

.conf2015

# Hunting the Known Unknowns (with DNS)

Ryan Kovar and Steve Brant  
Security Strategists @ Splunk

splunk>

# Tools

- **URL Toolbox**

- <https://splunkbase.splunk.com/app/2734/>

- **Base64**

- <https://splunkbase.splunk.com/app/1922/>

- **Common Information Model (CIM)**

- <https://splunkbase.splunk.com/app/1621/>

Special thanks to Splunkers Cedric Le Roux and Sebastien Tricaud for making multiple tools that we love and adding "feature requests" whenever we come up with a new idea.

- DNS Tunneling
- DNS Spoofing

```
index=bro sourcetype=bro_dns dest_port=53 dest_ip!=10.0.0.0/8 | stats count by dest_ip
```

```
tag=dns dest_port=53 dest_ip!=10.0.0.0/8 | stats count by dest_ip
```

# Finding unauthorized DNS servers

splunk> App: Search & Reporting ▾ rkovar ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Pivot Reports Alerts Dashboards Search & Reporting

## New Search

Save As ▾ Close

index=stream sourcetype=stream:dns dest\_port=53 dest\_ip!=10.0.0.0/8 | stats count by dest\_ip

165,006 events (before 9/17/15 8:21:39.000 PM)

Job ▾ || ▢ ↶ ↷ ↵ ↴ 🖨 Smart Mode ▾

Events Patterns Statistics (1,556) Visualization

20 Per Page ▾ Format ▾ Preview ▾

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

dest_ip	count
192.168.0.1	94365
192.168.0.2	23023
8.8.8.8	12062
208.67.222.222	4832
8.8.4.4	2887
192.52.166.83	1723

01:45:52 -- [02/Feb/2011:16:00:23] GET /product.screen?product\_id=FW-4020-3E530000-94625F10...  
...category\_id=FLOWERS\* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/533.4; 197.143.248.146) ...  
...category\_id=TEDDY&JSESSIONID=SD9SL4FF4ADFF8 HTTP 1.1\* 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/533.4; 197.143.248.146) ...  
...category\_id=TEDDY\* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5060; Safari/533.4; 197.143.248.146) ...

- DNS Spoofing

```
31.45.62 - - [02/Feb/2011:16:00:23] GET /product.screen?product_id=FW-028.B3SSNID-SWES91 http://www.myflowershop.com/product.screen?product_id=FW-028.B3SSNID-SWES91 Mozilla/5.0 (Windows; U; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4332.573; http://www.myflowershop.com/category.screen?category_id=TEDDY8.JSESSIONID=SD9SL4FF4ADFF8 HTTP/1.1 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4332.573; http://www.myflowershop.com/category.screen?category_id=TEDDY8.JSESSIONID=SD9SL4FF4ADFF8 GET /category.screen?category_id=TEDDY8.JSESSIONID=SD9SL4FF4ADFF8 HTTP/1.1 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4332.573; http://www.myflowershop.com/category.screen?category_id=TEDDY8.JSESSIONID=SD9SL4FF4ADFF8 GET /category.screen?category_id=TEDDY8.JSESSIONID=SD9SL4FF4ADFF8 HTTP/1.1 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4332.573; http://www.myflowershop.com/category.screen?category_id=TEDDY8.JSESSIONID=SD9SL4FF4ADFF8
```

# Finding DNS Spoofing Activity

**splunk** App: Search & Reporting Administrator Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards Search & Reporting

## New Search

Save As Close

index=bro sourcetype=bro\_weird name=dns\_unmatched\_reply dest\_port=53 | stats count by src\_ip dest\_ip

All time

63 events (before 9/17/15 9:03:47.000 PM)

Job

Events Patterns Statistics (2) Visualization

20 Per Page Format Preview

src_ip	dest_ip	count
10.80.16.150	10.80.16.151	3
10.80.16.151	10.160.20.2	60

1.45.62 -- [02/Feb/2011:16:00:23] GET /product.screen?product\_id=FI-FW-4020.JSESSID=54625F10a1e5d100 http://www.nyflowershop.com/...  
...?category\_id=FLOWERS\* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5802 http://www.nyflowershop.com/category.screen?category\_id=FLOWERS\*  
...?category\_id=TEDDY&JSESSIONID=SD9SL4FF4ADFF8 HTTP 1.1 200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4322.5802 http://www.nyflowershop.com/category.screen?category\_id=TEDDY&JSESSIONID=SD9SL4FF4ADFF8  
...?category\_id=TEDDY\* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5802 http://www.nyflowershop.com/category.screen?category\_id=TEDDY\*  
...?category\_id=TEDDY\* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5802 http://www.nyflowershop.com/category.screen?category\_id=TEDDY\*

