Remixing Threat-Intelligence to Find Threats

Sebastien Tricaud
Devo Inc.

March 19 2020

What to do with Known Attacks?

Weiner's Law of Libraries

There are no answers, only cross-references.

What do we do with a known attack?

Anti-virus signature

Suricata Rule

Proxy block list

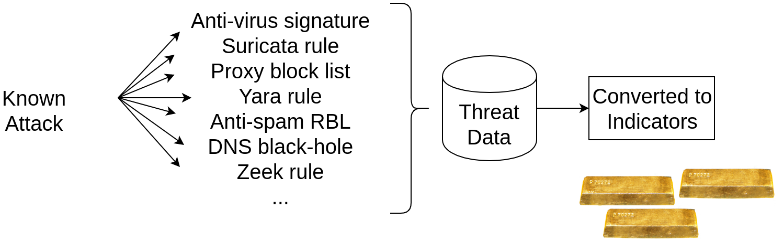
Anti-spam RBL

Yara Rule

DNS Black-hole

Zeek Rule

SIEM search pattern



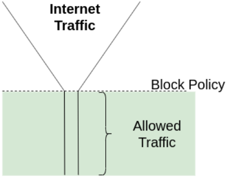
Known Attack

Anti-virus signature
Suricata rule
Proxy block list
Yara rule
Anti-spam RBL
DNS black-hole
Zeek rule
...

Threat Data

Converted to Indicators

Lessons Learned from Firewalls



DROP is the default Policy.

With Data, ACCEPT is the default Policy

Problem with Threat Intel

Describes what is bad.

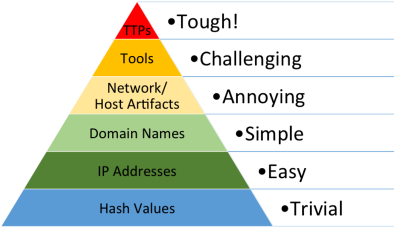
Threat Intelligence automation 101

To use all your data, you must have all your data in your SIEM.

1. Push to your SIEM, SOAR
2. Find something (hash, host, url, filename etc.) bad
3. SIEM alerts from matches

People struggle with that and shout **VICTORY** when matches occur then **cannot deal** with the amount of alerts and lack of context.

Pyramid of Pain[1]



- Read it from an attacker point of view
- Higher means more resources for the attacker
- A lot of people are sharing this Diagram as a great way to explain attack complexity

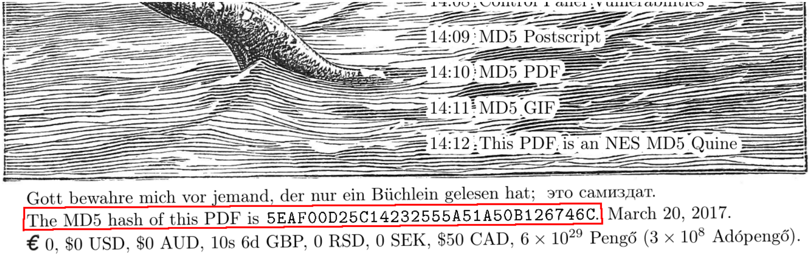
[1] Credited to David J. Bianco

Perception vs Reality

Hash Values, Trivial?

- Pyramid of Pain View
  - Highest Confidence Indicators
  - Trivial to Change
  - Least useful Indicators

Highest Confidence Indicators



14:08 Control Panel Vulnerabilities

14:09 MD5 Postscript

14:10 MD5 PDF

14:11 MD5 GIF

14:12 This PDF is an NES MD5 Quine

Gott bewahre mich vor jemand, der nur ein Büchlein gelesen hat; это самиздат.
The MD5 hash of this PDF is `5EAF00D25C14232555A51A50B126746C`. March 20, 2017.
€ 0, \$0 USD, \$0 AUD, 10s 6d GBP, 0 RSD, 0 SEK, \$50 CAD, 6×10^{29} Pengő (3×10^{8} Adópengő).

- MD5 is not trust worthy, see PoC||GTFO 14[2]
- SHA1 on MD5 footsteps

[2] Also check `https://github.com/corkami/collisions`

Trivial to Change

Sign a malware against a Microsoft Certificate. Possible? Yes. Trivial? not at all.

Perception vs Reality

Domain Names, Easy?

