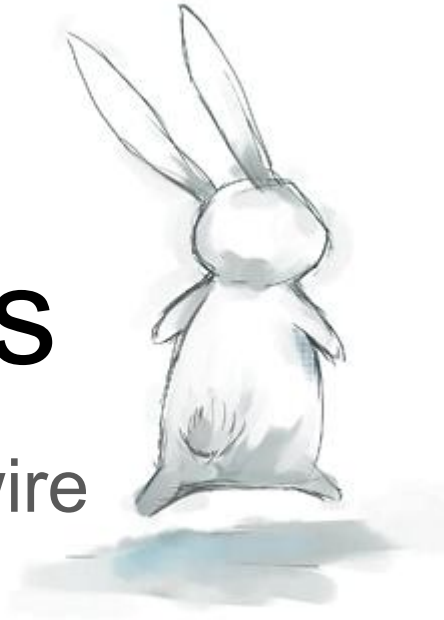
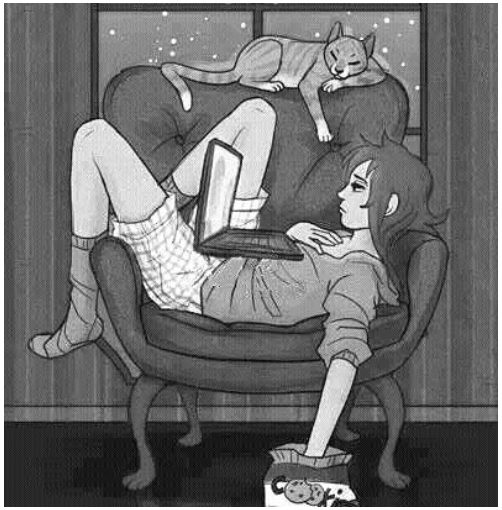
Network Forensics

Follow the Bad Rabbit down the wire



@casheeew

whoami



Essy - @casheeew

2nd time Blackhoodie attendee

I like to learn new stuff (:

Disclaimer

- ETOOMANY sub topics to cover in 30 minutes

→ Dig your own rabbit hole at the end...if you like.

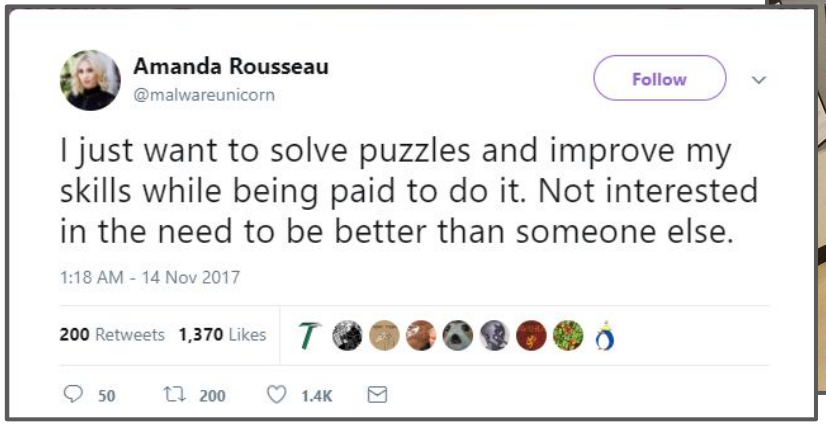
Definition

“Network forensics is the **capturing**, **recording** and **analysis**
of **network events**
in order to discover the source of security attacks.”

- Marcus J. Ranum

Motivation

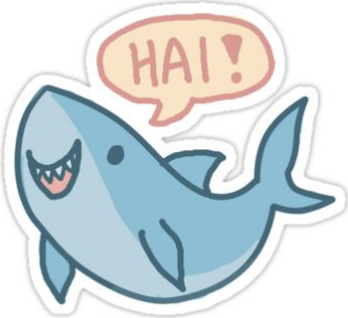
- Packets never lie!
- “Starring packets to death”
- Solving puzzles <3



Technique - Forensic Network Data Types

	Reveals	**Use case**
PCAP	What exactly went across the wire, most complete form of network monitoring	Deep dive & low level
Flow data	Amount of data transferred, time, patterns	Retrospective analysis & statistical flow analysis for traffic that hides in less obvious communications
Log/Alerts	Depending on Loglevel Events, outages, attacks, invalid parameters,....	Aggregated and corelated log analysis

Technique & Tools



Passive traffic capture

- Wireshark!!!11!!
- Microsoft Message Analyzer
- tcpdump, netsh trace, tshark
- strace, dtrace
- Sysinternals Process Monitor
- tcpflow, foremost
- ...