# Finding clients connecting to multiple DNS servers

- DNS Spoofing
- DNS Exfil
- DNS Tunneling

```
tag=dns dest_port=53 dest_ip!=10.0.0.0/8 | bucket _time span=1s | stats VALUES(dest_ip) AS IP_List  
dc(dest_ip) AS distinct by _time src_ip | search distinct > 2 | table src_ip IP_List distinct
```

# Finding clients connecting to multiple DNS servers

splunk> App: Search & Reporting ▾ rkovar ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Pivot Reports Alerts Dashboards Search & Reporting

Q New Search Save As ▾ Close

```
tag=dns dest_port=53 dest_ip!=10.0.0.0/8 | bucket _time span=1s | stats VALUES(dest_ip) AS IP_List dc(dest_ip) AS distinct by _time src_ip| search distinct > 2|
table src_ip IP_List distinct
```

1,808,280 events (before 9/17/15 10:34:25.000 PM) Job ▾ || ▢ ↶ ↷ ↵ ↴ ↶ ↷ ↵ ↴ Smart Mode ▾

Events Patterns Statistics (1,477) Visualization

20 Per Page ▾ Format ▾ Preview ▾ < Prev 1 2 3 4 5 6 7 8 9 ... Next >

src_ip ▾	IP_List ▾	distinct ^
10.125.15.233	4.2.2.3 4.2.2.4 8.8.4.4	3
10.142.15.178	192.168.0.1 68.28.208.215 8.8.8.8	3
10.130.15.153	192.168.0.1 198.6.1.83 8.8.4.4	3
10.125.15.233	4.2.2.4 4.2.2.6 8.8.8.8	3
10.128.15.176	192.168.0.1 192.168.24.2 68.238.96.12	3



# Finding Clients with extremely Looooooooooooooooong queries

- DNS Tunneling
- DNS Exfil

**Find anything that is 2 standard deviations**

```
sourcetype=bro_dns | eval len=len(query) | eventstats stdev(len) AS stdev avg(len) AS avg p50(len) AS p50 |  
eval length=len(query) | where length>(stdev*2) | stats count by length stdev avg p50 qtype_name query |  
sort -length
```

**Finding queries over 200 characters long**

```
sourcetype=bro_dns | `ut_parse(query)` | eval length=len(query) | search length>200 | stats count by query
```

# Finding Queries Two Standard Deviations Over Normal

[illegible]

# Finding Queries Over 200 characters

The screenshot shows the Splunk web interface with the search bar containing the query: `sourcetype=bro_dns | `ut_parse(query)` | eval length=len(query) | search length>200 | stats count by query`. The search results show 38,874 of 234,029 events matched. The interface includes navigation tabs for Search, Pivot, Reports, Alerts, and Dashboards. The search bar has a 'New Search' button and a 'Save As' button. The results are displayed in a table with columns for Events (38,874), Patterns, Statistics (38,874), and Visualization. The table shows a list of queries, with the first query being `0a0a85r\xe6t\xdc\xcd\xbd\xda\x5e8xw\dx1\x8c8x7\x4c1h\x2c2dfyrp\x56gm\xdc3xf0\x8e8x\da\xda\xcdde\x43zxf1\xcdid\xfd\xcd0p\x6b\xbf\xda\x7e1.bm1\x0d4c2ptfrbbma5\xdcw\xcfuy\x18z3\x3d3\x2\x6e2ig\x8\x8e8x4uqc\x`. The interface also includes a 'Verbose Mode' button and a 'Next' button.