- Pyramid of Pain View
  - Easy to change
  - Could require some updates

Easy to Change

- Fast-Flux is trivial to detect, hence making it hard to stick a domain to a pool of IP addresses
- DGA algorithms can be discovered, reversed (and subject to vulns ;-))
- The update process could be a mean to be detected
- WannaCry kill switches have not been changed and thus killed the malware spread

Perception vs Reality

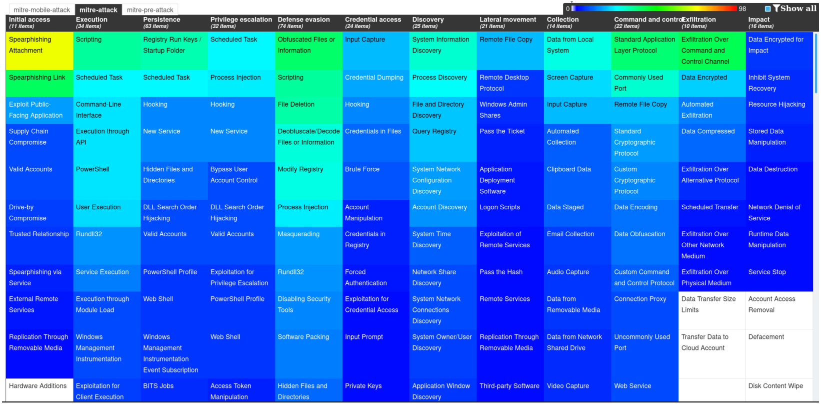
TTPs, Tough?

- Pyramid of Pain View
  - The Attacker Method
  - Hard to Change an Attack Method

Hard to Change an Attack Method

- MITRE maps TTPs in the ATT&CK Framework
- `https://attack.mitre.org/matrices/enterprise/`

Tactics, Techniques and Procedures (TTPs) categorized by MITRE ATT&CK Framework

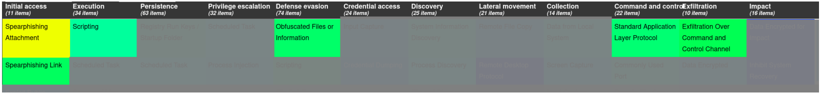


Initial access (11 items)	Execution (34 items)	Persistence (63 items)	Privilege escalation (32 items)	Defense evasion (74 items)	Credential access (24 items)	Discovery (25 items)	Lateral movement (21 items)	Collection (14 items)	Command and contro (22 items)	Exfiltration (10 items)	Impact (16 items)
Spearphishing Attachment	Scripting	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Input Capture	System Information Discovery	Remote File Copy	Data from Local System	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Spearphishing Link	Scheduled Task	Scheduled Task	Process Injection	Scripting	Credential Dumping	Process Discovery	Remote Desktop Protocol	Screen Capture	Commonly Used Port	Data Encrypted	Inhibit System Recovery
Exploit Public-Facing Application	Command-Line Interface	Hooking	Hooking	File Deletion	Hooking	File and Directory Discovery	Windows Admin Shares	Input Capture	Remote File Copy	Automated Exfiltration	Resource Hijacking
Supply Chain Compromise	Execution through API	New Service	New Service	Deobfuscate/Decode Files or Information	Credentials in Files	Query Registry	Pass the Ticket	Automated Collection	Standard Cryptographic Protocol	Data Compressed	Stored Data Manipulation
Valid Accounts	PowerShell	Hidden Files and Directories	Bypass User Account Control	Modify Registry	Brute Force	System Network Configuration Discovery	Application Deployment Software	Clipboard Data	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Data Destruction
Drive-by Compromise	User Execution	DLL Search Order Hijacking	DLL Search Order Hijacking	Process Injection	Account Manipulation	Account Discovery	Logon Scripts	Data Staged	Data Encoding	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Rundll32	Valid Accounts	Valid Accounts	Masquerading	Credentials in Registry	System Time Discovery	Exploitation of Remote Services	Email Collection	Data Obfuscation	Exfiltration Over Other Network Medium	Runtime Data Manipulation
Spearphishing via Service	Service Execution	PowerShell Profile	Exploitation for Privilege Escalation	Rundll32	Forced Authentication	Network Share Discovery	Pass the Hash	Audio Capture	Custom Command and Control Protocol	Exfiltration Over Physical Medium	Service Stop
External Remote Services	Execution through Module Load	Web Shell	PowerShell Profile	Disabling Security Tools	Exploitation for Credential Access	System Network Connections Discovery	Remote Services	Data from Removable Media	Connection Proxy	Data Transfer Size Limits	Account Access Removal
Replication Through Removable Media	Windows Management Instrumentation	Windows Management Instrumentation Event Subscription	Web Shell	Software Packing	Input Prompt	System Owner/User Discovery	Replication Through Removable Media	Data from Network Shared Drive	Uncommonly Used Port	Transfer Data to Cloud Account	Defacement
Hardware Additions	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Hidden Files and Directories	Private Keys	Application Window Discovery	Third-party Software	Video Capture	Web Service		Disk Content Wipe

From MISP Statistics over 1 year

Top 6 Sighted TTPs

Tough to change, really?