Active traffic capture

- Basically Proxies ¯_(ツ)_/¯
  - Port forwarding-Proxy
  - SOCKS-Proxy
  - HTTP-Proxy
  - Reverse Proxy
- ...

October 24, 2017

A new ransomware attack called Bad Rabbit looks related to NotPetya

Posted Oct 24, 2017 by Taylor Hatmaker (@tayhatmaker)

Bad Rabbit: Ten things you need to know about the latest ransomware outbreak

It's the third major outbreak of the year - here's what we know so far.

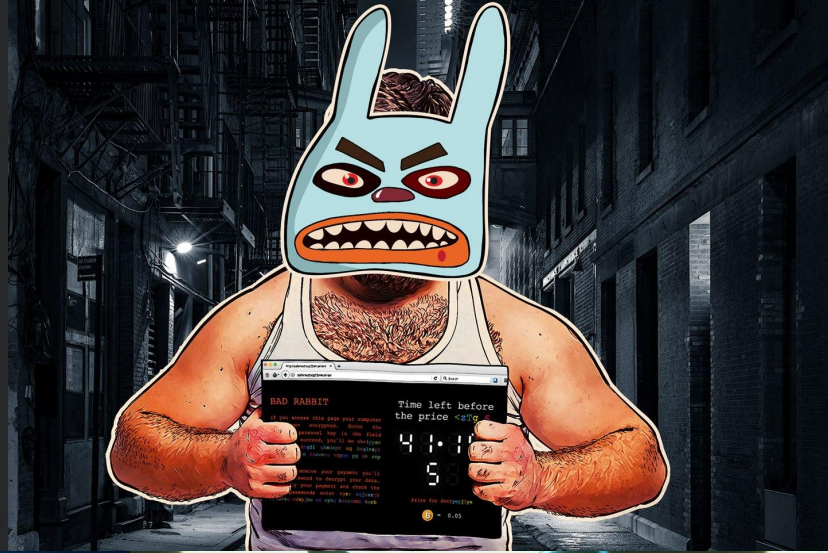
By Danny Palmer | October 25, 2017 -- 10:59 GMT (11:59 BST) | Topic: Security TV - Video Series

Bad Rabbit: Game of Thrones-referencing ransomware hits Europe

NotPetya-style malware infects Kiev's metro system, Odessa airport and Russian media, demanding bitcoin for decryption key

The Bad Rabbit malware was disguised as a Flash update


TALOS


BAD RABBIT
Time left before
the price

Bad Rabbit

Malicious website:
http://1dnscontrol.com/index.php
http://1dnscontrol.com/flash_install.php

install_flash_player.exe

C:\windows\infpub.dat

C:\windows\dspci.exe

C:\windows\cscc.dat

Mimikatz launch (SeDebugPrivilege)