- DNS Tunneling
- DNS Exfil

```
sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT  
  FP_entropy=* | `ut_shannon(ut_domain)` | search ut_shannon > 4.0 | stats count by query ut_shannon
```

```
sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT FP_entropy=* | `ut_shannon(ut_subdomain)` | search ut_shannon > 4.5 | stats count by query ut_shannon
```

# BUT FIRST...What is Entropy?

- It is the measure of randomness in a variable
  - The higher the randomness the higher the measure
- Most often “Shannon” entropy is calculated, but there are different calculations of entropy
- Example:
  - google.com
    - Shannon Entropy score of 2.6 (low)
  - A00wlkj—(-a.aslkn-C.a.2.sk.esasdfasf1111)-890209uC.4.com
    - Shannon Entropy score of 4.28 (high)

# Finding domains and subdomains with high Entropy

- DNS Tunneling
- DNS Exfil

## Domains

```
sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT  
FP_entropy=* | `ut_shannon(ut_domain)` | search ut_shannon > 4.0 | stats count by query ut_shannon
```

## Subdomains

```
sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT  
FP_entropy=* | `ut_shannon(ut_subdomain)` | search ut_shannon > 4.5 | stats count by query ut_shannon
```

# Finding Subdomains With High Entropy

**splunk>** App: Search & Reporting rkovar Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards Search & Reporting

**New Search** Save As Close

`sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT FP_entropy=* | `ut_shannon(ut_subdomain)` | search ut_shannon > 4.5 | stats count by query ut_shannon` All time Q

✓ 148 events (before 9/19/15 7:09:33.000 PM) Job || ↗ ↓ 🖨 Smart Mode

Events Patterns Statistics (29) Visualization

20 Per Page Format Preview < Prev 1 2 Next >

query	ut_shannon	count
p5-4m7fvu3jnwrx4-jnlncmi4qk7yyhlm-124650-i1-bogus-dnssec-bd.gexperiments3.com	4.744316617857939	1
p4-hwwxtbqzkw3pc-rwdkrdhl5zf6oq-121099-i1-bogus-dnssec-vd.gexperiments2.com	4.676520007688447	2
37a693ed8b84802248b26102fcd9674.azr.msnetworkanalytics.testanalytics.net	4.663000167991441	2
p4-hwwxtbqzkw3pc-rwdkrdhl5zf6oq-121099-i2-bogus-dnssec-bd.gexperiments3.com	4.642621702603701	1
267b6bf1561e43cba80004f878698a51.azr.msnetworkanalytics.testanalytics.net	4.620008750235073	1
86bfca60de3038109a2bd6cfbed5e7d5.azr.msnetworkanalytics.testanalytics.net	4.60628352292301	2
_ldap_tcp.4115b6eb-20d7-4740-88ec-3d5e410f71f3.domains_msdc.ancor2.r.recruit.co.jp	4.605398661874478	1
_ldap_tcp.4115b6eb-20d7-4740-88ec-3d5e410f71f3.domains_msdc.ancor2.r.recruit.co.jp	4.605398661874477	10
_ldap_tcp.4115b6eb-20d7-4740-88ec-3d5e410f71f3.domains_msdc.ancor2.r.recruit.co.jp	4.605398661874476	3
bcbfb7c439e264ba51781061659bf1ca.azr.msnetworkanalytics.testanalytics.net	4.581829378051256	1
4c97cbddd84f3697818b0ce4160a79a1.azr.msnetworkanalytics.testanalytics.net	4.578833068298884	1
p5-vigutpxf7xxbg-msjskcp3wgtyef2-123437-i1-bogus-dnssec-vd.gexperiments2.com	4.568646652152849	2
_ldap_tcp.7a56493b-4275-4132-8d95-0d4115fe06c3.domains_msdc.securepassage.com	4.564858157364012	1
5ab85055db7b06f3aacc2d91694bccc3.azr.msnetworkanalytics.testanalytics.net	4.562822440640042	2
y4ocuaacaakcamyaaeaaagsaqaabj25je6nxygcxisp3zabahaiajqaaaaa7g.csrxaeeaaofattqj5ov3niuyx6x5vpr5erh2j3rrbrxp75wzimmfj3ogb4nlo.ozcuujdv2xeyv5bsab.a.j.e5.sk	4.552926663614822	1
4sesuaacaakcamyaaeaaagsaqaabj25je6nxygcxisp3zabahaiajqaaaaajz.x6qdqeaaoafqb7jncsywywx7u2uvq7k2iw7o54gezayb72bugocelfw7tuvwk.w5llhcamoheampvtb.a.j.e5.sk	4.549354715087354	1

# Finding clients connecting to unauthorized DNS servers

- DNS Exfil
- DNS Tunneling

Corporate DNS  
server lookup table

```
tag=dns dest_port=53| lookup corp_nameservers nameserver AS dest_ip | search NOT isGood=TRUE|
    lookup nameservers ip AS dest_ip | search NOT checked_at=* | stats count by dest_ip
```