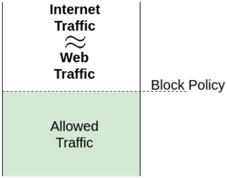


Initial access *(11 items)*	Execution *(34 items)*	Persistence *(63 items)*	Privilege escalation *(32 items)*	Defense evasion *(74 items)*	Credential access *(24 items)*	Discovery *(25 items)*	Lateral movement *(21 items)*	Collection *(14 items)*	Command and contro *(22 items)*	Exfiltration *(10 items)*	Impact *(16 items)*
Spearphishing Attachment	Scripting	Registry Run Keys / Startup Folder	Scheduled Task	Obfuscated Files or Information	Input Capture	System Information Discovery	Remote File Copy	Data from Local System	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	Data Encrypted for Impact
Spearphishing Link	Scheduled Task	Scheduled Task	Process Injection	Scripting	Credential Dumping	Process Discovery	Remote Desktop Protocol	Screen Capture	Commonly Used Port	Data Encrypted	Inhibit System Recovery

- Spearphishing Attachment
- Spearphishing Link
- Scripting
- Obfuscated Files or Information
- Standard Application Layer Protocol
- Exfiltration Over C&C Channel

Lessons Learned from Firewalls

If we drop web traffic now, we drop everything.



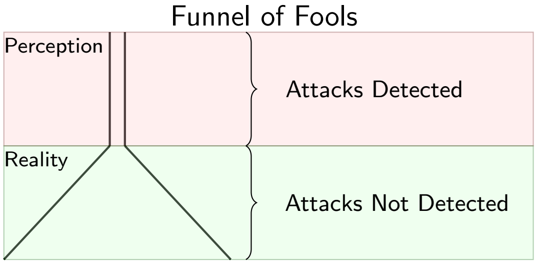
Internet Traffic ≈ Web Traffic

Block Policy

Allowed Traffic

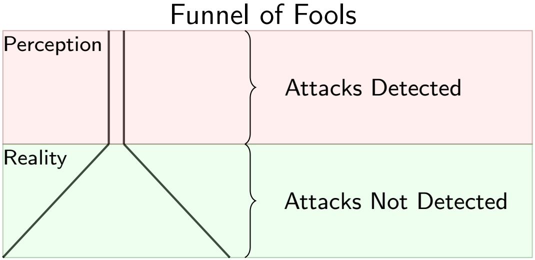
DROP Web Traffic?

Upside down funnel[3]



[3] Use it as you wish, you do not need to credit me for this

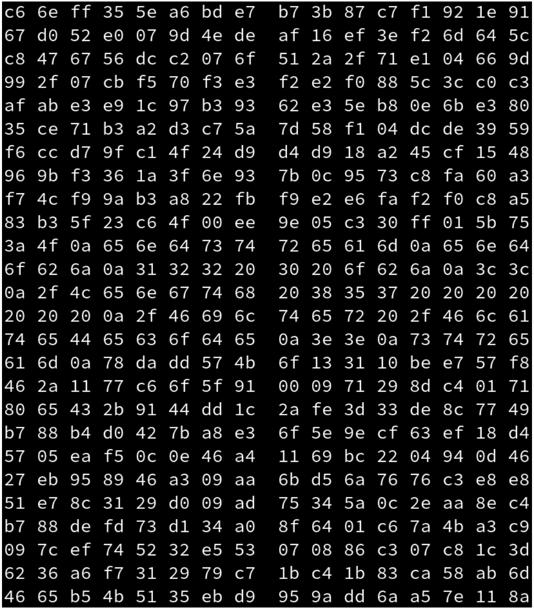
Upside down funnel[3]



- Attacks can last for years
- Incident Responder struggles to Investigate
- There are much more unnoticed attacks than alerts tell
- Challenging to cope with Unknown Attacks

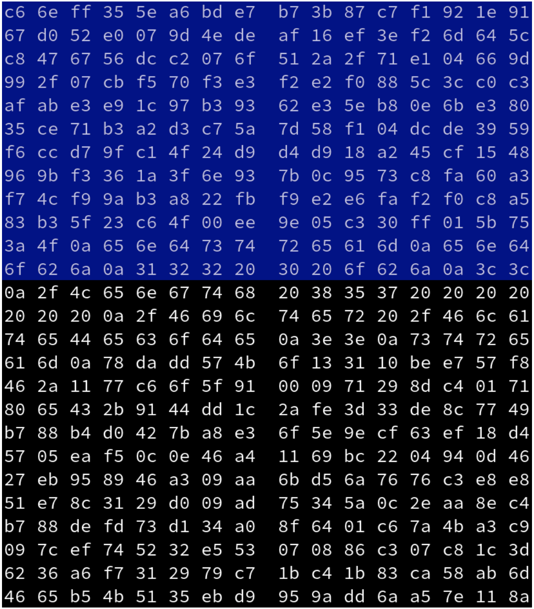
[3] Use it as you wish, you do not need to credit me for this