Propagating within network via
- SMB+WMI
- SMB+SCM
- SMB1+MS17-010

file encryption routine

Reboot via scheduled tasks
- drogon
- viserion_<minutes>

Bad Rabbit - Analysis Setup

192.168.56.101
WALNUT\flock3
WinXP SP3 32Bit

192.168.56.102
PEANUT\flock3
WinXP SP3 32Bit

Toolset

Wireshark, tcpflow, foremost

Malware Sample

SHA256:
630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

Bad Rabbit - Capture

Bad Rabbit - Workflow

No.	Time	Source	Destination	Protocol	Length	Info
66	7.530258	192.168.56.102	192.168.56.101	SMB	175	Session Setup AndX Response
67	7.530404	192.168.56.101	192.168.56.102	SMB	156	Tree Connect AndX Request, Path: \\192.168.56.102\ADMIN$
68	7.530767	192.168.56.102	192.168.56.101	SMB	120	Tree Connect AndX Response
69	7.531153	192.168.56.101	192.168.56.255	NBNS	92	Name query NB PEANUT<00>
70	7.531384	192.168.56.101	192.168.56.102	SMB	152	Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path: \cscc.dat
71	7.531502	192.168.56.102	192.168.56.101	NBNS	104	Name query response NB 192.168.56.102
72	7.531526	192.168.56.102	192.168.56.101	SMB	93	Trans2 Response, QUERY_PATH_INFO, Error: STATUS_OBJECT_NAME_NOT_FOUND
73	7.531567	192.168.56.101	192.168.56.102	ICMP	74	Echo (ping) request id=0x0200, seq=256/1, ttl=32 (reply in 74)
74	7.531943	192.168.56.102	192.168.56.101	ICMP	74	Echo (ping) reply id=0x0200, seq=256/1, ttl=128 (request in 73)
75	7.532360	192.168.56.101	192.168.56.102	SMB	166	NT Create AndX Request, FID: 0x4000, Path: \infpub.dat
76	7.532920	192.168.56.102	192.168.56.101	SMB	193	NT Create AndX Response, FID: 0x4000
77	7.532964	192.168.56.101	192.168.56.102	SMB	130	Trans2 Request, QUERY_FILE_INFO, FID: 0x4000, Query File Internal Info
78	7.533273	192.168.56.102	192.168.56.101	SMB	126	Trans2 Response, FID: 0x4000, QUERY_FILE_INFO
79	7.533343	192.168.56.101	192.168.56.102	TCP	1514	1036 → 445 [ACK] Seq=1212 Ack=784 Win=64752 Len=1460 [TCP segment of a reassembled PDU]
80	7.533475	192.168.56.101	192.168.56.102	TCP	1514	1036 → 445 [ACK] Seq=2672 Ack=784 Win=64752 Len=1460 [TCP segment of a reassembled PDU]
81	7.533604	192.168.56.102	192.168.56.101	TCP	60	445 → 1036 [ACK] Seq=784 Ack=4132 Win=65535 Len=0
82	7.533622	192.168.56.101	192.168.56.102	TCP	1514	1036 → 445 [ACK] Seq=4132 Ack=784 Win=64752 Len=1460 [TCP segment of a reassembled PDU]

```
QUERY_PATH_INFO Parameters
    Level of Interest: Query File Basic Info (1004)
    Reserved: 00000000
    File Name: \cscc.dat
```

```
0000  08 00 27 33 62 45 08 00  27 7d 0c 01 08 00 45 00   ..'3bE.. '}....E.
0010  00 8a 00 60 40 00 80 06  07 f2 c0 a8 38 65 c0 a8   ...`@... ....8e..
0020  38 66 04 0c 01 bd 7c 23  6a 12 e4 e8 e4 e8 50 18   8f....|# j.....P.
0030  fd ea f2 98 00 00 00 00  00 5e ff 53 4d 42 32 00   ........ .^.SMB2.
0040  00 00 00 18 07 c8 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 08 d8 05 00 08  40 00 0f 1a 00 00 00 02   ........ @.......
0060  00 28 00 00 00 00 00 00  00 00 00 00 00 1a 00 44   .(...... .......D
0070  00 00 00 00 00 01 00 05  00 1d 00 00 00 00 ec 03   ........ ........
0080  00 00 00 00 5c 00 63 00  73 00 63 00 63 00 2e 00   ....\.c. s.c.c...
0090  64 00 61 00 74 00 00 00                            d.a.t...
```

