NETWORK EXPLOITATION

PROFILING SSL AND ATTRIBUTING PRIVATE NETWORKS

An introduction to FLYING PIG and HUSH PUPPY

[redacted]

ICTR - Network Exploitation
GCHQ

Outline

NETWORK EXPLOITATION

- Two separate prototypes – FLYING PIG and HUSH PUPPY
- Both are cloud analytics which work on bulk unselected data
- FLYING PIG is a knowledge base for investigating TLS/ SSL traffic
- HUSH PUPPY is a tool for attributing private network traffic

FLYING PIG - TLS/SSL Background

- TLS/SSL (Transport Layer Security / Secure Sockets Layer) provides encrypted communication over the internet
- Simple TLS/SSL handshake:

Motivations for FLYING PIG

NETWORK EXPLOITATION

- More and more services used by GCHQ targets are moving to TLS/SSL to increase user confidence, e.g. Hotmail, Yahoo, Gmail, etc.

- Terrorists and cyber criminals are common users of TLS/SSL to hide their comms (not necessarily using the big providers).

- A TLS/SSL knowledge base could provide a means to extract as much information from the unencrypted traffic as possible.

FLYING PIG implementation

- **Federated QFD approach**
  - Multiple separate cloud analytics, each of which produce a QFD (Query Focussed Dataset).
  - Analytics are run once a week, on approximately 20 billion events.
  - A single query in the web interface results in calls to multiple QFDs, which are returned to the user in separate panels.
  - Results in:
    (a) fast queries,
    (b) easy-to-maintain modular code, and importantly
    (c) easy to add future TLS/SSL QFDs.

Query by certificate metadata

FLYING PIG
TLS/SSL Knowledge Base

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK ANT** - Tor events QFD

Prototype owner: [redacted] ICTR-NE

Query FLYING PIG

IP / network / certificate field: %mail.ru

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)]

Run Query!

Server certificate fields to search within:

- [x] Subject common name
- [ ] Subject organisation name
- [x] Issuer common name
- [ ] Issuer organisation name
- [ ] RSA modulus

Certificate field search: %mail.ru

All HTTP requests matching your query (?)

1 - 5 of 500 items — 10 | 25 | 50 | 100 — 1 2 3 4 5 6 7

Server IP	Host name	First seen	Last seen	Count w/e 25th Nov	Count all time
184.105	swa.mail.ru	2011-10-13 16:05:53.0	2011-11-25 21:11:59.0	6085663	42640739
184.104	swa.mail.ru	2011-10-13 17:29:18.0	2011-11-25 21:11:55.0	6073183	36825411
134.201	fc.ef.d4.cf.bd.a1.top.mail.ru	2011-10-13 21:43:10.0	2011-11-25 21:10:49.0	4049743	19360920
135.13	top5.mail.ru	2011-10-14 20:00:00.0	2011-11-25 21:12:05.0	3006868	14168963
135.12	top3.mail.ru	2011-10-14 20:00:00.0	2011-11-25 21:10:48.0	2480950	12386999

All certificates matching your query (?)

Tip 1: Right click on a row to find all server IPs that serve that certificate!
Tip 2: Click on the disk icon in the title bar to download data in CSV format!
Tip 3: Double-click on a field to enable copy and paste!
Tip 4: Change displayed columns ('Basic' is default; 'Advanced' adds RSA Modulus and cipher suite distribution columns): Basic columns | Advanced columns

