Copyright © 2015 Splunk Inc.

Hunting the Known Unknowns (with DNS)

Ryan Kovar and Steve Brant

Security Strategists @ Splunk

splunk>

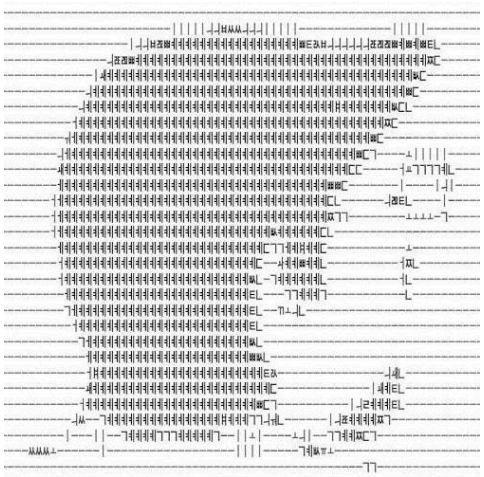
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

whoami

Ryan Kovar: CISSP, MSc(Dist)



Staff Security Strategist

Minster of the OODAloopers

@meansec

- 15 Years of cyber security experience
- Worked in US/UK Public Sector and DOD most recently in nation state hunting roles
- Enjoys clicking too fast, long walks in the woods, and data visualization
- Current role on Security Practice team focuses on incident/breach response, threat intelligence, and research
- Currently interested in automating methods to triage data collection for IR analyst review.
- Also investigating why printers are so insubordinate ಠ_ಠ

whoami

Steve Brant: CISSP

Security Strategist
Minister of Truth
@trustedtech

- 22 Years in the IT biz
- 7 Years in Security Information and Event Management
- Novice beer snob
- Working on improving the Splunk ES out of the box experience with improved workflow and searches

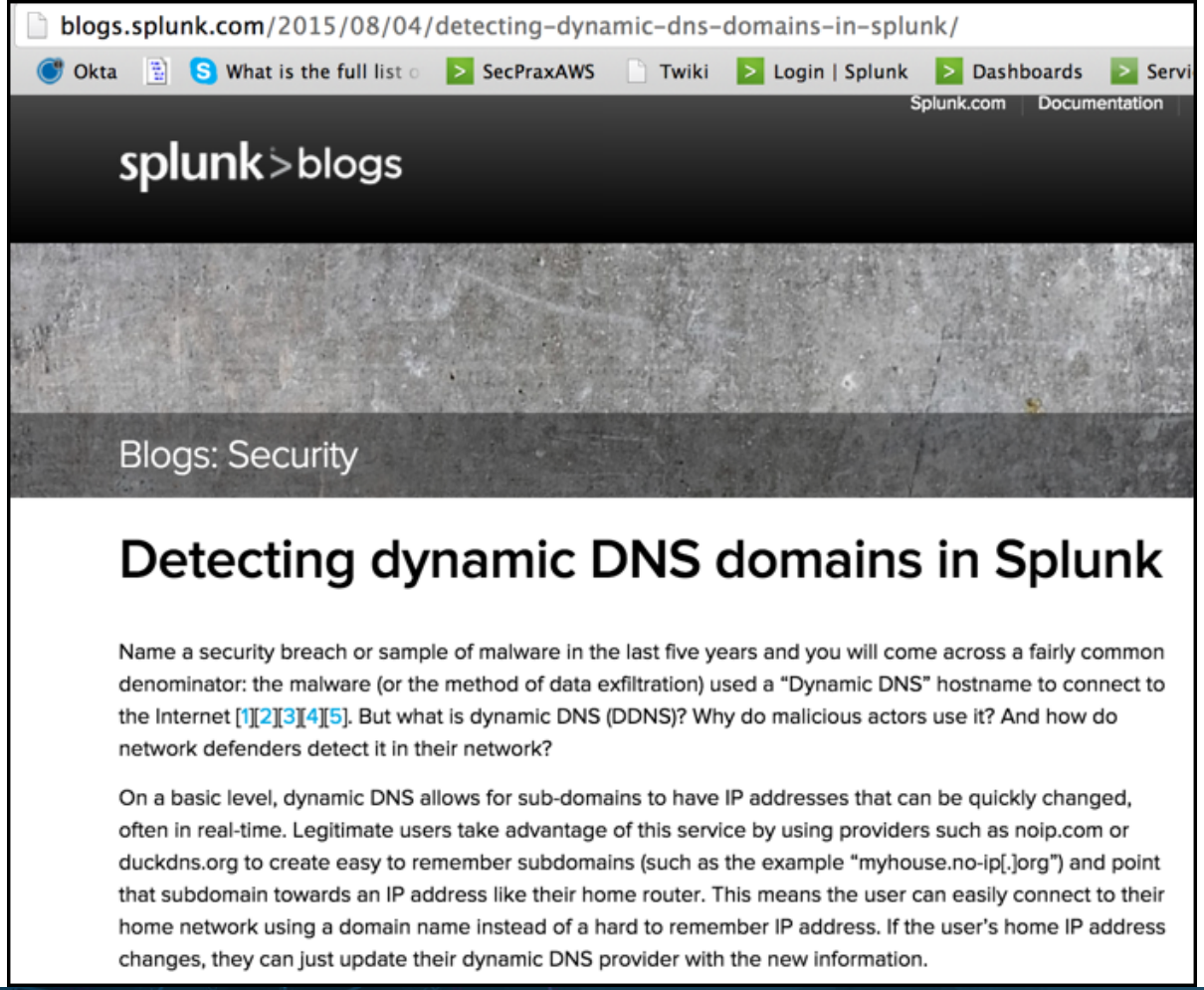
Agenda

- Answering some **W**'s
  - **W**hy are we doing this talk
  - **W**hat are the known unknowns of DNS
- Talk about the **H**
  - **H**ow do we can we find these attacks in our network?
- And now another **W**
  - **W**here can I find this app?
- Conclusion

Why?