Bad Rabbit - Workflow

No.	Time	Source	Destination	Protocol	Length	Info
4…	7.563238	192.168.56.102	192.168.56.101	SMB	114	Tree Connect AndX Response
4…	7.564192	192.168.56.101	192.168.56.102	SMB	158	NT Create AndX Request, FID: 0x4001, Path: \svcctl
4…	7.564548	192.168.56.102	192.168.56.101	SMB	193	NT Create AndX Response, FID: 0x4001
4…	7.565552	192.168.56.101	192.168.56.102	DCERPC	194	Bind: call_id: 1, Fragment: Single, 1 context items: SVCCTL V2.0 (32bit NDR)
4…	7.565826	192.168.56.102	192.168.56.101	SMB	105	Write AndX Response, FID: 0x4001, 72 bytes
4…	7.565917	192.168.56.101	192.168.56.102	SMB	117	Read AndX Request, FID: 0x4001, 1024 bytes at offset 0
4…	7.566167	192.168.56.102	192.168.56.101	DCERPC	186	Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance
4…	7.566296	192.168.56.101	192.168.56.102	SVCCTL	222	OpenSCManagerW request, 192.168.56.102
4…	7.567047	192.168.56.102	192.168.56.101	SVCCTL	162	OpenSCManagerW response
4…	7.567104	192.168.56.101	192.168.56.102	SVCCTL	422	CreateServiceW request
4…	7.573878	192.168.56.102	192.168.56.101	SVCCTL	166	CreateServiceW response
4…	7.574018	192.168.56.101	192.168.56.102	SVCCTL	194	StartServiceW request
4…	7.608273	192.168.56.102	192.168.56.101	SVCCTL	142	StartServiceW response
4…	7.608446	192.168.56.101	192.168.56.102	SVCCTL	186	QueryServiceStatus request
4…	7.608707	192.168.56.102	192.168.56.101	SVCCTL	170	QueryServiceStatus response
5…	7.608811	192.168.56.101	192.168.56.102	SVCCTL	186	DeleteService request
5…	7.609189	192.168.56.102	192.168.56.101	SVCCTL	142	DeleteService response
5…	7.609278	192.168.56.101	192.168.56.102	SVCCTL	186	CloseServiceHandle request, (null)
5…	7.609523	192.168.56.102	192.168.56.101	SVCCTL	162	CloseServiceHandle response
5…	7.609584	192.168.56.101	192.168.56.102	SVCCTL	186	CloseServiceHandle request, OpenSCManagerW(192.168.56.102\)
5…	7.609968	192.168.56.102	192.168.56.101	SVCCTL	162	CloseServiceHandle response

```
> Service Type: 0x00000010
  Service Start Type: SERVICE_DEMAND_START (3)
  Service Error Control: SERVICE_ERROR_IGNORE (0)
> Binary Path Name: C:\Windows\System32\rundll32.exe "C:\Windows\infpub.dat",#2 15
  NULL Pointer: Load Order Group
  Tag Id: 0
```

```
00e0  42 00 34 00 30 00 00 00  41 00 00 00 00 00 ff 01   B.4.0... A.......
00f0  0f 00 10 00 00 00 03 00  00 00 00 00 00 00 3f 00   ........ ......?.
0100  00 00 00 00 00 00 3f 00  00 00 43 00 3a 00 5c 00   ......?. ..C.:.\.
0110  57 00 69 00 6e 00 64 00  6f 00 77 00 73 00 5c 00   W.i.n.d. o.w.s.\.
0120  53 00 79 00 73 00 74 00  65 00 6d 00 33 00 32 00   S.y.s.t. e.m.3.2.
0130  5c 00 72 00 75 00 6e 00  64 00 6c 00 6c 00 33 00   \.r.u.n. d.l.l.3.
0140  32 00 2e 00 65 00 78 00  65 00 20 00 22 00 43 00   2...e.x. e. .".C.
0150  3a 00 5c 00 57 00 69 00  6e 00 64 00 6f 00 77 00   :.\.W.i. n.d.o.w.
0160  73 00 5c 00 69 00 6e 00  66 00 70 00 75 00 62 00   s.\.i.n. f.p.u.b.
0170  2e 00 64 00 61 00 74 00  22 00 2c 00 23 00 32 00   ..d.a.t. ".,.#.2.
0180  20 00 31 00 35 00 00 00  00 00 00 00 00 00 00 00    .1.5... ........
```