Open name servers  
lookup table



# Finding clients connecting to unauthorized DNS servers

splunk

App: conf2015\_dns

Administrator

Messages

Settings

Activity

Help

Find

Search

Pivot

Reports

Alerts

Dashboards

conf2015\_dns

New Search

tag=dns dest\_port=53| lookup corp\_nameservers nameserver AS dest\_ip | search NOT isGood=TRUE| lookup nameservers ip AS dest\_ip | search NOT checked\_at=\* | stats count by dest\_ip

All time

✓ 1,006,456 events (before 9/19/15 8:01:58.000 PM)

Job

||

Verbose Mode

Events (1,006,456)

Patterns

Statistics (2)

Visualization

20 Per Page

Format

Preview

dest_ip	count
10.80.16.151	977938
52.4.172.96	28518

```
SL145.62 -- [02/Feb/2011:16:00:23] GET /product.screen?product_id=F-W-C8SSESSION=94C7F67E http://www.myflowershop.com/product.screen?category_id=FLOWERS* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 1.1 C55P-01110204) POST /category.screen?category_id=TEDDY&JSESSIONID=SD9SL4FF4ADFF8 HTTP 1.1*200 3439 Windows NT 5.1; SV1; JET CL 1.1 C55P-01110204 http://www.myflowershop.com/category.screen?category_id=TEDDY* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 1.1 C55P-01110204) http://www.myflowershop.com/category.screen?category_id=TEDDY* Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; JET CL 1.1 C55P-01110204)
```



**BONUS ROUND**

# Finding DOMAINS With High Entropy

- Malware
- DNS Tunneling

## Domains

```
sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT  
FP_entropy=* | `ut_shannon(ut_domain)` | search ut_shannon > 4.0 | stats count by query ut_shannon
```

# Finding Domains With High Entropy

splunk> App: Search & Reporting ▾ rkovar ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Pivot Reports Alerts Dashboards Search & Reporting

🔍 New Search Save As ▾ Close

sourcetype=bro\_dns | `ut\_parse(query)` | lookup FP\_entropy\_domains domain AS ut\_domain | search NOT FP\_entropy=\* | `ut\_shannon(ut\_domain)` | stats count by query ut\_shannon

📌 All time ▾ 🔍

✓ 1,621,137 events (before 9/19/15 7:19:31.000 PM) Job ▾ ⏸ ⏹ ↶ ⏴ ⏵ ⏷ 🧠 Smart Mode ▾

Events Patterns Statistics (130,740) Visualization

20 Per Page ▾ Format ▾ Preview ▾ < Prev 1 2 3 4 5 6 7 8 9 ... Next >

query	ut_shannon ▾	count
3wirqs5imc.vi9y6kmcksy7xw2rf8e4klb3t.com	4.487122805397798	1
jq94wtm6-vlo9i-a8cdvu4.dti9613wn-lsvbnrgsv3vj0ya.com	4.487122805397798	1
4k4hck0sxe1a4-auxgo67jq-.emy2egline26ztbhlpad7831i.com	4.487122805397797	1
qzpt2o7szq9j4v-rregr.2fzni4p95jvmcwyhbmd7oguzn62.com	4.478232197413861	1
twcn95gmh8aepzl.d4m2kss4mazxbvj-en9c57f7qy.com	4.478232197413861	1
rdlb2pgcy-zxgnyqpqe.ivczg0s1w4brp-yd5vnu9g.com	4.469670487371861	1
uew0t1ytlmyirhci1.cspexioh91r0qyalid-oxqsftnjq.com	4.453880987666651	1
movhbu4du3nd0g1umrz575d.1q950idlpnkeus2-zrfii.com	4.453660689688184	1

# Passive DNS dashboards

- Inspired by work done by Brian Warehime and his blog post: <http://nullsecure.org/building-your-own-passivedns-feed/>