1 - 10 of 70 items — **10** | 25 | 50 | 100 — 1 2 3 4 5 6 7

Full Certificate	First seen	Last seen	Count w/e 25th Nov	Count all time	Valid from	Valid to	Subject common name	Subject country	Subject org name	Issuer common name	Issuer country	Issuer org name	Self signe
308203CD3082(	2011-09-22 13:17:32	2011-11-25 19:01:59	2952729	16638958	2011-01-31 00:00:00	2012-03-27 23:59:59	*.mail.ru	ru	llc mail.ru	thawte ssl ca	us	thawte, inc.	N
308203613082(	2011-09-22 14:05:50	2011-11-25 18:58:32	249926	1085232	2010-01-21 00:00:00	2011-02-20 23:59:59	*.mail.ru	ru	llc mail.ru	thawte premium server ca	za	thawte consulting cc	N
308203D33082(	2011-10-07 20:29:55	2011-11-25 18:53:40	10059	30520	2011-09-25 00:00:00	2013-11-23 23:59:59	*.money.mail.ru	ru	llc mail.ru	thawte ssl ca	us	thawte, inc.	N
308203513082(	2011-09-23 17:01:58	2011-11-25 15:40:05	976	8517	2010-01-25 15:42:05	2012-01-27 18:12:59	mail.ru.is	is	mail.ru.is		us	equifax	N
308202C83082(	2011-08-22 08:14:21	2011-09-06 06:15:36	0	1482	2011-03-04 06:42:12	2012-03-03 06:42:12	mail.ru-sib.ru	us		mail.ru-sib.ru	us		Y
308204383082(	2011-10-17 14:09:52	2011-11-25 18:50:10	22	1236	2011-05-27 00:00:00	2012-07-25 23:59:59	mail.ru-com.ru		mail.ru-com.ru	thawte dv ssl ca	us	thawte, inc.	N
308203C43082(	2011-10-08 00:05:24	2011-11-25 17:04:02	301	1150	2010-02-13 14:19:06	2012-11-08 14:19:06	mx1.shogo-mail.ru	ru	shogo	shogo.ru	ru	shogo	N
308204153082(	2011-11-01 07:36:53	2011-11-25 14:26:29	246	693	2011-09-15 11:47:51	2012-09-14 11:47:51	limgs.mail.ru	ru		isp.cegedim.fr	fr	cegedim	N
308202E43082(	2011-10-14 18:20:34	2011-11-21 05:13:34	201	306	2011-10-05 08:07:34	2014-10-04 08:07:34	moder.foto.mail.ru	ru	mail.ru	moder.foto.mail.ru	ru	mail.ru	Y
308204153082(	2011-10-31 14:14:12	2011-11-25 15:45:50	99	259	2011-09-15 11:47:51	2012-09-14 11:47:51	auth.mail.ru	ru		isp.cegedim.fr	fr	cegedim	N

Server IPs (?):

Tip 1: Right click on a server IP to explore it further!

1 - 25 of 500 items — 1 2 3 4 5 6 7

Server IP	Cert count w/e 25th Nov	Cert count all time
184.14	257642	2250179
177.1	333592	1052618
191.213	330212	1388617
184.16	308599	2496916
184.17	297282	2226133
184.15	294437	2395012
189.160	168414	659037
184.77	120533	560336
184.74	113555	515169
184.75	112574	538512
184.76	110325	690098
135.55	3779	6023
135.56	3740	7358
134.151	3564	8498
63.121	2532	4887
136.43	2523	9226
134.98	2360	9165
179.89	2227	7600
179.90	2051	7320
136.84	1981	8442

Explore this server IP further!

Query by server IP

FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK ANT** - Tor events QFD

Prototype owner: [redacted] ICTR-NE

Query FLYING PIG

IP / network / certificate fiel .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)]

Run Query!

Server IP-specific panels

General IP info	☑	SSL Server certificates seen on this IP	☑
Top 10 SSL client geos	☑	SSL Pattern of life	☑
Top 10 SSL server ports	☑	HTTP requests to this IP	☑
Top 10 SSL case notations	☑	Top 100 SSL clients	☑
SSL Traffic stats	☑		

Certificate field search: %mail.ru ⊗ **Server I .184.14** ⊗

General IP info for server IP .184.14

Geolocation (?):
Country: **RU** (M)
City: **MOSCOW** (L)

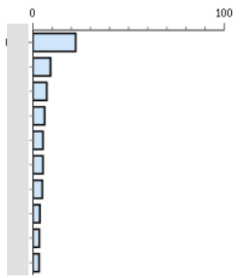
WHOIS info (?):
Network: 76.0/20. Network type: No results.
Company: **Mail.Ru**. Domain: **mail.ru**.

AS info (?):
Advertised by AS: **47764**. Found within network:
76.0/20.
AS name: **MAILRU-AS Limited liability company Mail.Ru**.

