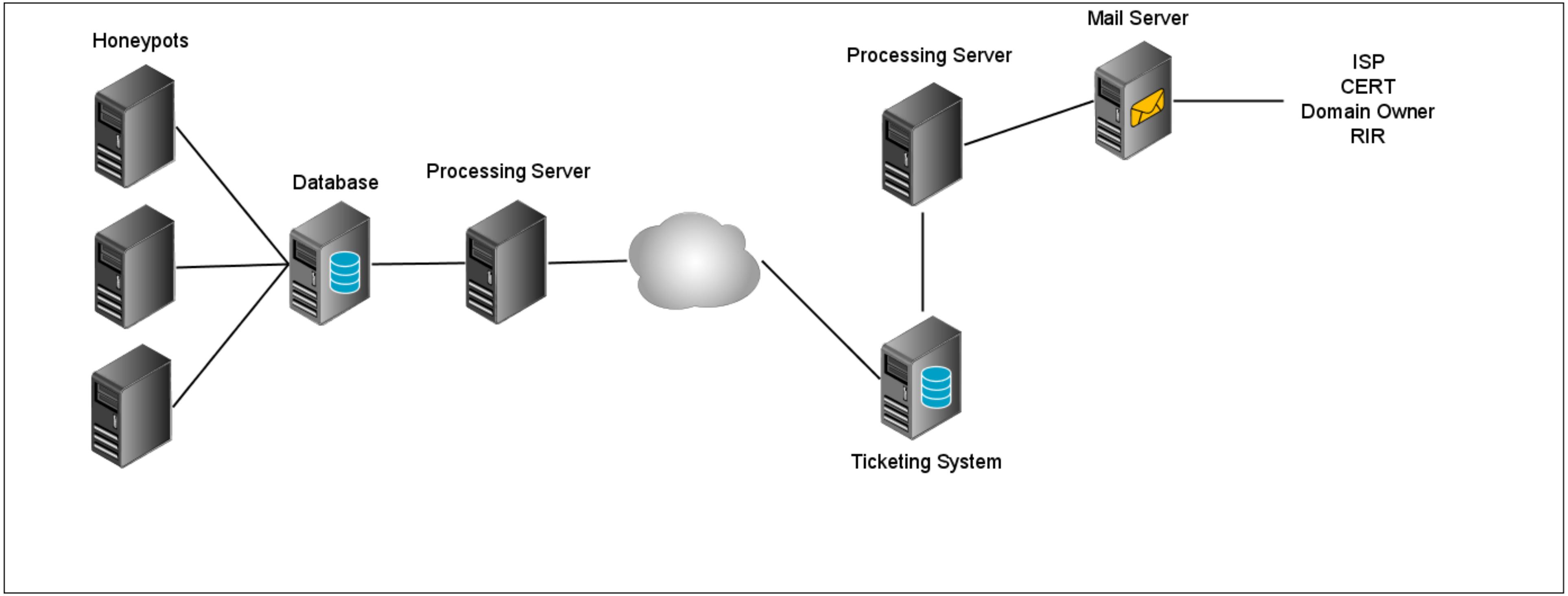


```
2009-03-25 11:26:29 MYT 201.x.y.202   http://thalesnn.justfree.com/rox/cmd.txt?
 2009-03-25 11:26:29 MYT 201.x.y.202   http://thalesnn.justfree.com/rox/cmd.txt?
```