splunk>


FTP
ActiveDirectory
Netflow
voip
Blogs
Networking
WinEvent
Github
CMDB
Email
DNS
Logs
Travel
Proxy


blogs.splunk.com/2015/08/04/detecting-dynamic-dns-domains-in-splunk/
Okta
What is the full list o
SecPraxAWS
Twiki
Login | Splunk
Dashboards
Servi
Splunk.com
Documentation
splunk>blogs
Blogs: Security
Detecting dynamic DNS domains in Splunk
Name a security breach or sample of malware in the last five years and you will come across a fairly common denominator: the malware (or the method of data exfiltration) used a "Dynamic DNS" hostname to connect to the Internet [1][2][3][4][5]. But what is dynamic DNS (DDNS)? Why do malicious actors use it? And how do network defenders detect it in their network?
On a basic level, dynamic DNS allows for sub-domains to have IP addresses that can be quickly changed, often in real-time. Legitimate users take advantage of this service by using providers such as noip.com or duckdns.org to create easy to remember subdomains (such as the example "myhouse.no-ip[.]org") and point that subdomain towards an IP address like their home router. This means the user can easily connect to their home network using a domain name instead of a hard to remember IP address. If the user's home IP address changes, they can just update their dynamic DNS provider with the new information.

DNS Is An Unknown Threat To Your Network

DNS Exfiltration

"New FrameworkPOS variant exfiltrates data via DNS requests"
– Gdata Security Blog, October 2014

DNS Tunneling

".. two large-scale security breaches using tunneling, affecting millions of accounts"
– CircleID, Oct 2013

DNS Spoofing

"Back in 1996, a security bug was found in Netscape Navigator and Internet Explorer using DNS spoofing"
*– archive.mozilla.org, **1997***

TCP SYN Flood Attacks

Valid is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake

UDP Flood Attack

Is a denial-of-service (DoS) attack using UDP floods to make the victims server unreachable

DNS Amplification Attack

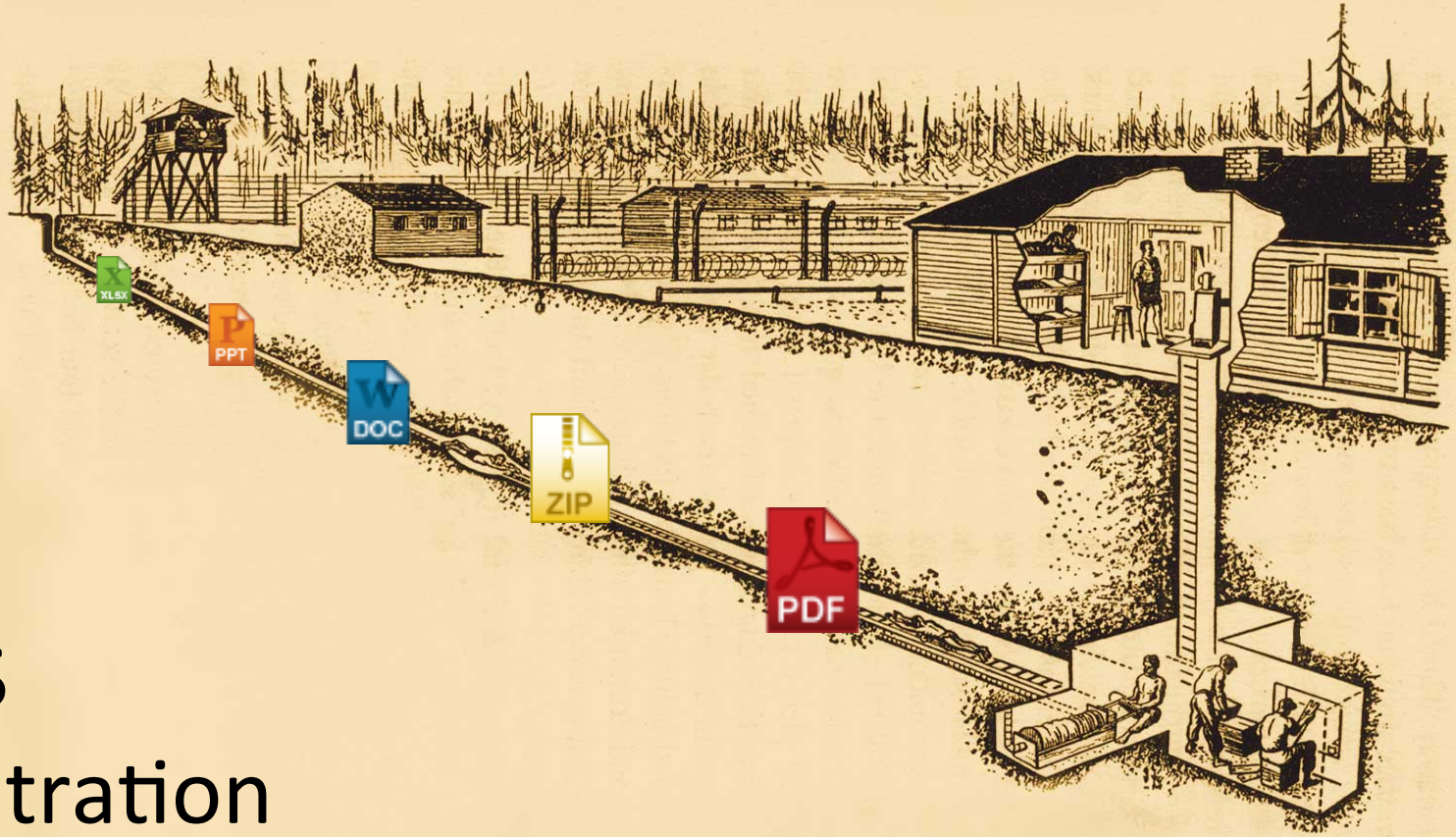
Is a reflection-based distributed denial of service (DDos) attack. The attacker spoofs look-up requests to domain name system (DNS) servers to hide the source of the exploit and direct the response to the target.

What?

