Network forensics is not dead

Why we are not always too late

Chloé HUET-LE RUMEUR

« Non, ça ne sert pas à rien…
Mais bon,
ça n’est pas très utile non plus… »

Captures réseau

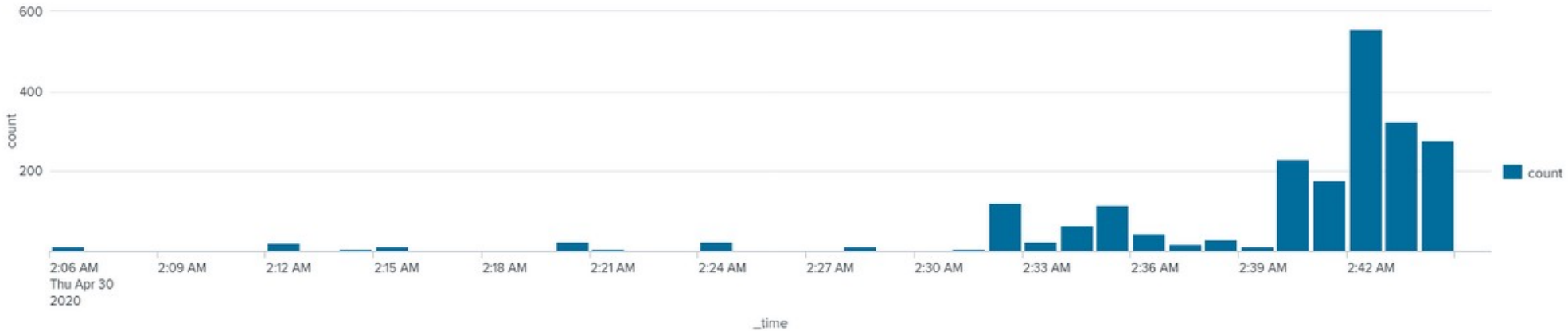
NIDS

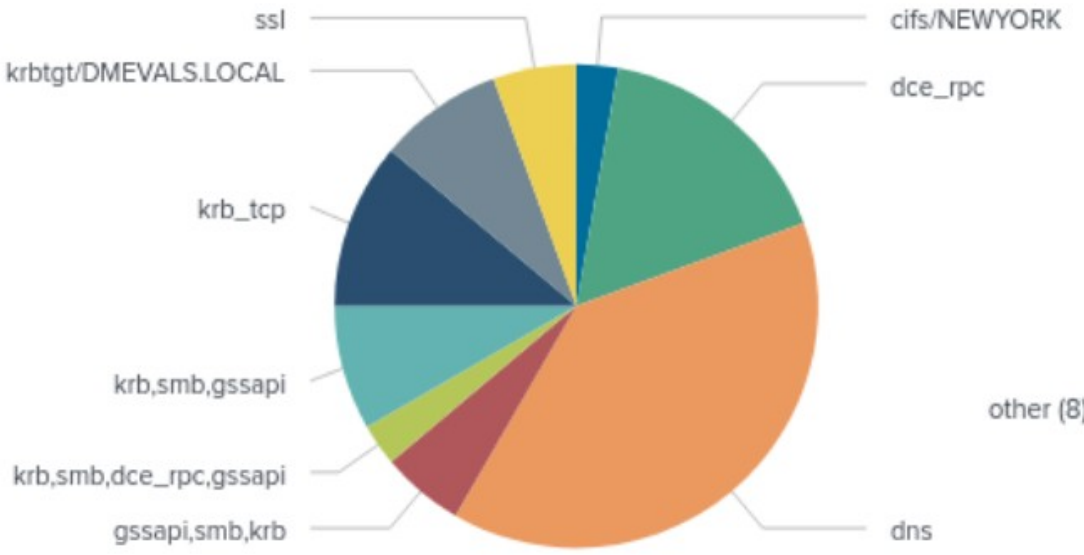
Journaux issus du réseau

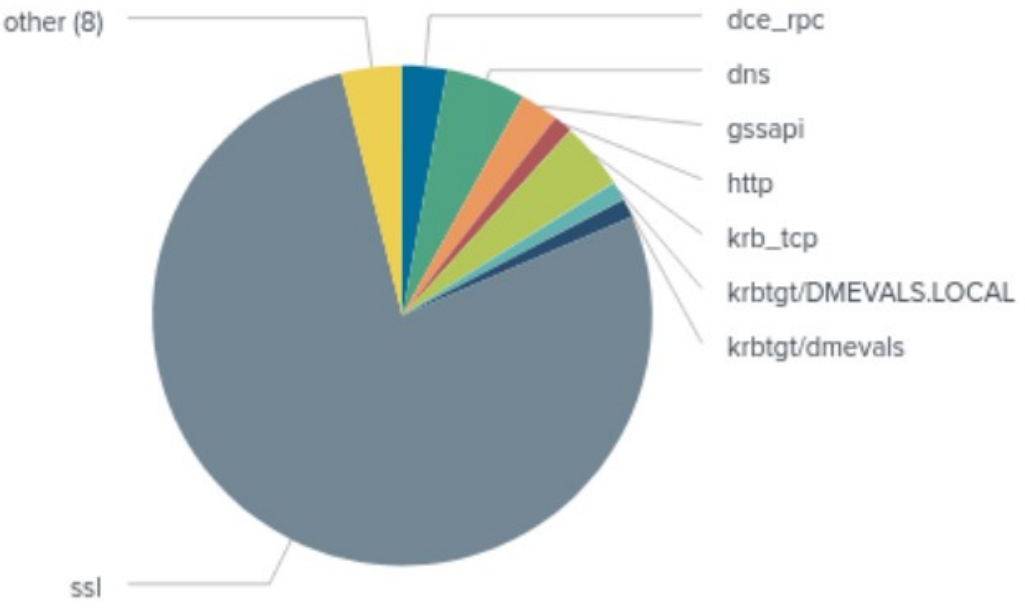
Journaux issus des machines associés au réseau

Détecter,
au quotidien

Actions flagrantes

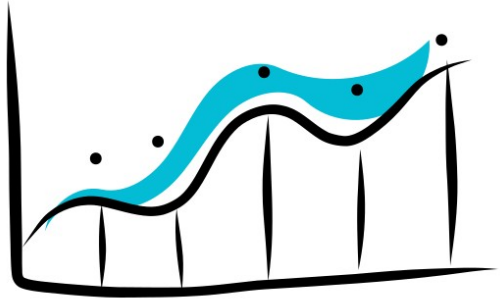

600
400
200
count
2:06 AM
Thu Apr 30
2020
2:09 AM
2:12 AM
2:15 AM
2:18 AM
2:21 AM
2:24 AM
2:27 AM
2:30 AM
2:33 AM
2:36 AM
2:39 AM
2:42 AM
_time
count


ssl
krbtgt/DMEVALS.LOCAL
krb_tcp
krb,smb,gssapi
krb,smb,dce_rpc,gssapi
gssapi,smb,krb
cifs/NEWYORK
dce_rpc
dns


other (8)
ssl
dce_rpc
dns
gssapi
http
krb_tcp
krbtgt/DMEVALS.LOCAL
krbtgt/dmevals

Respect

des politiques



Actions plus discrètes

```
source="combined_zeek.log" host="zeek" index="zeek_mordor" sourcetype="custom:zeek" service="dns"
| bucket _time span=5m
| eventstats count as nbPerMin by _time,id_orig_h
| eventstats mean(nbPerMin) as moyenne, stdev(nbPerMin) as ecart by id_orig_h
| where nbPerMin>(moyenne+2*ecart) OR nbPerMin<(moyenne+2*ecart)
| stats count by _time id_orig_h moyenne ecart
```

