Passive SSL

Passive Detection and Reconnaissance Techniques, to Find, Track, and Attribute Vulnerable "Devices"

CIRCL
Computer Incident
Response Center
Luxembourg

UNIVERSITY OF CAMBRIDGE
Judge Business School
Centre for
Risk Studies

Alexandre Dulaunoy
@adulau
Eireann Leverett
@blackswanburst

TLP:WHITE

June 17, 2015

Datasets used

- Eireann used Shodan stream of certificates (350k certificates in counting Bloomfilter).
    - Thanks to John (Shodan) Matherly.
- Alex used the CIRCL Passive SSL datasets (around 100 millions certificates).
    - Thanks to GCHQ (for the idea).

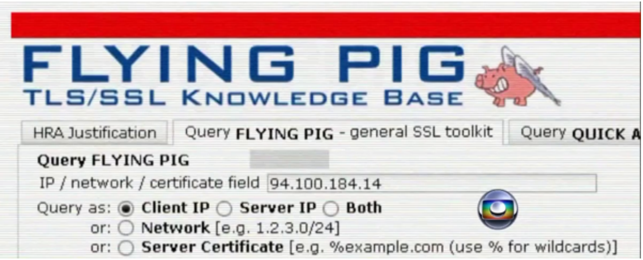
Problem statement

CSIRT or LIRT or security analysts have recurring issues to:

- Find owners of IP addresses.
- Detect usage of CIDR blocks.
- Find vulnerable systems passively (and avoid intrusive scanning).
  - Scale of potential impact.
- Detect compromised services.

Acknowlegement

- Thanks to GCHQ and the FLYING PIG program
- and Edward Snowden for releasing the document.



FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK A**

Query FLYING PIG

IP / network / certificate field: 94.100.184.14

Query as: ● **Client IP** ○ **Server IP** ○ **Both**
or: ○ **Network** [e.g. 1.2.3.0/24]
or: ○ **Server Certificate** [e.g. %example.com (use % for wildcards)]

- Double edge techniques that can be used for good or bad reasons.
- Another opportunity to improve your threat modeling and your weak TLS knowledge.

Passive SSL

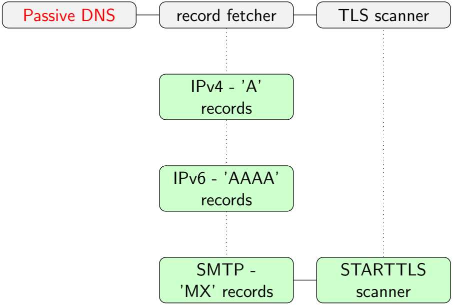
- Replicating Passive DNS concepts into SSL/TLS.
- Keeping a history of X.509 certificates seen per IP address.
  - Usage over time of the X.509 certificates.
- Providing a search ReST interface per IP address, CIDR block.
- Tracing the use of CA and CRL/OCSP.

Collecting X.509 Certificates - Internet Scanning

- Scan the Internet yourself (e.g. In a single scan of the IPv4 space, close to 50 millions certificates).
- Which port to scan? protocol or service? pps?
- How often? (e.g. weekly scan helps to determine the stability of an IP,Certificate tuple)
- Cannot scan, you can reuse existing scanning data (e.g. `scans.io`).

Collecting X.509 Certificates - Passive DNS - SNI

- On a single IPv4 address, you can have more than one certificate.
  - Alternate SSL ports, multihomed systems
  - Other services: SSL-VPN, ESMTP, DTLS, IMAP, ...
- How to scan IPv6 address space for X.509 Certificates.
- Passive DNS used as a source for SNI (Server Name Indication) value or IPv6 addresses.



Collecting X.509 Certificates - Network Interception

- Tapping a network interface where SSL/TLS handshakes are performed.
- TCP reassembly is still hard and finding SSL/TLS handshakes is a complementary problem.
- ssldump[1], Suricata, Moloch,...
- If you collect SSL/TLS handshakes in your internal network, don't forget the impact of intercepting proxies.

[1] `http://www.github.com/adulau/ssldump`

Collecting X.509 Certificates from Tor exit nodes

- Tor exit nodes traffic is an interesting source of alternative X.509 certificates (e.g. Tor circuits, XMPP sessions, TLS on non-standard ports).
- A huge proportion of flows uses TLS which provides a good overview of the most active X.509 certificates (e.g. Google, .vk.com...).
- Don't forget, not all the security researchers have good intention (e.g. FLYING PIG).