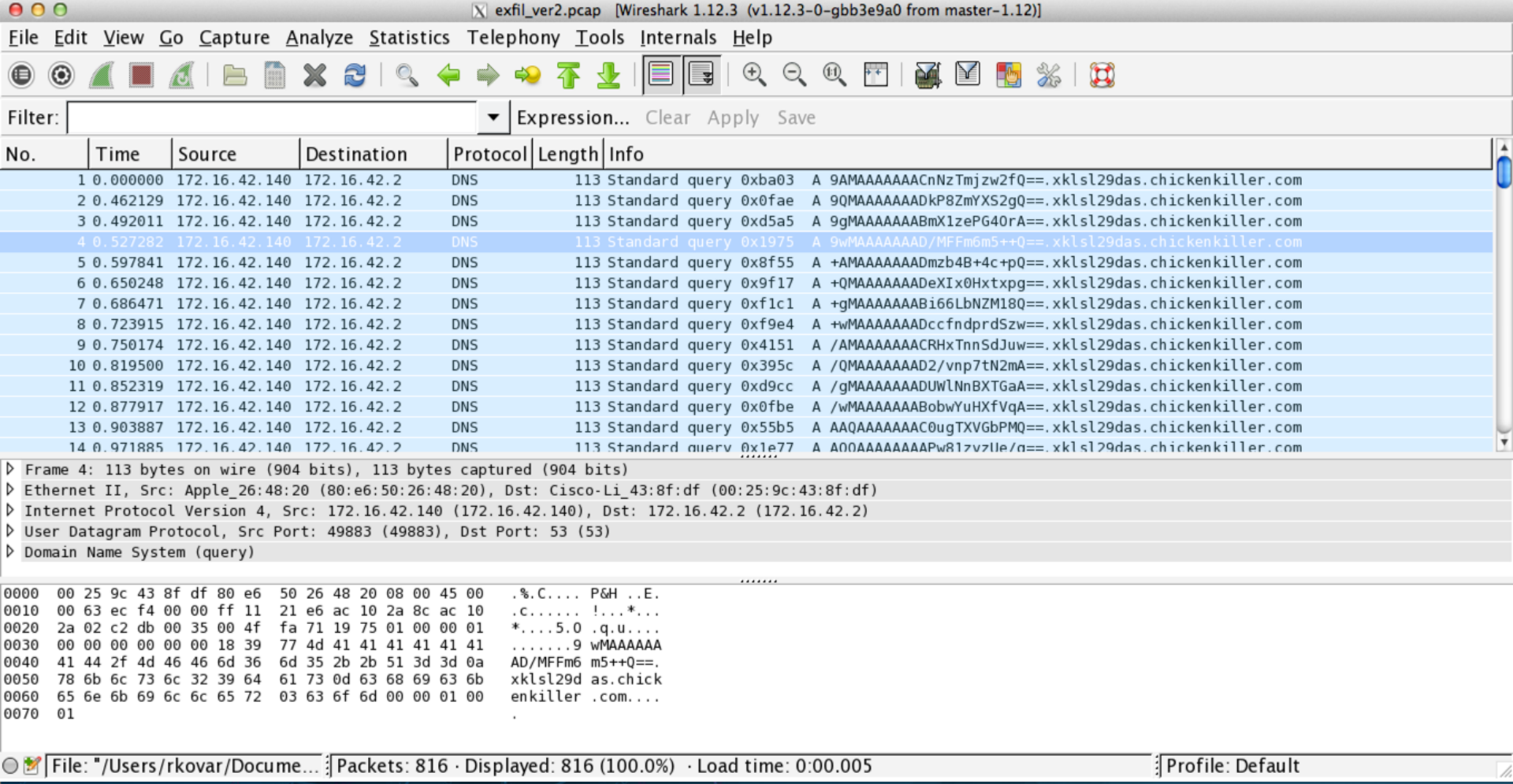
splunk>

DNS Tunneling

~~IMITATION~~ Spoofing, THE SINCEREST FLATTERY.