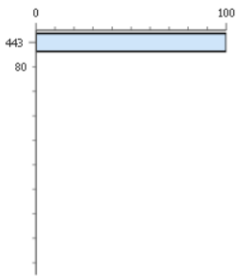
DNS (?):
No results

Tor node (?):
No matches

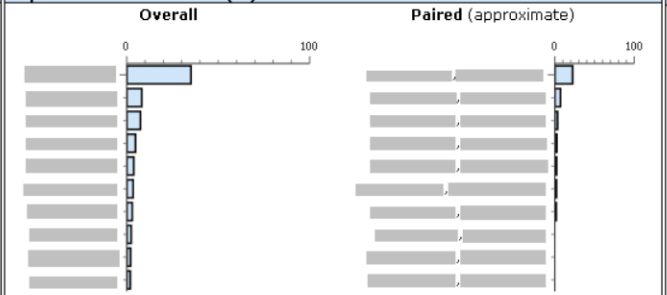
Top 10 SSL client geos (?)



Top 10 SSL server ports (?)

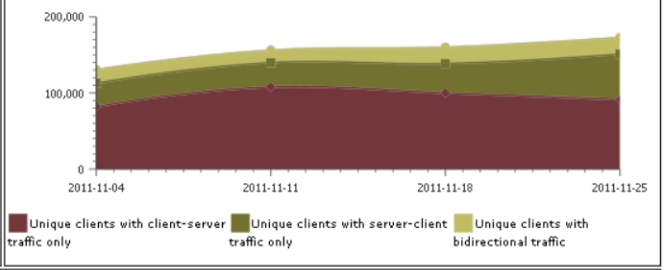


Top 10 SSL case notations (?)



SSL Traffic stats (?):

For week ending **2011-12-23**:
No. unique clients = **104317**.
% client-server IPs with traffic seen in both directions = **14.7%**.



SSL Certificates seen on this IP (?)

Tip 1: Right click on a certificate to explore it further!

1 - 3 of 3 items 10 | 25 | 50 | 100 1

First seen on this IP	Last seen on this IP	Count w/e 25th Nov	Count all time	Valid from	Valid to	Subject common name	Issuer common name
2011-09-22 13:31:06	2011-11-25 19:01:47	357643	2359179	2011-01-31 00:00:00	2012-03-27 23:59:59	*.mail.ru	thawte ssl ca
2011-08-08 12:23:45	2011-11-25 07:50:07	1441	1447304	2011-01-31 00:00:00	2012-03-27 23:59:59	*.mail.ru	thawte ssl ca
2011-11-16 14:13:03	2011-11-16 14:13:03	0	1	2011-08-05 18:34:19	2014-08-05 18:34:19	*.vkontakte.ru	go daddy secure certification authority

Average pattern of life for a client (seeded around SSL events to this server IP) (?)

Tip 1: Filter by min. % occurrences of event: 1% Apply filtering

1 - 8 of 233 items 10 | 25 | 50 | 100 1 2 3 4 5 6 7

Correlated event	Event IP	Event port	Percentage occurrences of event
GET request to top3.mail.ru	135.12	80	28.1
GET request to top5.mail.ru	135.13	80	15.1
GET request to d0.c1.bf.a1.top.mail.ru	134.253	80	14.2
GET request to my.mail.ru	184.40	80	13.2

HTTP requests to this IP (top 100) (?)

Tip 1: Right click on a server IP to explore it as an SSL server!

1 - 10 of 226 items 10 | 25 | 50 | 100 1 2 3 4 5 6 7

Server IP	Host name requested	First seen	Last seen	Count last week	Count all time
184.14	e.mail.ru	2011-10-14	2011-11-25	1989215	13992636
184.14	m.mail.ru	2011-10-14	2011-11-25	89268	664189
184.14	184.14	2011-10-14	2011-11-25	17426	108536
184.14	auth.mail.ru	2011-10-14	2011-11-25	11738	70020
184.14	tel.mail.ru	2011-10-14	2011-11-25	8994	65540

Query by server IP

FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK ANT** - Tor events QFD

Prototype owner: [redacted] ICTR-NE

Query FLYING PIG

IP / network / certificate fiel 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)]

Run Query!