Date time range

✓ **39 events** (4/30/20 2:00:00.000 AM to 4/30/20 3:00:00.000 AM) No Event Sampling Job Smart Mode

Events Patterns **Statistics (13)** Visualization

20 Per Page Format Preview

_time	id_orig_h	moyenne	ecart	count
2020-04-30 02:05:00	10.0.1.4	5.666666666666667	2.6320213205603133	2
2020-04-30 02:05:00	10.0.1.6	3.533333333333333	2.0998866182543785	2
2020-04-30 02:10:00	10.0.1.4	5.666666666666667	2.6320213205603133	1
2020-04-30 02:15:00	10.0.1.4	5.666666666666667	2.6320213205603133	1
2020-04-30 02:15:00	10.0.1.6	3.533333333333333	2.0998866182543785	2
2020-04-30 02:20:00	10.0.1.4	5.666666666666667	2.6320213205603133	1
2020-04-30 02:25:00	10.0.1.4	5.666666666666667	2.6320213205603133	4
2020-04-30 02:25:00	10.0.1.6	3.533333333333333	2.0998866182543785	1
2020-04-30 02:30:00	10.0.1.4	5.666666666666667	2.6320213205603133	8

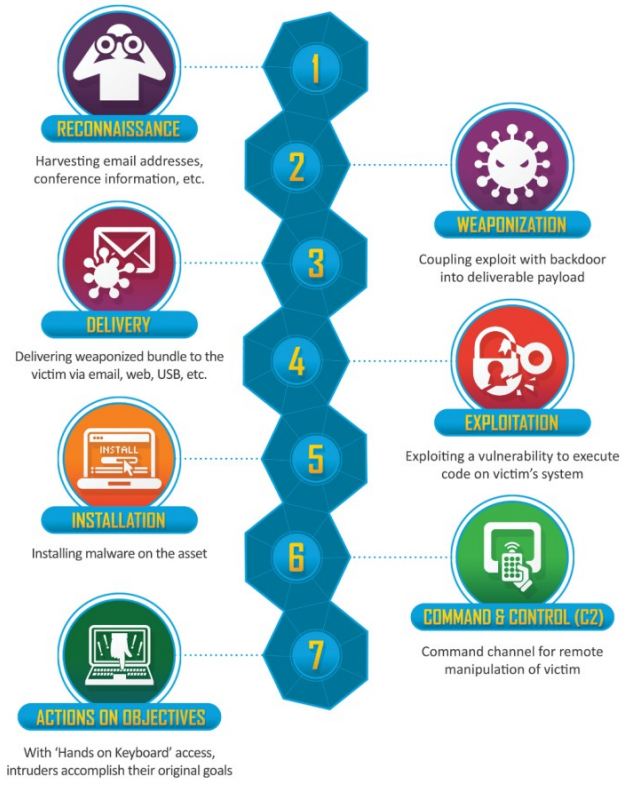
Hunting your DNS Dragons | Splunk

https://www.splunk.com/en_us/blog/security/hunting-your-dns-dragons.html

Hunting beacons | Bartosz Jerzman

https://www.x33fcon.com/archive/2019/slides/x33fcon19_Hunting_Beacons_Bartek.pdf

Investiguer, sur incident

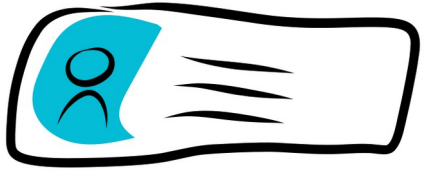


« Vous arrivez toujours trop tard ! »

https://www.lockheedmartin.com/

Pivot

sur les éléments d’intérêt



Contenu des requêtes

Un élément d’intérêt

Contenu des requêtes

... pas fondamental

John Althouse

Jeff Atkinson

Josh Atkins

Network forensics is not dead !

Merci à Nicolas, Erwan, Isabelle et Jérémy