Bad Rabbit - Workflow

No.	Time	Source	Destination	Protocol	Length	Info
5…	7.609968	192.168.56.102	192.168.56.101	SVCCTL	162	CloseServiceHandle response
5…	7.610021	192.168.56.101	192.168.56.102	SMB	99	Close Request, FID: 0x4001
5…	7.610458	192.168.56.102	192.168.56.101	SMB	93	Close Response, FID: 0x4001
5…	7.671476	192.168.56.101	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x32d3a65c
5…	7.781128	192.168.56.101	192.168.56.102	TCP	54	1036 → 445 [ACK] Seq=414147 Ack=2329 Win=64768 Len=0
5…	10.485254	192.168.56.101	192.168.56.100	TCP	62	[TCP Retransmission] 1038 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5…	10.485692	192.168.56.101	192.168.56.100	TCP	62	[TCP Retransmission] 1039 → 139 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5…	10.676335	192.168.56.101	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x32d3a65c
5…	11.486686	PcsCompu_7d:0c:01	Broadcast	ARP	42	Who has 192.168.56.1? Tell 192.168.56.101
5…	11.487143	0a:00:27:00:00:07	PcsCompu_7d:0c:01	ARP	60	192.168.56.1 is at 0a:00:27:00:00:07
5…	11.487157	192.168.56.101	192.168.56.1	TCP	62	1043 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5…	11.488019	192.168.56.1	192.168.56.101	TCP	62	445 → 1043 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
5…	11.488051	192.168.56.101	192.168.56.1	TCP	54	1043 → 445 [ACK] Seq=1 Ack=1 Win=65535 Len=0
5…	11.488227	192.168.56.101	192.168.56.1	TCP	54	1043 → 445 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
5…	11.488656	192.168.56.1	192.168.56.101	TCP	60	445 → 1043 [ACK] Seq=1 Ack=2 Win=64240 Len=0
5…	11.488672	192.168.56.1	192.168.56.101	TCP	60	445 → 1043 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
5…	11.488992	PcsCompu_7d:0c:01	Broadcast	ARP	42	Who has 192.168.56.2? Tell 192.168.56.101
5…	13.737209	PcsCompu_33:62:45	Broadcast	ARP	60	Who has 192.168.56.1? Tell 192.168.56.102
5…	13.737224	0a:00:27:00:00:07	PcsCompu_33:62:45	ARP	60	192.168.56.1 is at 0a:00:27:00:00:07
5…	13.737410	192.168.56.102	192.168.56.1	TCP	62	1034 → 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5…	13.737480	192.168.56.1	192.168.56.102	TCP	62	445 → 1034 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Bad Rabbit - Workflow

```
flock4@box:~$ tcpflow -r capture.pcapng -o tcpflows
flock4@box:~$ ls -l tcpflows/
total 460
-rw-rw-r-- 1 flock4 flock4    953 Nov 19 15:37 192.168.056.101.01033-192.168.056.102.00139
-rw-rw-r-- 1 flock4 flock4    961 Nov 19 15:37 192.168.056.101.01035-192.168.056.102.00139
-rw-rw-r-- 1 flock4 flock4 414267 Nov 19 15:37 192.168.056.101.01036-192.168.056.102.00445
-rw-rw-r-- 1 flock4 flock4    209 Nov 19 15:37 192.168.056.101.01041-192.168.056.102.00139
-rw-rw-r-- 1 flock4 flock4    137 Nov 19 15:37 192.168.056.101.01048-192.168.056.001.00445
-rw-rw-r-- 1 flock4 flock4   1063 Nov 19 15:37 192.168.056.101.01054-192.168.056.102.00139
-rw-rw-r-- 1 flock4 flock4    714 Nov 19 15:37 192.168.056.102.00139-192.168.056.101.01033
-rw-rw-r-- 1 flock4 flock4    741 Nov 19 15:37 192.168.056.102.00139-192.168.056.101.01035
-rw-rw-r-- 1 flock4 flock4     93 Nov 19 15:37 192.168.056.102.00139-192.168.056.101.01041
-rw-rw-r-- 1 flock4 flock4    641 Nov 19 15:37 192.168.056.102.00139-192.168.056.101.01054
-rw-rw-r-- 1 flock4 flock4   2449 Nov 19 15:37 192.168.056.102.00445-192.168.056.101.01036
-rw-rw-r-- 1 flock4 flock4  11289 Nov 22 16:57 report.xml
flock4@box:~$
```

Bad Rabbit - Workflow

```
flock4@box:~/tcpflows$ foremost -T -i *
Processing: 192.168.056.101.01033-192.168.056.102.00139
|*|
Processing: 192.168.056.101.01035-192.168.056.102.00139
|*|
Processing: 192.168.056.101.01036-192.168.056.102.00445
|*|
Processing: 192.168.056.101.01041-192.168.056.102.00139
|*|
Processing: 192.168.056.101.01048-192.168.056.001.00445
|*|
Processing: 192.168.056.101.01054-192.168.056.102.00139
|*|
Processing: 192.168.056.102.00139-192.168.056.101.01033
|*|
Processing: 192.168.056.102.00139-192.168.056.101.01035
|*|
Processing: 192.168.056.102.00139-192.168.056.101.01041
|*|
Processing: 192.168.056.102.00139-192.168.056.101.01054
|*|
Processing: 192.168.056.102.00445-192.168.056.101.01036
|*|
```

```
flock4@box:~/tcpflows$ tree output/
output/
├── audit.txt
└── dll
    └── 00000002.dll

1 directory, 2 files
```

```
flock4@box:~/tcpflows$ sha256sum output/dll/*
79acf0106c2bf585d41163a6a63460951c857331009e25d5f3266b980a4d7330  output/dll/00000002.dll
```