Security Perspective of X.509 Certificates

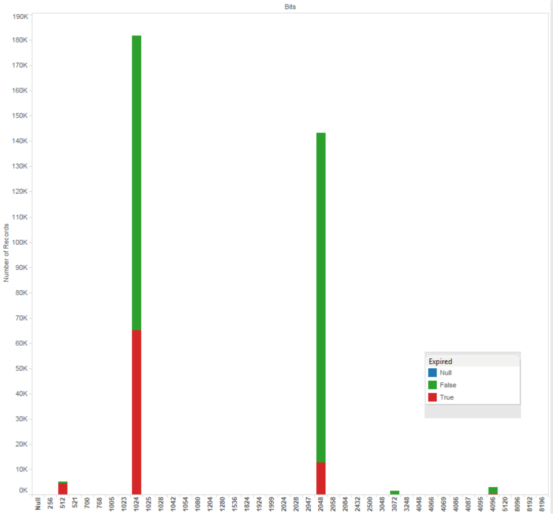
- Subject Name and Issuer Name can provide a lot of details about the devices, issuers or the overall security practices.
  - A lot of X.509 certificates are automatically generated without the users knowledge.
  - Detailed or sensitive information can leak in the X.509 certificate fields.

```
4fd64e325ec7a14ac2e34bb5cfed28fef24c3ffb,C=DE, ST=Bavaria, L=Ingolstadt, O=Kaspersky Lab GmbH, OU=Pre-Sales, CN=rdg.klab.it.cx/emailAddress=consulting@kaspersky.de
dc4a127eae8a47a8041a4ce7f1a214c3e6957cd6,C=RU, ST=Moscow, L=Moscow, O=Kaspersky Lab ZAO, OU=IT, CN=nordnetsync.anti-theft.kaspersky.com
8a9c839f2ff275c79a985ea84b89bc9fa404d010,C=RU, ST=Moscow, L=Moscow, O=Kaspersky Lab, OU=IT, CN=owa.kaspersky.com
```

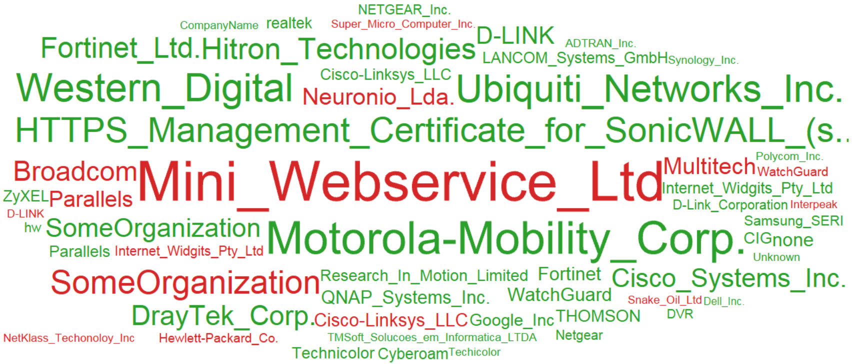
Key-size distribution

Occurences	Key-size
181899	1024
143532	2048
4997	512
2845	4096
1467	3072
36	1023
33	256
30	2432
26	768
13	8192
11	2047
10	1536

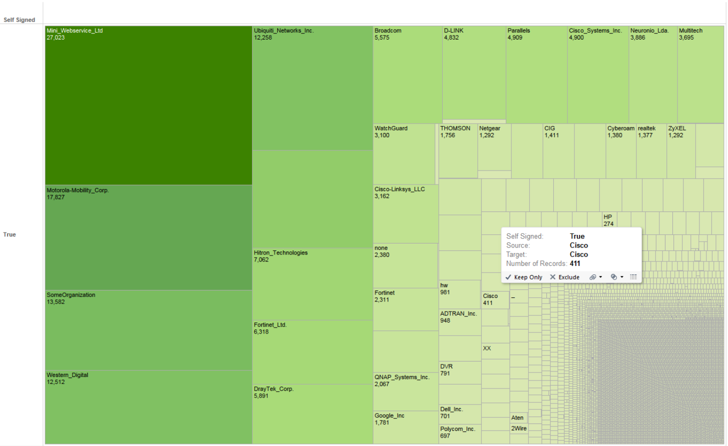
Key-size and Revocation



An Overview of Most Common Self-signed Certificates



Most Common Subject and Org Names in X.509



Self Signed: True
Source: Cisco
Target: Cisco
Number of Records: 411

Dyre malware and SSL fingerprint

- Dyre malware contains a list of static IP addresses to reach as C&C. What kind of C&C?

```
{"5.44.15.70": ["C=US, ST=CA, L=San Jose, O=Ubiquiti Networks Inc., OU=Technical Support, CN=UBNT/emailAddress=support@ubnt.com"]}
{"93.184.71.88": ["C=US, ST=CA, L=San Jose, O=Ubiquiti Networks Inc., OU=Technical Support, CN=UBNT/emailAddress=support@ubnt.com"]}
```

- The compromised Ubiquiti routers (with default password) were compromised to proxy SSL connections.