This is all your Data



```
c6 6e ff 35 5e a6 bd e7  b7 3b 87 c7 f1 92 1e 91
67 d0 52 e0 07 9d 4e de  af 16 ef 3e f2 6d 64 5c
c8 47 67 56 dc c2 07 6f  51 2a 2f 71 e1 04 66 9d
99 2f 07 cb f5 70 f3 e3  f2 e2 f0 88 5c 3c c0 c3
af ab e3 e9 1c 97 b3 93  62 e3 5e b8 0e 6b e3 80
35 ce 71 b3 a2 d3 c7 5a  7d 58 f1 04 dc de 39 59
f6 cc d7 9f c1 4f 24 d9  d4 d9 18 a2 45 cf 15 48
96 9b f3 36 1a 3f 6e 93  7b 0c 95 73 c8 fa 60 a3
f7 4c f9 9a b3 a8 22 fb  f9 e2 e6 fa f2 f0 c8 a5
83 b3 5f 23 c6 4f 00 ee  9e 05 c3 30 ff 01 5b 75
3a 4f 0a 65 6e 64 73 74  72 65 61 6d 0a 65 6e 64
6f 62 6a 0a 31 32 32 20  30 20 6f 62 6a 0a 3c 3c
0a 2f 4c 65 6e 67 74 68  20 38 35 37 20 20 20 20
20 20 20 0a 2f 46 69 6c  74 65 72 20 2f 46 6c 61
74 65 44 65 63 6f 64 65  0a 3e 3e 0a 73 74 72 65
61 6d 0a 78 da dd 57 4b  6f 13 31 10 be e7 57 f8
46 2a 11 77 c6 6f 5f 91  00 09 71 29 8d c4 01 71
80 65 43 2b 91 44 dd 1c  2a fe 3d 33 de 8c 77 49
b7 88 b4 d0 42 7b a8 e3  6f 5e 9e cf 63 ef 18 d4
57 05 ea f5 0c 0e 46 a4  11 69 bc 22 04 94 0d 46
27 eb 95 89 46 a3 09 aa  6b d5 6a 76 76 c3 e8 e8
51 e7 8c 31 29 d0 09 ad  75 34 5a 0c 2e aa 8e c4
b7 88 de fd 73 d1 34 a0  8f 64 01 c6 7a 4b a3 c9
09 7c ef 74 52 32 e5 53  07 08 86 c3 07 c8 1c 3d
62 36 a6 f7 31 29 79 c7  1b c4 1b 83 ca 58 ab 6d
46 65 b5 4b 51 35 eb d9  95 9a dd 6a a5 7e 11 8a
```

This what you know about your Data

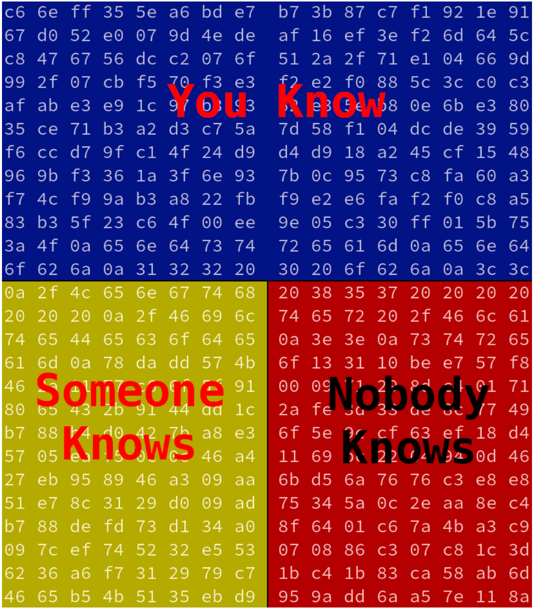


```
c6 6e ff 35 5e a6 bd e7  b7 3b 87 c7 f1 92 1e 91
67 d0 52 e0 07 9d 4e de  af 16 ef 3e f2 6d 64 5c
c8 47 67 56 dc c2 07 6f  51 2a 2f 71 e1 04 66 9d
99 2f 07 cb f5 70 f3 e3  f2 e2 f0 88 5c 3c c0 c3
af ab e3 e9 1c 97 b3 93  62 e3 5e b8 0e 6b e3 80
35 ce 71 b3 a2 d3 c7 5a  7d 58 f1 04 dc de 39 59
f6 cc d7 9f c1 4f 24 d9  d4 d9 18 a2 45 cf 15 48
96 9b f3 36 1a 3f 6e 93  7b 0c 95 73 c8 fa 60 a3
f7 4c f9 9a b3 a8 22 fb  f9 e2 e6 fa f2 f0 c8 a5
83 b3 5f 23 c6 4f 00 ee  9e 05 c3 30 ff 01 5b 75
3a 4f 0a 65 6e 64 73 74  72 65 61 6d 0a 65 6e 64
6f 62 6a 0a 31 32 32 20  30 20 6f 62 6a 0a 3c 3c
0a 2f 4c 65 6e 67 74 68  20 38 35 37 20 20 20 20
20 20 20 0a 2f 46 69 6c  74 65 72 20 2f 46 6c 61
74 65 44 65 63 6f 64 65  0a 3e 3e 0a 73 74 72 65
61 6d 0a 78 da dd 57 4b  6f 13 31 10 be e7 57 f8
46 2a 11 77 c6 6f 5f 91  00 09 71 29 8d c4 01 71
80 65 43 2b 91 44 dd 1c  2a fe 3d 33 de 8c 77 49
b7 88 b4 d0 42 7b a8 e3  6f 5e 9e cf 63 ef 18 d4
57 05 ea f5 0c 0e 46 a4  11 69 bc 22 04 94 0d 46
27 eb 95 89 46 a3 09 aa  6b d5 6a 76 76 c3 e8 e8
51 e7 8c 31 29 d0 09 ad  75 34 5a 0c 2e aa 8e c4
b7 88 de fd 73 d1 34 a0  8f 64 01 c6 7a 4b a3 c9
09 7c ef 74 52 32 e5 53  07 08 86 c3 07 c8 1c 3d
62 36 a6 f7 31 29 79 c7  1b c4 1b 83 ca 58 ab 6d
46 65 b5 4b 51 35 eb d9  95 9a dd 6a a5 7e 11 8a
```