Bad Rabbit - Workflow

32 / 66

32 engines detected this file

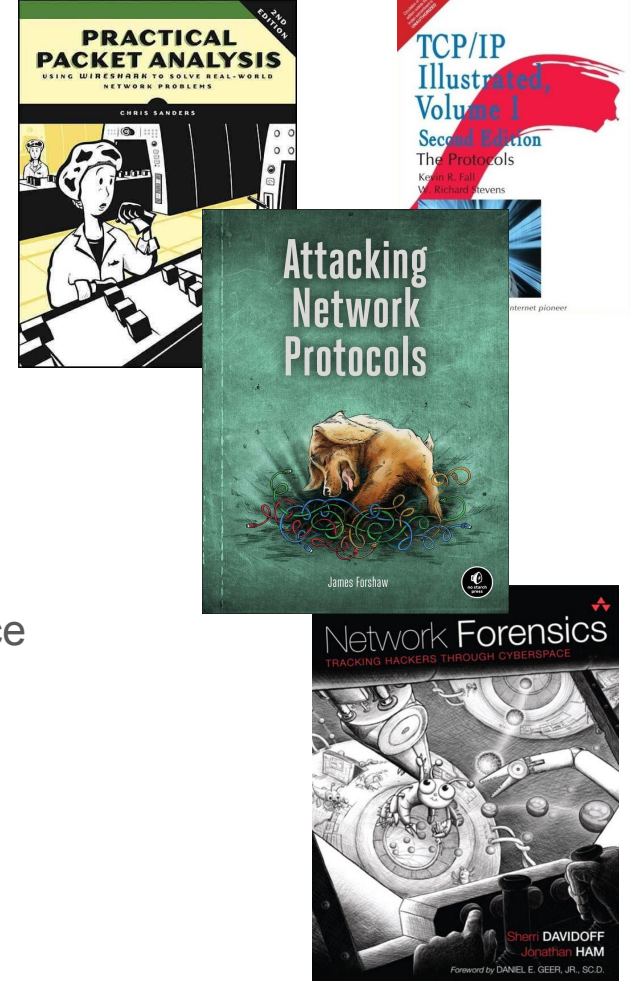
SHA-256	79acf0106c2bf585d41163a6a63460951c857331009e25d5f3266b980a4d7330
File name	00000002.dll
File size	388 KB
Last analysis	2017-11-22 21:27:43 UTC

Detection | Details | Community

Ad-Aware	Gen:Heur.Ransom.BadRabbit.1	ALYac	Gen:Heur.Ransom.BadRabbit.1
Arcabit	Trojan.Ransom.BadRabbit.1	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	BitDefender	Gen:Heur.Ransom.BadRabbit.1
Bkav	W32.RabInND.Worm	CAT-QuickHeal	Ransom.BadRabbit.A5

Down the rabbit hole…**Books!**

- TCP/IP Ilustrated - W. Richard Stevens
- Attacking Network Protocols - James Forshaw
- Practical Packet Analysis - Chris Sanders
- Network Forensics - Tracking Hackers through Cyberspace
  Sherri Davidoff, Jonathan Ham
- SANS Institute Reading Room
  https://www.sans.org/reading-room/



Down the rabbit hole…**Conferences&Trainings**

- SharkFest https://www.youtube.com/user/SharkFest2015/playlists
  - e.g. SF16EU - Forensic Network Analysis by Christian Landström
  - incl. SharkBytes

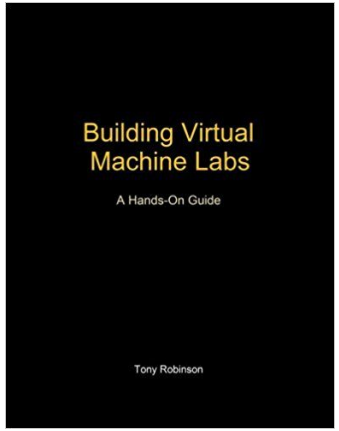
- @netdetect - Betty DuBois
  - https://www.netdetect.co/sharkfest-europe

- @LauraChappell
  - Wireshark Core Training Courses
    https://www.youtube.com/playlist?list=PL_yWypNx3Y8A279XnAEVqYjNl0HJ7_MFV

Down the rabbit hole… **Practice**

- @malware_traffic
  - http://www.malware-traffic-analysis.net
- http://forensicscontest.com/puzzles
- CTF Forensic Challenges, hint: https://ctftime.org/tasks/?hidden-tags=network%2Cforensics

& Setup a suitable lab environment (@da_667 might help)



```
$ strace -e trace=network,write presentation
...
socket(PF_INET, SOCK_STREAM, IPPROTO_TCP) = 3
connect(3, {sa_family=AF_INET, sin_port=htons(1337),
            sin_addr=inet_addr("255.255.255.255")}, 16) = 0
write(3, "Thank your for your attention!\n", 31) = 31
...
```