Server IP-specific panels

General IP info	✓	SSL Server certificates seen on this IP	✓
Top 10 SSL client geos	✓	SSL Pattern of life	✓
Top 10 SSL server ports	✓	HTTP requests to this IP	✓
Top 10 SSL case notations	✓	Top 100 SSL clients	✓
SSL Traffic stats	✓		

Certificate field search: %mail.ru Server I .184.14

GET request to top3.mail.ru	135.12	80	28.1
GET request to top5.mail.ru	135.13	80	15.1
GET request to d0.c1.bf.a1.top.mail.ru	134.253	80	14.2
GET request to my.mail.ru	184.40	80	13.2
GET request to my.mail.ru	184.41	80	12.9
GET request to stat.my.mail.ru	184.40	80	10.8
GET request to stat.my.mail.ru	184.41	80	10.5
GET request to mrimraker1.mail.ru	189.183	80	10.4

184.14	m.mail.ru	2011-10-14	2011-11-25	89268	664189
184.14	94.100.184.14	2011-10-14	2011-11-25	17426	108536
184.14	auth.mail.ru	2011-10-14	2011-11-25	11738	70020
184.14	tel.mail.ru	2011-10-14	2011-11-25	8994	65540
184.14	e.	2011-10-15	2011-11-25	307	616
184.14	e.mai	2011-10-14	2011-11-25	155	1101
184.14	e.mail.	2011-10-14	2011-11-25	119	705
184.14	mail.ru	2011-10-24	2011-11-23	110	367
184.14	e.m	2011-10-15	2011-11-25	107	400

Top 100 SSL clients of serve 184.14 (?)

Tip 1: Filter by country of client IP (e.g. enter nothing to avoid filtering or PK,IR,IQ to filter by multiple countries): GB,US,CA,NZ,AU

( ) Only show clients in these countries (•) Remove clients in these countries

[✓] Remove clients that also act as servers

Number of results returned: 100

Filter! RESET

Tip 2: Right click on a client or server IP to explore it further!

1 - 20 of 100 items 10 | 25 | 50 | 100 1 2 3 4 5

Client IP	Client country (conf)	Client company	First seen	Last seen	Count w/e 25th Nov	Count all time	Pairing status w/e 25th Nov	Pairing status all time
.212	ES(V)	Telefonica_de_Espana_SAU;rima-tde.net	2011-10-16	2011-11-19	1415	50136	Server -> Client only	Both directions
.139	ES(H)	R_Cable_y_Telecomunicaciones_Galicia_S.A.;mundo-r.	2011-10-24	2011-11-25	424	726	Client -> Server only	Client -> Server only
.111	DE(V)	Bertelsmann_ZI_GmbH;mediaways.net	2011-11-23	2011-11-23	417	417	Server -> Client only	Server -> Client only
.56	NO(V)	Telenor_Nextel_AS;telenor.net	2011-11-21	2011-11-24	403	403	Server -> Client only	Server -> Client only
.38	IE(V)	Vodafone_ISP;UNKNOWN	2011-11-23	2011-11-23	330	330	Both directions	Both directions
.114	DE(V)	Bertelsmann_ZI_GmbH;mediaways.net	2011-11-23	2011-11-23	329	329	Server -> Client only	Server -> Client only
.127	KR(M)	Korea_Telecor	2011-09-04	2011-11-25	325	2266	Both directions	Both directions
.250	-(-)	-	2011-11-18	2011-11-18	296	296	Both directions	Both directions
.152	EC(H)	Ecuadortelecom_S.A.;ecutel.net.ec	2011-11-10	2011-11-25	290	291	Both directions	Both directions
.186	IE(V)	Vodafone_ISP;UNKNOWN	2011-11-20	2011-11-20	196	196	Both directions	Both directions
.9	MY(H)	TMNET;holcim.net	2011-09-03	2011-11-24	189	383	Both directions	Both directions
.153	KR(M)	QRIXNET;UNKNOWN	2011-10-20	2011-11-25	181	198	Both directions	Both directions
.53	MY(H)	CORE_IP_DEVELOPMENT ;dancom.com.my	2011-11-19	2011-11-25	179	179	Both directions	Both directions
.121	IR(V)	Static-Pool-TP3;pol.ir	2011-11-21	2011-11-21	177	177	Client -> Server only	Client -> Server only
.41	IE(V)	UTV_PLC;utvinternet.net	2011-11-19	2011-11-20	167	167	Both directions	Both directions
.237	KR(M)	KRNIC;ktcu.or.kr	2011-09-03	2011-11-25	150	1007	Both directions	Both directions
.38	BR(M)	Comite_Gestor_da_Internet_no_Brasil;ampernet.com	2011-11-23	2011-11-25	145	145	Server -> Client only	Server -> Client only
.87	KR(H)	Korea_Telecom;postman.co.kr	2011-10-16	2011-11-25	143	161	Both directions	Both directions
.155	KR(H)	Korea_Telecom;kornet.net	2011-10-24	2011-11-24	138	583	Both directions	Both directions
.1	IE(V)	Vodafone_ISP;UNKNOWN	2011-11-18	2011-11-18	137	158	Client -> Server only	Both directions