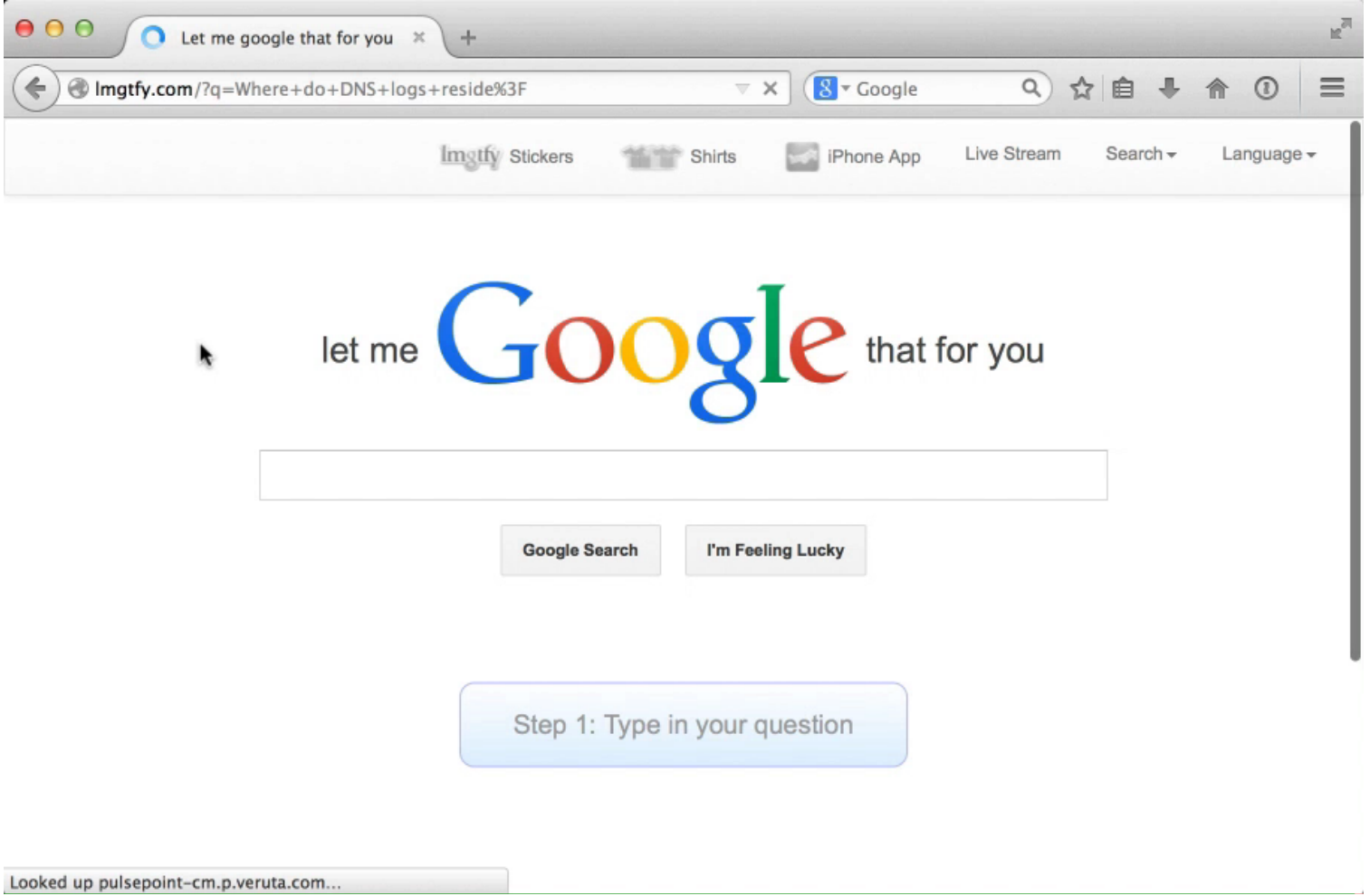
DNS Exfiltration


exfil_ver2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 172.16.42.140 172.16.42.2 DNS 113 Standard query 0xba03 A 9AMAAAAAAACnNzTmjzw2fQ==.xklsl29das.chickenkiller.com
2 0.462129 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x0fae A 9QMAAAAAAADkP8ZmYXS2gQ==.xklsl29das.chickenkiller.com
3 0.492011 172.16.42.140 172.16.42.2 DNS 113 Standard query 0xd5a5 A 9gMAAAAAAABmX1zePG4OrA==.xklsl29das.chickenkiller.com
4 0.527282 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x1975 A 9wMAAAAAAAD/MFFm6m5++Q==.xklsl29das.chickenkiller.com
5 0.597841 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x8f55 A +AMAAAAAAADmzb4B+4c+pQ==.xklsl29das.chickenkiller.com
6 0.650248 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x9f17 A +QMAAAAAAADeXIx0Hxtxpg==.xklsl29das.chickenkiller.com
7 0.686471 172.16.42.140 172.16.42.2 DNS 113 Standard query 0xf1c1 A +gMAAAAAAABi66LbNZM18Q==.xklsl29das.chickenkiller.com
8 0.723915 172.16.42.140 172.16.42.2 DNS 113 Standard query 0xf9e4 A +wMAAAAAAADccfndprdSzw==.xklsl29das.chickenkiller.com
9 0.750174 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x4151 A /AMAAAAAAACRHxTnnSdJuw==.xklsl29das.chickenkiller.com
10 0.819500 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x395c A /QMAAAAAAAD2/vnp7tN2mA==.xklsl29das.chickenkiller.com
11 0.852319 172.16.42.140 172.16.42.2 DNS 113 Standard query 0xd9cc A /gMAAAAAAADUWlNnBXTGaA==.xklsl29das.chickenkiller.com
12 0.877917 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x0fbe A /wMAAAAAAABobwYuHXfVqA==.xklsl29das.chickenkiller.com
13 0.903887 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x55b5 A AAQAAAAAAAC0ugTXVGbPMQ==.xklsl29das.chickenkiller.com
14 0.971885 172.16.42.140 172.16.42.2 DNS 113 Standard query 0x1e77 A AQQAAAAAAAAPw81zvzUe/g==.xklsl29das.chickenkiller.com
Frame 4: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
Ethernet II, Src: Apple_26:48:20 (80:e6:50:26:48:20), Dst: Cisco-Li_43:8f:df (00:25:9c:43:8f:df)
Internet Protocol Version 4, Src: 172.16.42.140 (172.16.42.140), Dst: 172.16.42.2 (172.16.42.2)
User Datagram Protocol, Src Port: 49883 (49883), Dst Port: 53 (53)
Domain Name System (query)
0000 00 25 9c 43 8f df 80 e6 50 26 48 20 08 00 45 00 .%.C.... P&H ..E.
0010 00 63 ec f4 00 00 ff 11 21 e6 ac 10 2a 8c ac 10 .c...... !...*...
0020 2a 02 c2 db 00 35 00 4f fa 71 19 75 01 00 00 01 *....5.O .q.u....
0030 00 00 00 00 00 00 18 39 77 4d 41 41 41 41 41 41 ....9 wMAAAAAA
0040 41 44 2f 4d 46 46 6d 36 6d 35 2b 2b 51 3d 3d 0a AD/MFFm6 m5++Q==.
0050 78 6b 6c 73 6c 32 39 64 61 73 0d 63 68 69 63 6b xklsl29d as.chick
0060 65 6e 6b 69 6c 6c 65 72 03 63 6f 6d 00 00 01 00 enkiller .com....
0070 01 .
File: "/Users/rkovar/Docume... Packets: 816 · Displayed: 816 (100.0%) · Load time: 0:00.005 Profile: Default

.conf2015

Where?

splunk>


Let me google that for you
lmgtfy.com/?q=Where+do+DNS+logs+reside%3F
Google
lmgtfy Stickers
Shirts
iPhone App
Live Stream
Search
Language
let me Google that for you
Google Search
I'm Feeling Lucky
Step 1: Type in your question
Looked up pulsepoint-cm.p.veruta.com...