This what others know about your Data

```
c6 6e ff 35 5e a6 bd e7  b7 3b 87 c7 f1 92 1e 91
67 d0 52 e0 07 9d 4e de  af 16 ef 3e f2 6d 64 5c
c8 47 67 56 dc c2 07 6f  51 2a 2f 71 e1 04 66 9d
99 2f 07 cb f5 70 f3 e3  f2 e2 f0 88 5c 3c c0 c3
af ab e3 e9 1c 97 b3 93  62 e3 5e b8 0e 6b e3 80
35 ce 71 b3 a2 d3 c7 5a  7d 58 f1 04 dc de 39 59
f6 cc d7 9f c1 4f 24 d9  d4 d9 18 a2 45 cf 15 48
96 9b f3 36 1a 3f 6e 93  7b 0c 95 73 c8 fa 60 a3
f7 4c f9 9a b3 a8 22 fb  f9 e2 e6 fa f2 f0 c8 a5
83 b3 5f 23 c6 4f 00 ee  9e 05 c3 30 ff 01 5b 75
3a 4f 0a 65 6e 64 73 74  72 65 61 6d 0a 65 6e 64
6f 62 6a 0a 31 32 32 20  30 20 6f 62 6a 0a 3c 3c
0a 2f 4c 65 6e 67 74 68  20 38 35 37 20 20 20 20
20 20 20 0a 2f 46 69 6c  74 65 72 20 2f 46 6c 61
74 65 44 65 63 6f 64 65  0a 3e 3e 0a 73 74 72 65
61 6d 0a 78 da dd 57 4b  6f 13 31 10 be e7 57 f8
46 2a 11 77 c6 6f 5f 91  00 09 71 29 8d c4 01 71
80 65 43 2b 91 44 dd 1c  2a fe 3d 33 de 8c 77 49
b7 88 b4 d0 42 7b a8 e3  6f 5e 9e cf 63 ef 18 d4
57 05 ea f5 0c 0e 46 a4  11 69 bc 22 04 94 0d 46
27 eb 95 89 46 a3 09 aa  6b d5 6a 76 76 c3 e8 e8
51 e7 8c 31 29 d0 09 ad  75 34 5a 0c 2e aa 8e c4
b7 88 de fd 73 d1 34 a0  8f 64 01 c6 7a 4b a3 c9
09 7c ef 74 52 32 e5 53  07 08 86 c3 07 c8 1c 3d
62 36 a6 f7 31 29 79 c7  1b c4 1b 83 ca 58 ab 6d
46 65 b5 4b 51 35 eb d9  95 9a dd 6a a5 7e 11 8a
```

Global Picture

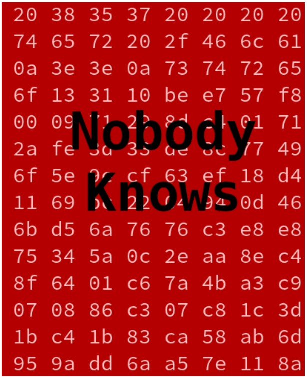


```
c6 6e ff 35 5e a6 bd e7  b7 3b 87 c7 f1 92 1e 91
67 d0 52 e0 07 9d 4e de  af 16 ef 3e f2 6d 64 5c
c8 47 67 56 dc c2 07 6f  51 2a 2f 71 e1 04 66 9d
99 2f 07 cb f5 70 f3 e3  f2 e2 f0 88 5c 3c c0 c3
af ab e3 e9 1c 97 b3 93  b2 e3 5e b8 0e 6b e3 80
35 ce 71 b3 a2 d3 c7 5a  7d 58 f1 04 dc de 39 59
f6 cc d7 9f c1 4f 24 d9  d4 d9 18 a2 45 cf 15 48
96 9b f3 36 1a 3f 6e 93  7b 0c 95 73 c8 fa 60 a3
f7 4c f9 9a b3 a8 22 fb  f9 e2 e6 fa f2 f0 c8 a5
83 b3 5f 23 c6 4f 00 ee  9e 05 c3 30 ff 01 5b 75
3a 4f 0a 65 6e 64 73 74  72 65 61 6d 0a 65 6e 64
6f 62 6a 0a 31 32 32 20  30 20 6f 62 6a 0a 3c 3c
0a 2f 4c 65 6e 67 74 68  20 38 35 37 20 20 20 20
20 20 20 0a 2f 46 69 6c  74 65 72 20 2f 46 6c 61
74 65 44 65 63 6f 64 65  0a 3e 3e 0a 73 74 72 65
61 6d 0a 78 da dd 57 4b  6f 13 31 10 be e7 57 f8
46 2a 11 77 c9 6f 5f 91  00 09 71 22 8d c4 01 71
80 65 43 2b 91 44 dd 1c  2a fe 3d 33 de 8c 77 49
b7 88 b4 d0 42 7b a8 e3  6f 5e 0c cf 63 ef 18 d4
57 05 ea f5 0c 03 46 a4  11 69 bc 22 04 94 0d 46
27 eb 95 89 46 a3 09 aa  6b d5 6a 76 76 c3 e8 e8
51 e7 8c 31 29 d0 09 ad  75 34 5a 0c 2e aa 8e c4
b7 88 de fd 73 d1 34 a0  8f 64 01 c6 7a 4b a3 c9
09 7c ef 74 52 32 e5 53  07 08 86 c3 07 c8 1c 3d
62 36 a6 f7 31 29 79 c7  1b c4 1b 83 ca 58 ab 6d
46 65 b5 4b 51 35 eb d9  95 9a dd 6a a5 7e 11 8a
```

