Handling Incidents from Honeypot data

Adli Wahid
Head, Malaysia CERT (MyCERT)
CyberSecurity Malaysia
Agenda

- MyCERT Honeynet Project
- Handling Data
- Numbers
- Issues
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

- Threat analysis
- ‘Early Warning’
- Collaboration & Information Sharing
* http://images8.cafepress.com/product/15114178v1_350x350_Front.jpg

Securing Our Cyberspace
- Incident Response Service a.k.a Cyber999
- Automated Notification
Pattern

Source/Host -> Honeypot

Honeypot -> Host

Host -> Source/Host
1. Source of attack
2. Host hosting the payload / dropper

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
Securing Our Cyberspace
Securing Our Cyberspace

Work Flow
Numbers

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

IP: 116.x.y.230
Binary hash: e269d0462eb2b0b70d5e64dcd7c676cd
ClamAV detection: Trojan.SdBot-4763
Avira detection: W32/Trojan5.DCW
Antivir detection: WORM/Rbot.147456.27
We detected the following malicious 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

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 regularly my space, then he come back when i delete files, and i don’t now how to block it, i’va put in a .htaccess 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]
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