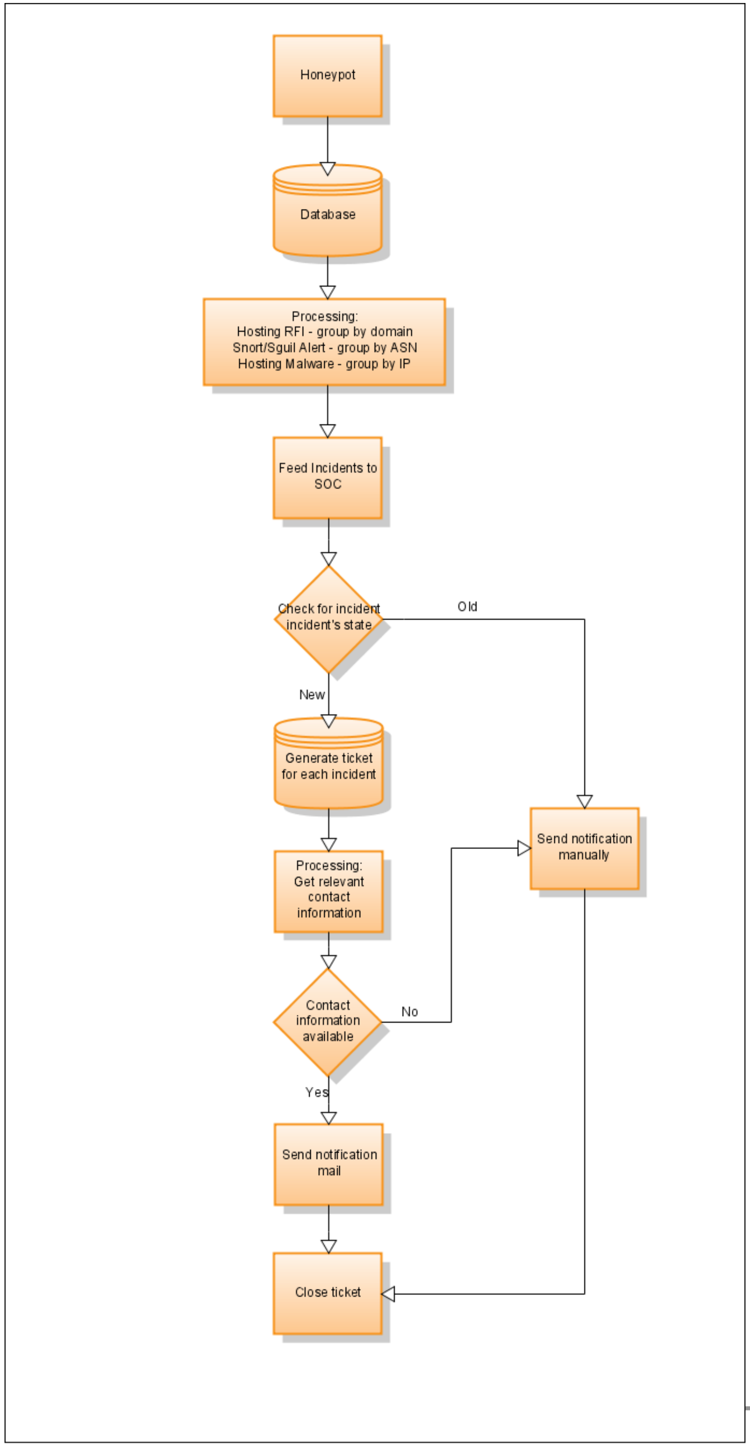
Source of Attack

RFI Script hosted here

LIDHJA.TXT
PBOT.TXT
ID2.TXT
SPREADZ.TXT
IDROSE.TXT
JUNUB.TXT
ALZA.CONF
FX29ID2.TXT
ID16.TXT
SPREAD.TXT
COPYRIGHT.TXT
MIRCO.TXT
TESI.TXT
ID.TXT
BOOT4.TXT
UNIX.TXT
DDOS.TXT
FER.TXT
ROBOTS.TXT
INBOX.TXT
FX29ID.TXT
BOT.TXT
ID1.TXT
PHP.TXT
CMD.TXT
FX29ID1.TXT
TEST.TXT
IDPIT.TXT
README.TXT
VERSION.TXT
NIG.TXT


Honeypots
Database
Processing Server
Processing Server
Mail Server
ISP
CERT
Domain Owner
RIR
Ticketing System