Bro DNS Logs

bro.dns.log

```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dns
#open   2013-09-05-23-41-46
#fields ts  uid id.orig_h   id.orig_p   id.resp_h   id.resp_p   proto   trans_id    query   qclass  qclass_name qtype   qtype_name  rcode   rcode_name  AA  TC  RD  RA  Z   answers TTLs
#types  time    string  addr    port    addr    port    enum    count   string  count   string  count   string  count   string  bool    bool    bool    bool    count   vector[string]  vector[interval]
1331904608.080000   XjBvx4mGhOf 192.168.204.59  137 192.168.204.255 137 udp 36744   PRINTER 1   C_INTERNET  32  NB  -   -   F   F   T   F   1   -   -
1331904609.190000   FyJEybjuJ89 192.168.202.83  48516   192.168.207.4   53  udp 31220   44.206.168.192.in-addr.arpa 1   C_INTERNET  12  PTR -   -   F   F   T   F   0   -   -
1331904611.280000   u1tasGLgM8b 192.168.202.83  40917   192.168.207.4   53  udp 40840   44.206.168.192.in-addr.arpa 1   C_INTERNET  12  PTR -   -   F   F   T   F   0   -   -
1331904612.260000   qrm56HBFtO2 192.168.202.103 54528   192.168.207.4   53  udp 31822   www.freepbx.org 1   C_INTERNET  1   A   -   -   F   F   T   F   0   -   -
1331904612.260000   VXqdKYJKmSk 192.168.202.103 41343   192.168.207.4   53  udp 3307    freepbx.org 1   C_INTERNET  1   A   -   -   F   F   T   F   0   -   -
1331905096.890000   bwCm4I14XIb 192.168.202.84  61704   192.168.202.255 137 udp 30252   VIRII   1   C_INTERNET  32  NB  -   -   F   F   T   F   1   -   -
1331905096.900000   0KYKyANxYQ7 192.168.202.84  59446   192.168.202.255 137 udp 15530   LENOVO-E33AADF9 1   C_INTERNET  32  NB  -   -   F   F   T   F   1
```

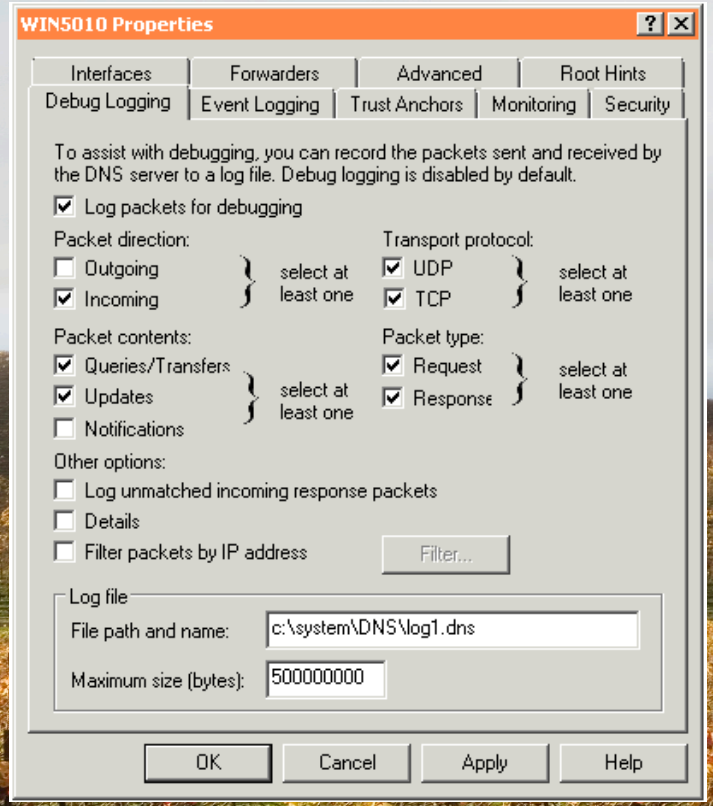
Pro's of Bro:

- High Adoption by Security Community
- Incredibly Flexible

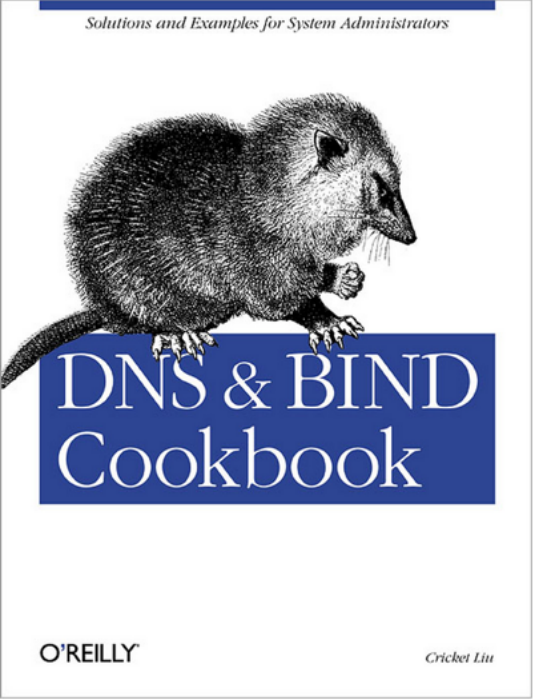
Con's of Bro:

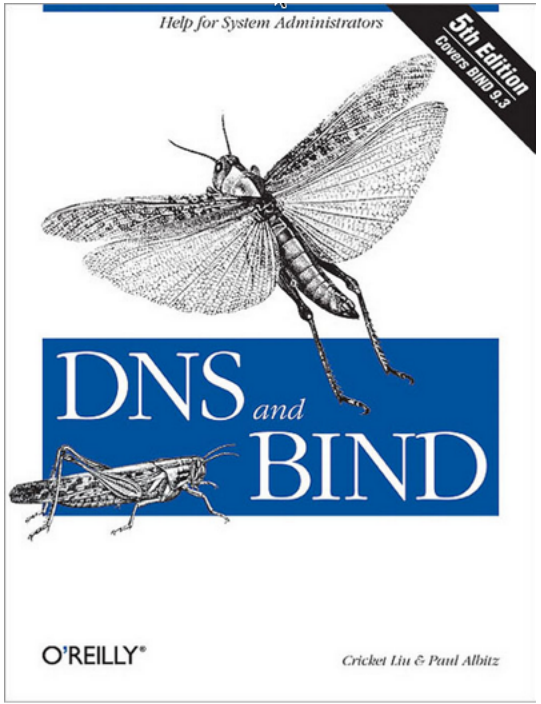
- Can be difficult to install/ administer/configure
- Sets all DNS logs to lower Camel Case