How to find user of a specific software?

- Who use MobileIron Mobile Device Management? More than 11000 certificates on a two-year period.

```
c2ef4df6c7be287f78ae9178d65e8078f253cfb1,C=US, ST=California, L=Sunnyvale, O=MobileIron, OU=Support, CN=ActiveSyncProxyCA/emailAddress=support@mobileiron.com
5c10590f0e977c15805124ddc00f470383768b10,C=US, ST=California, L=Sunnyvale, O=MobileIron, OU=Support, CN=usslmmdmsecapp004.net.plm.eds.com/emailAddress=support@mobileiron.com
9ce9edf68ecbf59c746e0d3bbe6d98d72b65fed3,C=US, ST=California, L=Sunnyvale, O=MobileIron, OU=Support, CN=mbx-desat-otn.defdh.astrium.eads.net/emailAddress=support@mobileiron.com
b47ec8382624035448eebcf15a1cd402425ca661,C=US, ST=California, L=Sunnyvale, O=MobileIron, OU=Support, CN=ActiveSyncProxyCA/emailAddress=support@mobileiron.com
5190314e4590420e75a2e7b21c74b34255da0806,C=US, ST=California, L=Sunnyvale, O=MobileIron, OU=Support, CN=ats.patrizia.ag/emailAddress=support@mobileiron.com
```

Detecting dynamic IP ranges?

- SSL/TLS services are often running on dynamic IP ranges. Users use dynamic DNS. Dynamic ranges managed by ISP can be detected and associated users too.

```
d53cc7380ed06c8b8ef0163952c9c534afad7ab8,CN=pino007.ath.cx
92bfef7362de7b381c723a2a352d54d82d49712a,CN=profinance.ath.cx
2cd0f2033c756222c976b631dba1a95a87aeadf9,CN=kschaub.ath.cx
c0de4fe83452046c0529b74f6081a39f82907746,CN=fferemote.ath.cx
b0d04a23ff6da2191d7b78f72352f1196802f61f,CN=hm01-server.Filmhotel.local, CN=
    localhost, CN=hm01-server, CN=companyweb, CN=filmhotel.ath.cx
a4b54adb780a5c9ea737399f9492f9f4dafc721d,CN=praxis-drciftci.ath.cx
77b89a57304256562ebfa42024fa9adeb304ad5a,CN=remote.mandk.ath.cx
```

Popcorn time

```
e4bd71c2e365b61b39d775ba43ef936a4fe9175c,C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=*.*
1fc3a857a14ca15d3c37fdb2c8b7e0de01e4f0fd,C=IL, ST=Tel Aviv, O=Visonic Ltd., CN=*.*
397b25c864131bc78aff25622296171d60843318,C=IE, ST=Dublin, O=Fuck SSL Cartels, CN=*.nosmo.me/emailAddress=nosmo@nosmo.me
```

- We can laugh at everything? Especially with this certificate proposed by 94.242.58.131

```
06892001be0854570546b1e609d33a5510290e3b,C=US, ST=California, L=Mountain View, O=GeoTrust Inc., OU=GeoTrust Global CA, CN=*.*

Issuer: C=US, ST=California, L=Mountain View, O=GeoTrust Inc., OU=GeoTrust Global CA, CN=*.*
Validity
    Not Before: May 19 09:54:04 2015 GMT
    Not After : May 16 09:54:04 2025 GMT
Subject: C=US, ST=California, L=Mountain View, O=GeoTrust Inc., OU=GeoTrust Global CA, CN=*.*
```

Conclusion

- Passive SSL helped us to get in contact with owners of vulnerable or abused systems.
- Passive SSL is an ongoing project and you can request access if do incident handling or security research[2].
- Weird occurences in dataset lead to additional insights.
- Analysing the same dataset with different eyes improved analysis.
- Comparing different datasets can be independant verification of facts or proportion.
- Information visualisation can be used as a navigation strategy before deep diving.

[2] `https://www.circl.lu/services/passive-ssl/`

Q&A

- @blackswanburst - eireann.leverett@cantab.net
- @adulau - alexandre.dulaunoy@circl.lu