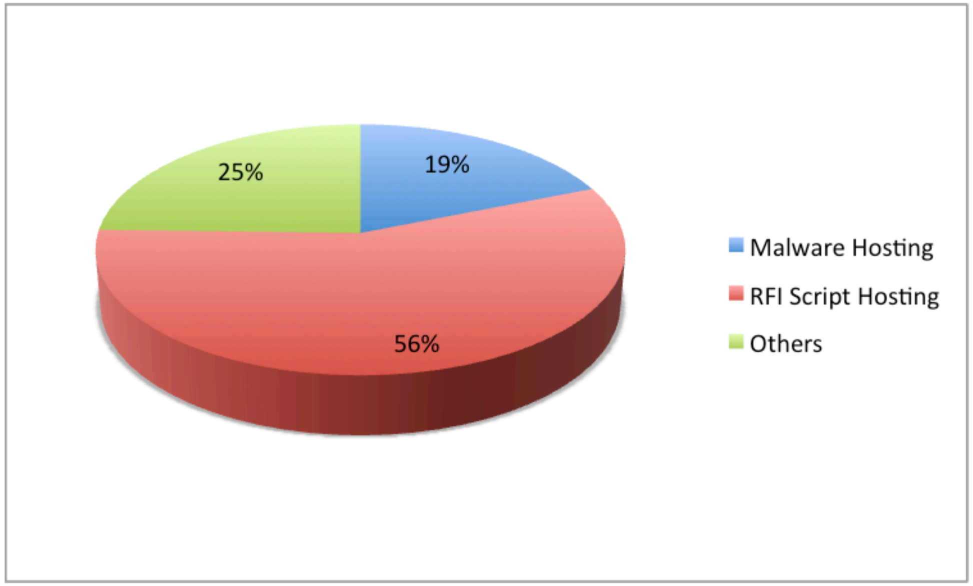
Work Flow


Honeypot
Database
Processing:
Hosting RFI - group by domain
Snort/Sguil Alert - group by ASN
Hosting Malware - group by IP
Feed Incidents to SOC
Check for incident incident's state
Old
New
Generate ticket for each incident
Send notification manually
Processing: Get relevant contact information
Contact information available
No
Yes
Send notification mail
Close ticket

Securing Our Cyberspace

Numbers

- Notifications sent out in 09
  - Q1: 1052
  - Q2: 8481
  - Manual – 93
  - Breakdown
    - Malware hosting: 1799
    - RFI hosting: 5390
    - Other : 2344



Malware template (partial)

```
======================================[ LOG ]======================================

Timestamp: 2009-05-30 21:22:45 GMT+8
IP: 116.x.y.230
Link: ftp://116.x.y.230:30913/ssms.exe
Binary hash: e269d0462eb2b0b70d5e64dcd7c676cd
ClamAV detection: Trojan.SdBot-4763
Avira detection: W32/Trojan5.DCW
Antivir detection: WORM/Rbot.147456.27

======================================================================================
```

We detected the following malicous code used for RFI activity on this resource:

Domain Name = www.some_free_web_hosting_domain.com
Ip a.b.c.e
ASN = XYZ
Country = US

File(s) below exist as per our checking on Sat May 16 10:41:57 +0800 2009

1 - http://www.some_free_web_hosting_domain.com/clim_nonblok/Mistery.txt
2 - http://www.some_free_web_hosting_domain.com/daffa_remex/jembod.txt
3 - http://www.some_free_web_hosting_domain.com/daffa_remex/php.txt
4 - http://www.some_free_web_hosting_domain.com/dedet_hot/phpcohul.txt
5 - http://www.some_free_web_hosting_domain.com/deniseroderick/Send_To.txt
6 - http://www.some_free_web_hosting_domain.com/dinonatadijaya/c.txt
7 - http://www.some_free_web_hosting_domain.com/dinonatadijaya/dd.txt
8 - http://www.some_free_web_hosting_domain.com/dinoshiefa/ds1.txt
9 - http://www.some_free_web_hosting_domain.com/dj.bend/bot.txt
10 - http://www.some_free_web_hosting_domain.com/ginn45/angga.txt
11 - http://www.some_free_web_hosting_domain.com/ginn45/budi3.txt
12 - http://www.some_free_web_hosting_domain.com/ginn45/diam.txt
13 - http://www.some_free_web_hosting_domain.com/ginn45/pingin.txt
14 - http://www.some_free_web_hosting_domain.com/gp_davied/jembod/g.txt
15 - http://www.some_free_web_hosting_domain.com/gp_davied/jembod/load.txt
16 - http://www.some_free_web_hosting_domain.com/Hudhaa86//alnet.txt
17 - http://www.some_free_web_hosting_domain.com/partner_komputer/inject.txt
18 - http://www.some_free_web_hosting_domain.com/sandy_zazmit/fx29id2.txt

Good Responses

Hello,

I'm forwarding your email to the proper contacts for this network so they can investigate this incident.