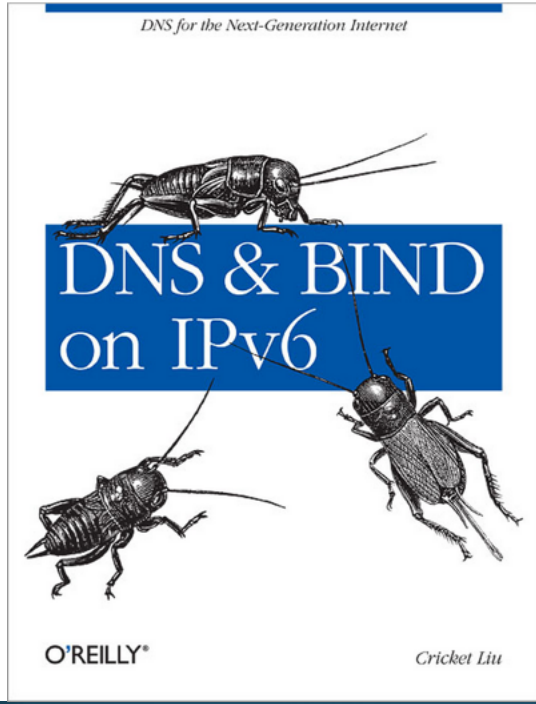
Windows DNS Logs



http://secattic.blogspot.com/203_08_01_archive.html


Solutions and Examples for System Administrators
DNS & BIND Cookbook
O'REILLY
Cricket Liu

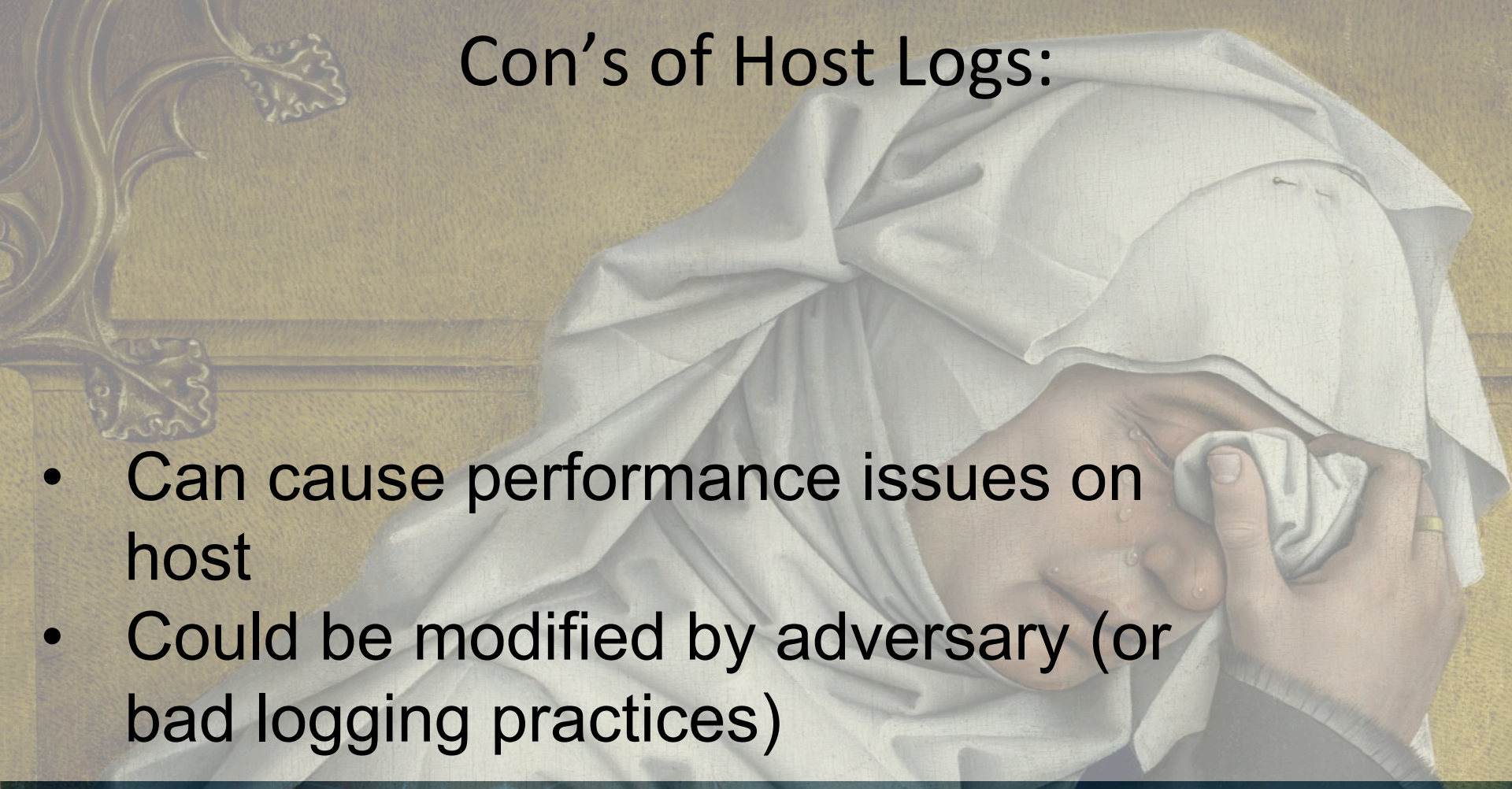

Help for System Administrators
5th Edition
Covers BIND 9.3
DNS and BIND
O'REILLY
Cricket Liu & Paul Albitz