### Accelerated data model version of Brian's query (requires CIM app installed)

```
| datamodel Network_Resolution DNS search | rename DNS.* AS * | search query=splunk4eva.mooo.com
answers!="-" | stats earliest(_time) AS first_time latest(_time) AS latest_time by answers, record_type |
eval first_time=strftime(first_time, "%m/%d/%y %H:%M:%S") | eval latest_time=strftime(latest_time, "%m/
%d/%y %H:%M:%S") | rename first_time AS "Earliest Time" latest_time AS "Latest Time" answers AS
"Answer" record_type AS "Record Type"
```

splunk> App: conf2015\_dns Administrator Messages Settings Activity Help Find

Search Pivot Reports Alerts Dashboards conf2015\_dns

Edit More Info

splunk4eva.com

Answer	Record Type	query	src_ip	Earliest Time	Latest Time
111.222.233.233	A	splunk4eva.com	10.80.16.151	09/15/15 21:28:18	09/15/15 21:31:21
111.222.255.255	A	splunk4eva.com	10.80.16.151	09/15/15 21:27:34	09/15/15 21:27:39
200.0.0.0	A	splunk4eva.com	10.80.16.151	09/15/15 21:26:21	09/15/15 21:26:21

# Base64 encoded DNS queries

- **\*NOTE\*** Can only detect Base64 with DNS logs that preserve case. Bro will not work
- Further note, this uses a new tool called gather which has not yet been released but will be released shortly

## Base64 Decoded

```
sourcetype=stream:dns | `ut_parse(query)`|fields ut_subdomain_level_2| base64
field=ut_subdomain_level_2 action=decode mode=append suppress_error=True| search base64=* | eval
base64 = replace(base64, "\\x\\w{2}", " ") | dedup base64 | gather counter=2 fieldname=base64 | sort -
_time | table glue
```

**HUGE thanks to Cedric Le Roux and Sebastien Tricaud for creating great tools like FAUP, URL Toolbox, base64, and gather. Not only did they create tools we love, they implemented "Feature Requests" that we asked for within 20-30 minutes of receipt of email. Thanks guys!**

# Base64 encoded DNS queries

SearchPivotReportsAlertsDashboards

Search & Reporting

New Search

Save AsClose

sourcetype=stream:dns | `ut\_parse(query)`|fields ut\_subdomain\_level\_2| base64 field=ut\_subdomain\_level\_2 action=decode mode=append suppress\_error=True| search base64=\* | eval base64 = replace(base64, "\\x\\w{2}", " ") | dedup base64 | gather counter=2 fieldname=base64 | sort - \_time | table glue

All time

177 events (Partial results for before 9/23/15 3:29:39.000 PM)

Job

Smart Mode

EventsPatternsStatistics (177)Visualization

20 Per PageFormatPreview

Prev123456789Next

glue

[S!^Z7X>XbKVhTRA.IP'n[N~L{I-lh!l!tGOOECA?=:97531/-+)'%#!ypes).xm[CPK%C~|z3xv0CtrpEnIjChfDb`o^\\Z8XzEV)T(RCPNLCJHEGNUBx86-64.s@/lib64/15NE3N.@@@tE%@d@tE(d@@@> 'm{w d';yOy)0)m>}mj~m|X!zxmta)r,p=n=)l=j&hX!Vf)d["b)p^\*8ZWUSLlx9D bjbjv[0] eak\_file # Run Pr p Excepti ose) ak~|t\*Complz x elv continut r t Exceptp n DNS\_ZONI me(b64\_pj cket.geth f ignore id w an excb # This w^ print p\\Z art = paX V e(payloadT base64.R b64\_pP N', part,L struct.pj paH g F 2 + 8 byD k the daB # Bi@> < if dat: ad(8) 8 data6 hile 1: 4 rt = 0 2 'rb) 0 file(fi. ry:, filename\* def bre(efaulti& com) soc\$ splunk4e" 64 DNS\_Z rather t se hex e stname, acters i e non-va lf you d queries em Then nd b64 e e chunks unks Seq small 8 large f sys "" rt struc port bas