Handling Unknown Attacks

“Unknown Attack” has been stiffed by poor marketing speeches.
Let us apply a methodology.

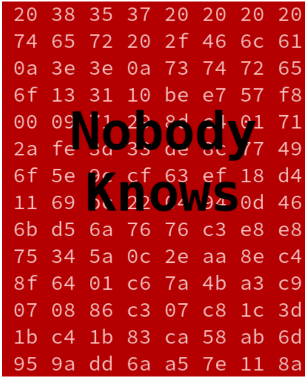
Nobody Knows



```
20 38 35 37 20 20 20 20
74 65 72 20 2f 46 6c 61
0a 3e 3e 0a 73 74 72 65
6f 13 31 10 be e7 57 f8
00 09 71 22 8d c4 01 71
2a fe 3d 35 de 8c 77 49
6f 5e 0c cf 63 ef 18 d4
11 69 5c 22 04 94 0d 46
6b d5 6a 76 76 c3 e8 e8
75 34 5a 0c 2e aa 8e c4
8f 64 01 c6 7a 4b a3 c9
07 08 86 c3 07 c8 1c 3d
1b c4 1b 83 ca 58 ab 6d
95 9a dd 6a a5 7e 11 8a
```

- Machine Learning? $\Longrightarrow$ Learning from uncertainty? Slow results

Nobody Knows



```
20 38 35 37 20 20 20 20
74 65 72 20 2f 46 6c 61
0a 3e 3e 0a 73 74 72 65
6f 13 31 10 be e7 57 f8
00 09 71 22 8d c4 01 71
2a fe 3d 33 de 8c 77 49
6f 5e 0c cf 63 ef 18 d4
11 69 6c 22 04 94 0d 46
6b d5 6a 76 76 c3 e8 e8
75 34 5a 0c 2e aa 8e c4
8f 64 01 c6 7a 4b a3 c9
07 08 86 c3 07 c8 1c 3d
1b c4 1b 83 ca 58 ab 6d
95 9a dd 6a a5 7e 11 8a
```

- Machine Learning? $\Longrightarrow$ Learning from uncertainty? Slow results
- Investigate? $\Longrightarrow$ Bet on luck? Slow results

One week analyzing proxy logs URLs with million users

We use faup[4] to parse URLs.

```
echo "http://root:admin@example.com:80/client32.dll?GetAd=&PG=IM23&AP=321#foo"
 | faup -o json
{
"scheme": "http",
"credential": "root:admin",
"subdomain": "",
"domain": "example.com",
"domain_without_tld": "example",
"host": "example.com",
"tld": "com",
"port": "80",
"resource_path": "/myclient32.dll",
"query_string": "?GetAd=&PG=IM23&AP=321",
"fragment": "#foo",
"url_type": "mozilla_tld"
}
```

[4] https://github.com/stricaud/faup

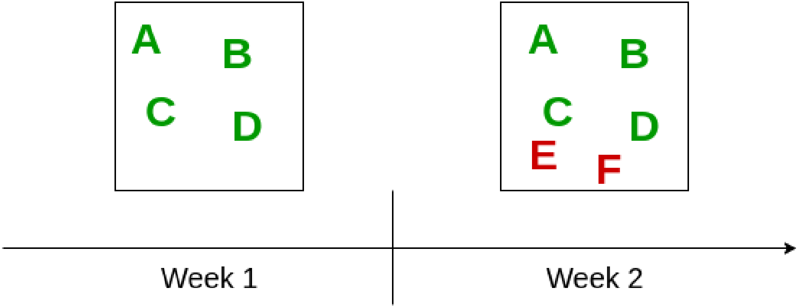
Time Frame

From	2011-08-04 21:00:00
To	2011-08-05 14:05:54

9.7Gb	Total file size
22 843 587	Total number of events
64 193	Unique domains
28 520	Subdomains and TLDs removed