DNS for the Next-Generation Internet
DNS & BIND on IPv6
O'REILLY
Cricket Liu

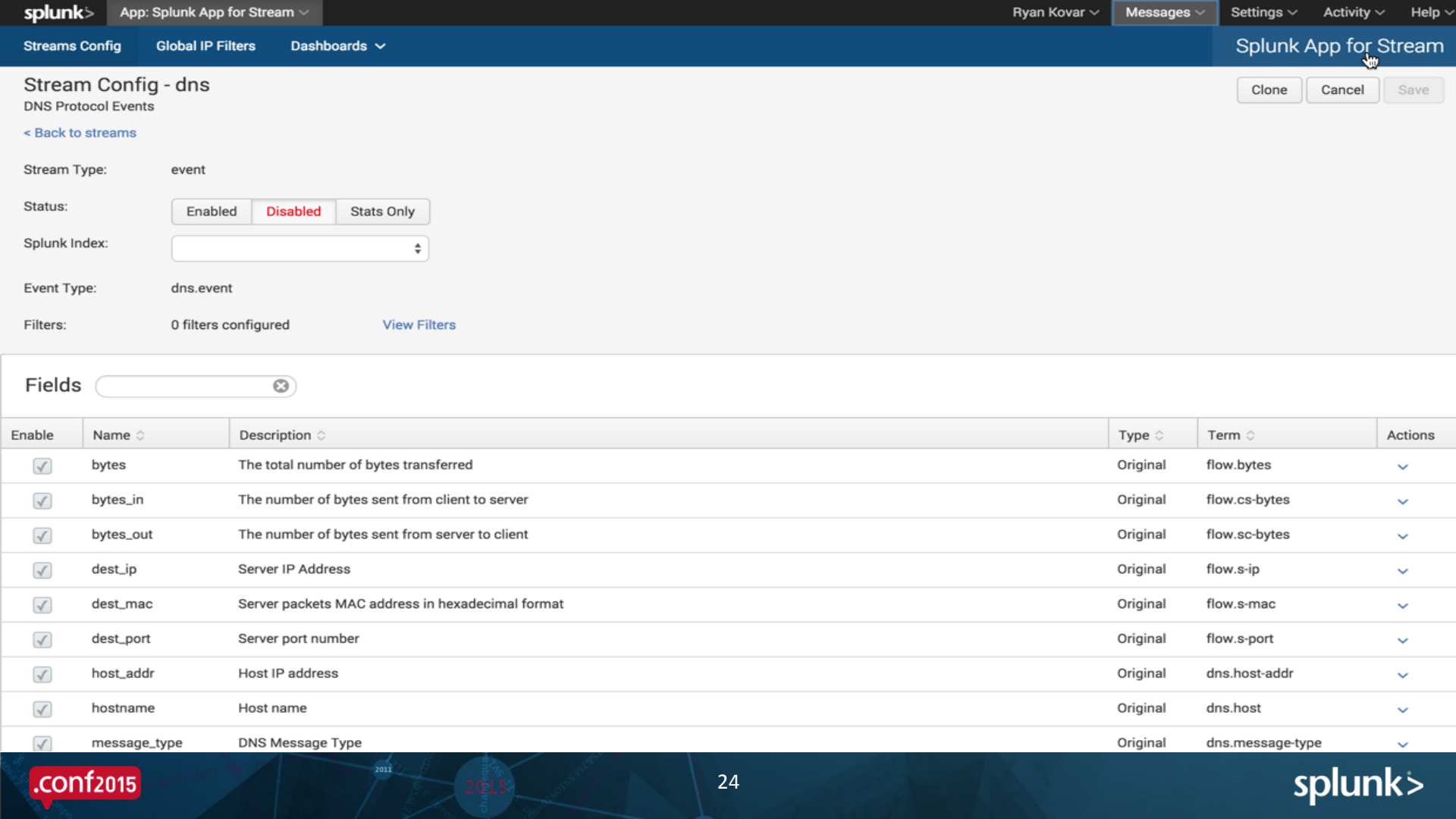
Pro's of Host Logs:

- Easy to gather
- Log DNS server issues along with resolutions

Con's of Host Logs:

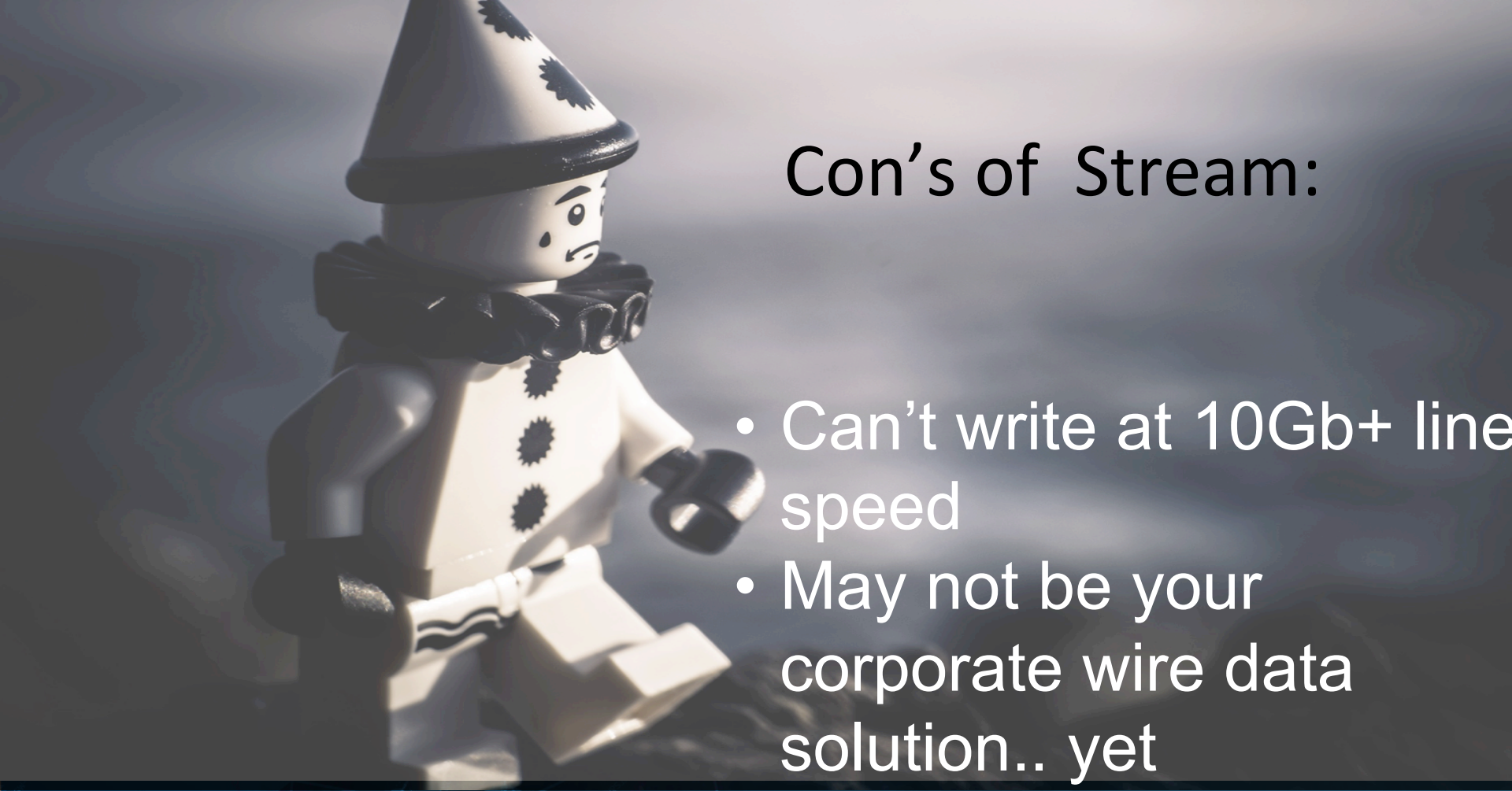


- Can cause performance issues on host
- Could be modified by adversary (or bad logging practices)