Thank you for reporting this incident,

Thank you for your report!
The files are deleted and now we are looking how they could come to our customers page.

thanks ans regards

Hello,

Thank you for informing us. The site tampok.xyz.com has been removed from our network.

Best Regards,

Dear MYCERT Administrators,

Thank you for your feedback.

Please be informed that Xnet Abuse has identified the source involved in the unusual activity originating from 202.x.y.202 you have reported on 21 June 2009. Further action has been taken to inhibit such activity.

The relevant administrator of the said IP address has been informed, warned and advised to fix the problem at the soonest time possible.

Good

Hy

i'va delete the directory "letter" , but this attack regulary my space, then he come back when ! delete files, and i don't now how to block it, i'va put in a .htacces this 2 lines :

```
RewriteCond %{QUERY_STRING} ^(.*&)?error=http://
RewriteRule ^(.*/)?errors.php - [F,L]
```

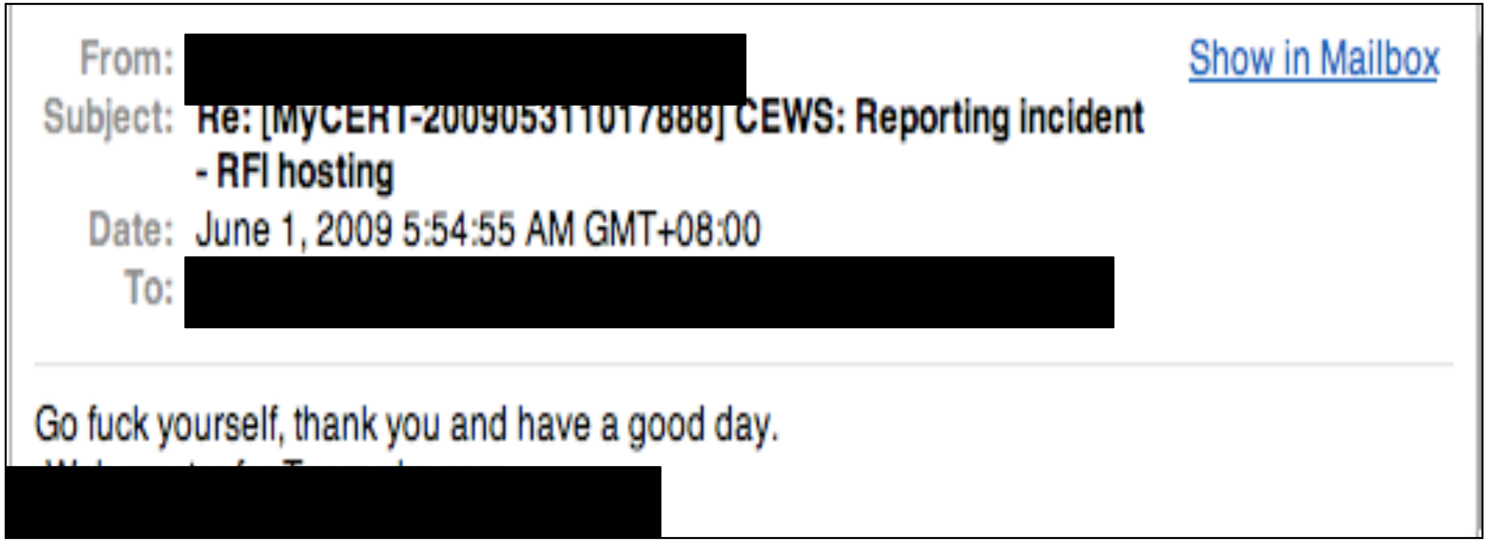
but I'm not shure that ok for this.

To MyCERT,

I have shutdown this server, as it is against our terms and conditions.

Thanks for this report.

Ugly



From: [redacted]

Show in Mailbox

Subject: Re: [MyCERT-200905311017888] CEWS: Reporting incident - RFI hosting

Date: June 1, 2009 5:54:55 AM GMT+08:00

To: [redacted]

Go fuck yourself, thank you and have a good day.

[redacted]

Conclusion

- Additional work
- Need further refinement
- Ideas?
  - ○ adli@cybersecurity.my
  - ○ http://www.mycert.org.my