Reduction of 80%

Faup with Snapshots



Creating a snapshot with faup

```
$ cat test.snapshot
www.cansecwest.com
www.cansecwest.com
https://packetstormsecurity.com

$ faup -q -s test test.snapshot
```

Checking a domain from that snapshot

```
$ faup $ snapshot get test domain cansecwest.com
{"value": "cansecwest.com", "count": 2, \
 "first seen": "2020-03-18 10:16:59 -0700", \
 "last seen": "2020-03-18 10:16:59 -0700"}
```

Automating Whitelisting 1/2

Create a Snapshot

Take one month of your URLs

- We know there is bad stuff in there
- We assume it is all good
- We can always investigate later

Automating Whitelisting 2/2

Compare your snapshot

Focus on new URLs, compare

- Malware generally do not persist over time
- Focus on newness

This is Sightings

```
{"value": "cansecwest.com", "count": 2, \
 "first seen": "2020-03-18 10:16:59 -0700", \
 "last seen": "2020-03-18 10:16:59 -0700"}
```

Sightings

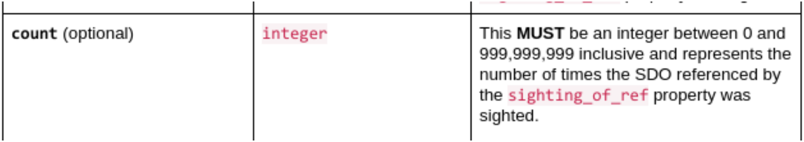
Sightings is the art of moving Threat Intel from **what is bad** to **when is observed**.

Who is standardizing Sightings?

- The MISP Project
  - https://www.misp-standard.org/rfc/sightingdb-format.txt
- ATT&CK
  - https://attack.mitre.org/resources/sightings/
- OASIS STIX v2
  - https://oasis-open.github.io/cti-documentation/stix/intro.html
  - https://docs.google.com/document/d/1IvkLxg_tCnICsatu2lyxKmWmh1gY2h8HUNssKIE-UIA/

Interesting constraints in OASIS STIX v2

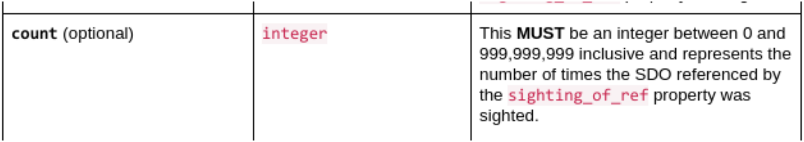
A Sightings value can only **count** up to 999,999,999.



count (optional)	integer	This **MUST** be an integer between 0 and 999,999,999 inclusive and represents the number of times the SDO referenced by the sighting_of_ref property was sighted.

Interesting constraints in OASIS STIX v2

A Sightings value can only **count** up to 999,999,999.



count (optional)	integer	This **MUST** be an integer between 0 and 999,999,999 inclusive and represents the number of times the SDO referenced by the sighting_of_ref property was sighted.

From the JSON Standard:

```
numbers that are integers and are in the
range [-(2**53)+1, (2**53)-1] are interoperable
in the sense that implementations will agree
exactly on their numeric values
```

```
  >>> 2**53-1
  9007199254740991
```

Introducing SightingDB 0.2!

CanSecWest 2020 release!

Introducing SightingDB 0.2!

CanSecWest 2020 release!

`https://github.com/stricaud/sightingdb/`

A Scalable Sighting Database, hybrid in-memory/on-disc whose goal is to provide an easy to use way to count attributes.

Design

- Modeled after Zookeeper for its key-value store capability:
  - a key is a namespace, such as “foo/bar” where “bar” is a child of “foo”.
  - it allows to create as many placeholders as anyone dream
  - a value is simply a string

Why not Redis?

- Redis is not tailored for our very specific use-case
- Incrementing a value (INCR) in Redis is atomic
- Atomic means a lock on the key for writing, preventing multiple threads / resources to increment at the same time

REST API: Write

```
$ curl -k https://localhost:9999/w/foo/bar/?val=hello
{"message":"ok"}
```

REST API: Read

```
$ curl -k https://localhost:9999/r/foo/bar/?val=hello
{"value":"hello","first_seen":1581627580,
 "last_seen":1581627580,"count":1,"tags":"",
 "ttl":0}
```

Key being a namespace, powerful.

- Want to be compatible with ATT&CK?
  /direct-software-sighting/JCry

Key being a namespace, powerful.

- Want to be compatible with ATT&CK? **/direct-software-sighting/JCry**
- Want to store relationships with a particular IP in the finance BU? **/finance/8.8.8.8/**

Key being a namespace, powerful.

- Want to be compatible with ATT&CK? **/direct-software-sighting/JCry**
- Want to store relationships with a particular IP in the finance BU? **/finance/8.8.8.8/**
- Want to store a url? **/url/**

Key being a namespace, powerful.