splunk>
App: Splunk App for Stream
Ryan Kovar
Messages
Settings
Activity
Help
Streams Config
Global IP Filters
Dashboards
Splunk App for Stream
Stream Config - dns
DNS Protocol Events
Clone
Cancel
Save
< Back to streams
Stream Type: event
Status: Enabled Disabled Stats Only
Splunk Index:
Event Type: dns.event
Filters: 0 filters configured View Filters
Fields
Enable Name Description Type Term Actions
bytes The total number of bytes transferred Original flow.bytes
bytes_in The number of bytes sent from client to server Original flow.cs-bytes
bytes_out The number of bytes sent from server to client Original flow.sc-bytes
dest_ip Server IP Address Original flow.s-ip
dest_mac Server packets MAC address in hexadecimal format Original flow.s-mac
dest_port Server port number Original flow.s-port
host_addr Host IP address Original dns.host-addr
hostname Host name Original dns.host
message_type DNS Message Type Original dns.message-type

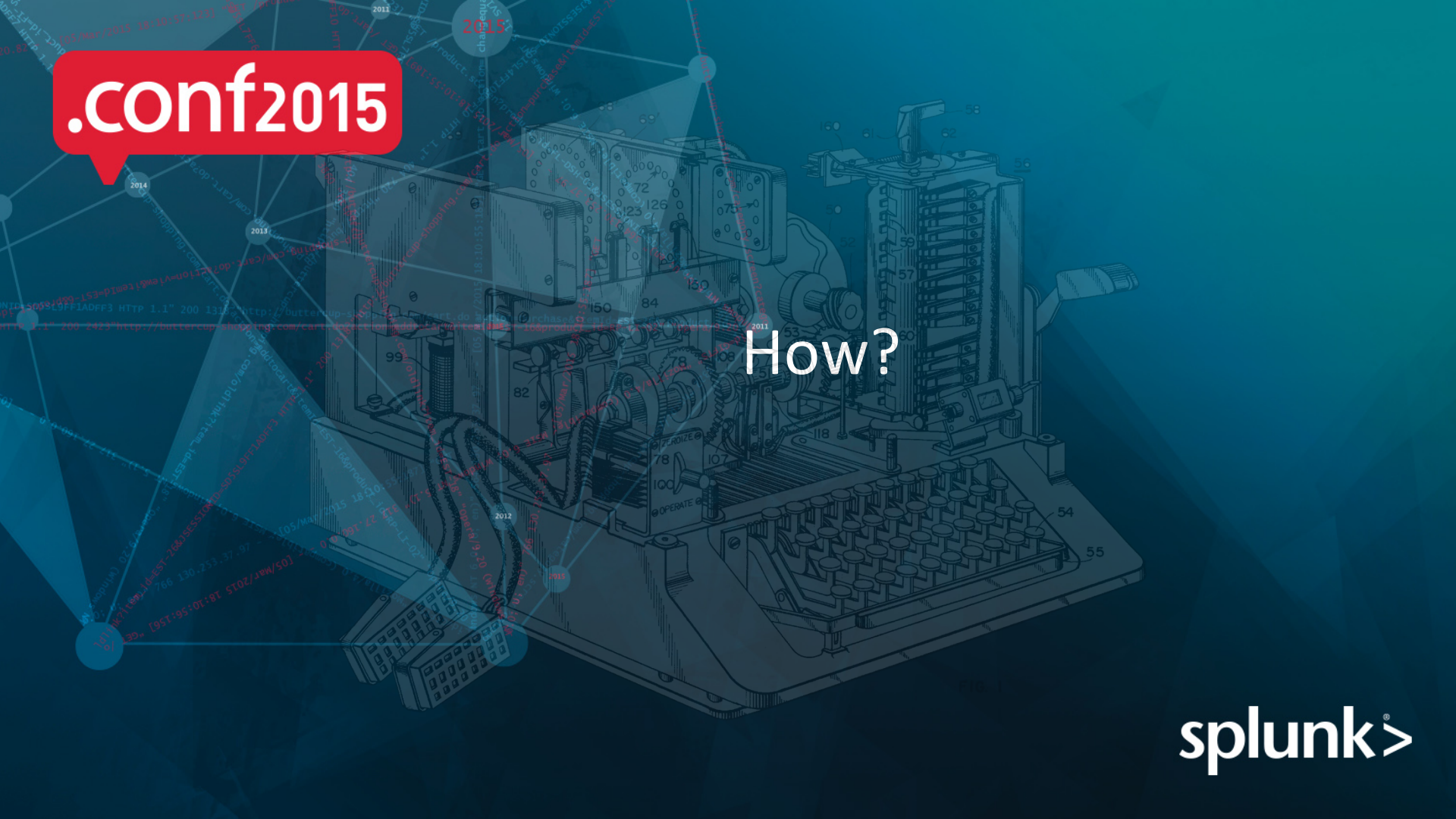
Pro's of Stream :

- Splunk Supported
- Easy to install
- Ground truth



Con's of Stream:

- Can't write at 10Gb+ line speed
- May not be your corporate wire data solution.. yet


.conf2015
How?
splunk>

Conclusion

splunk>

Take-Aways

- DNS Is everywhere in your network
- You have tools to record and analyze it
- The methods to detect threats via DNS exist and are easy to implement

Questions?

THANK YOU

splunk>