[S!^Z7X>XbKVhTRA.IP'n[N~L{I-lh!l!tGOOECA?=:97531/-+)'%#!ypes).xm[CPK%C~|z3xv0CtrpEnIjChfDb`o^\\Z8XzEV)T(RCPNLCJHEGNUBx86-64.s@/lib64/15NE3N.@@@tE%@d@tE(d@@@> 'm{w d';yOy)0)m>}mj~m|X!zxmta)r,p=n=)l=j&hX!Vf)d["b)p^\*8ZWUSLlx9D bjbjv[0] eak\_file # Run Pr p Excepti ose) ak~|t\*Complz x elv continut r t Exceptp n DNS\_ZONI me(b64\_pj cket.geth f ignore id w an excb # This w^ print p\\Z art = paX V e(payloadT base64.R b64\_pP N', part,L struct.pj paH g F 2 + 8 byD k the daB # Bi@> < if dat: ad(8) 8 data6 hile 1: 4 rt = 0 2 'rb) 0 file(fi. ry:, filename\* def bre(efaulti& com) soc\$ splunk4e" 64 DNS\_Z rather t se hex e stname, acters i e non-va lf you d queries em Then nd b64 e e chunks unks Seq small 8 large f sys "" rt struc

[S!^Z7X>XbKVhTRA.IP'n[N~L{I-lh!l!tGOOECA?=:97531/-+)'%#!ypes).xm[CPK%C~|z3xv0CtrpEnIjChfDb`o^\\Z8XzEV)T(RCPNLCJHEGNUBx86-64.s@/lib64/15NE3N.@@@tE%@d@tE(d@@@> 'm{w d';yOy)0)m>}mj~m|X!zxmta)r,p=n=)l=j&hX!Vf)d["b)p^\*8ZWUSLlx9D bjbjv[0] eak\_file # Run Pr p Excepti ose) ak~|t\*Complz x elv continut r t Exceptp n DNS\_ZONI me(b64\_pj cket.geth f ignore id w an excb # This w^ print p\\Z art = paX V e(payloadT base64.R b64\_pP N', part,L struct.pj paH g F 2 + 8 byD k the daB # Bi@> < if dat: ad(8) 8 data6 hile 1: 4 rt = 0 2 'rb) 0 file(fi. ry:, filename\* def bre(efaulti& com) soc\$ splunk4e" 64 DNS\_Z rather t se hex e stname, acters i e non-va lf you d queries em Then nd b64 e e chunks unks Seq small 8 large f sys ""

[S!^Z7X>XbKVhTRA.IP'n[N~L{I-lh!l!tGOOECA?=:97531/-+)'%#!ypes).xm[CPK%C~|z3xv0CtrpEnIjChfDb`o^\\Z8XzEV)T(RCPNLCJHEGNUBx86-64.s@/lib64/15NE3N.@@@tE%@d@tE(d@@@> 'm{w d';yOy)0)m>}mj~m|X!zxmta)r,p=n=)l=j&hX!Vf)d["b)p^\*8ZWUSLlx9D bjbjv[0] eak\_file # Run Pr p Excepti ose) ak~|t\*Complz x elv continut r t Exceptp n DNS\_ZONI me(b64\_pj cket.geth f ignore id w an excb # This w^ print p\\Z art = paX V e(payloadT base64.R b64\_pP N', part,L struct.pj paH g F 2 + 8 byD k the daB # Bi@> < if dat: ad(8) 8 data6 hile 1: 4 rt = 0 2 'rb) 0 file(fi. ry:, filename\* def bre(efaulti& com) soc\$ splunk4e" 64 DNS\_Z rather t se hex e stname, acters i e non-va lf you d queries em Then nd b64 e e chunks unks Seq small 8 large f

[S!^Z7X>XbKVhTRA.IP'n[N~L{I-lh!l!tGOOECA?=:97531/-+)'%#!ypes).xm[CPK%C~|z3xv0CtrpEnIjChfDb`o^\\Z8XzEV)T(RCPNLCJHEGNUBx86-64.s@/lib64/15NE3N.@@@tE%@d@tE(d@@@> 'm{w d';yOy)0)m>}mj~m|X!zxmta)r,p=n=)l=j&hX!Vf)d["b)p^\*8ZWUSLlx9D bjbjv[0] eak\_file # Run Pr p Excepti ose) ak~|t\*Complz x elv continut r t Exceptp n DNS\_ZONI me(b64\_pj cket.geth f ignore id w an excb # This w^ print p\\Z art = paX V e(payloadT base64.R b64\_pP N', part,L struct.pj paH g F 2 + 8 byD k the daB # Bi@> < if dat: ad(8) 8 data6 hile 1: 4 rt = 0 2 'rb) 0 file(fi. ry:, filename\* def bre(efaulti& com) soc\$ splunk4e" 64 DNS\_Z rather t se hex e stname, acters i e non-va lf you d queries em Then nd b64 e e chunks unks Seq small 8