- Want to be compatible with ATT&CK? **/direct-software-sighting/JCry**
- Want to store relationships with a particular IP in the finance BU? **/finance/8.8.8.8/**
- Want to store a url? **/url/**
- Want to store the url for all TLD in ch? **/url/tld/ca/**

Key being a namespace, powerful.

- Want to be compatible with ATT&CK? **/direct-software-sighting/JCry**
- Want to store relationships with a particular IP in the finance BU? **/finance/8.8.8.8/**
- Want to store a url? **/url/**
- Want to store the url for all TLD in ch? **/url/tld/ca/**
- Want to store the ch TLD related URLs to find them faster? **/ca/tld/url/**

Key being a namespace, powerful.

- Want to be compatible with ATT&CK? **/direct-software-sighting/JCry**
- Want to store relationships with a particular IP in the finance BU? **/finance/8.8.8.8/**
- Want to store a url? **/url/**
- Want to store the url for all TLD in ch? **/url/tld/ca/**
- Want to store the ch TLD related URLs to find them faster? **/ca/tld/url/**
- Want to see how many times somebody searched for the value `https://www.cansecwest.com` from */url/*? **Shadow Sightings!**

Shadow Sightings

- When we read, we write!

Shadow Sightings

- When we read, we write!
- How many time did somebody searched for a value in a namespace?
- SightingDB stores automatically into /**_shadow**/
- SightingDB also stores recursive access

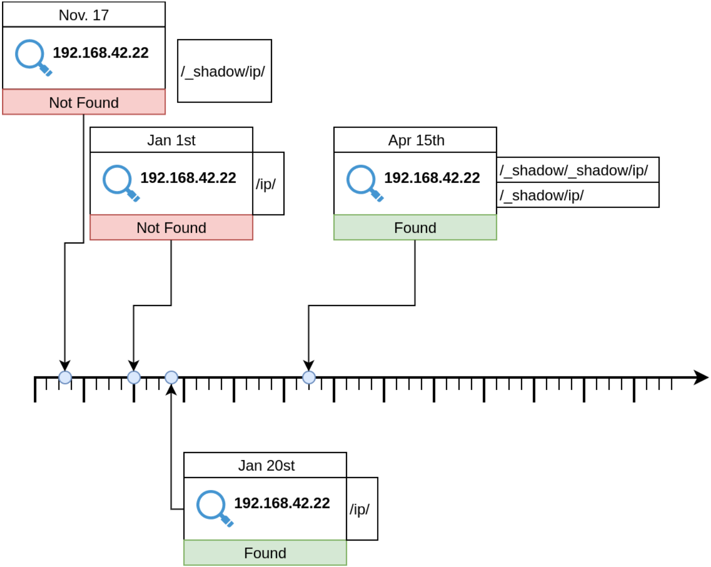
Sightings on our proxy dataset

```
$ curl -k https://localhost:9999/r/cansec/proxy?val=www.cansecwest.com
{"error":"Value not found","path":"cansec/proxy","value":"www.cansecwest.com"}

$ curl -k https://localhost:9999/r/_shadow/cansec/proxy?val=www.cansecwest.com
{"value":"www.cansecwest.com","first_seen":1584581469,
 "last_seen":1584581487,"count":1,"tags":"","ttl":0}
```

Shadow Sightings

Leading indicator: **someone has searched**, not the detection

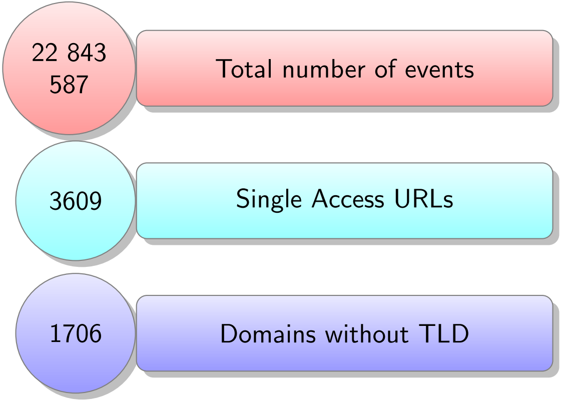


Top 3 Sightings matches

Domain	Count
www.google.com	1208671
www.google-analytics.com	890044
au.download.windowsupdate.com	435872

$\approx$ 11% of total events

How many had only a single access?



22 843 587	Total number of events
3609	Single Access URLs
1706	Domains without TLD

Not much data to look at.

Indicators of Trust

Mirror Approach

Reuse the principle of DROP policy established in Firewalling

- Instead of Sharing Bad Stuff to look at, Share Good Stuff
- MISP tag="svc:trust-domain="cansecwest.com""
- Use the Path in SightingDB: svc/trust-domain/ for domains

Benefits

- You can process all the data, making life harder to the attacker
- The more data, the better Sightings are
- Enable a community to influence credibility
- Lower the amount of **unknown to everyone** data
- Work on things you care about on your data: unique, new etc.

Want to join the community? CanSecWest is Trustworthy, email me and let's get started!

Thank You!

sebastien.tricaud@devo.com
@tricaud