Explore this client IP further!

Query by client IP

FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK ANT** - Tor events QFD

Prototype owner: [redacted] ICTR-NE

Query FLYING PIG

IP / network / certificate field [redacted].127

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)]

Run Query!

Client IP-specific panels
General IP info ☑
SSL Servers visited ☑

Certificate field search: %mail.ru | Server IP: [redacted]184.14 | **Client IP:** [redacted].127

General IP info for client IP [redacted].127

Geolocation (?):
Country: **KR** (**M**)
City: **SEOUL** (**L**)

WHOIS info (?):
Network: [redacted].**0/20**. Network type: No results.
Company: **Korea Telecom**. Domain: **groupon.kr**.

AS info (?):
Advertised by AS: **4766**. Found within network: [redacted].**0.0/13**.
AS name: **KIXS-AS-KR Korea Telecom**.

DNS (?): No results

Tor node (?):

Top 100 SSL servers visited by [redacted].127 **(?):**

Tip 1: Filter by country of server IP (e.g. enter PK to filter by Pakistan only or PK,IR,IQ to filter by multiple countries): | Only show servers in these countries | Remove servers in these countries | RESET

Tip 2: Right click on a client or server IP to explore it further!

1 - 8 of 8 items | 10 | 25 | 50 | 100 | 1

Client IP	Server IP	Server country (conf)	Server company info (from GEOFUSION export)	First seen	Last seen	Count w/e 25th Nov	Count all time	Pairing status w/e 25th Nov	Pairing status all time
[redacted].127	[redacted]184.14	RU(M)	Mail.Ru;mail.ru	04-09-11 02:23:55	25-11-11 13:47:52	325	2266	Both directions	Both directions
[redacted].127	[redacted]184.17	RU(M)	Mail.Ru;mail.ru	04-09-11 02:13:48	25-11-11 13:23:36	299	2207	Both directions	Both directions
[redacted].127	[redacted]184.16	RU(M)	Mail.Ru;mail.ru	03-09-11 05:18:48	25-11-11 10:15:23	269	2240	Both directions	Both directions
[redacted].127	[redacted]184.15	RU(M)	Mail.Ru;mail.ru	03-09-11 03:20:27	25-11-11 11:49:27	213	2354	Both directions	Both directions
[redacted].127	[redacted]2.131.207	DE(M)	BBBK91667;rapidshare.com	14-11-11 02:39:15	14-11-11 02:39:15	0	1	No traffic w/e 25th Nov	Client -> Server only
[redacted].127	[redacted]213.87	NL(L)	Mozilla_Corporati[redacted]	09-10-11 05:07:48	06-11-11 22:38:50	0	8	No traffic w/e 25th Nov	Server -> Client only
[redacted].127	[redacted]181.127	RU(M)	Mail.Ru;mail.ru	16-10-11 19:05:16	13-11-11 21:31:31	0	13	No traffic w/e 25th Nov	Client -> Server only
[redacted].127	[redacted]191.213	RU(M)	Mail.Ru;mail.ru	24-10-11 17:53:21	24-10-11 17:53:21	0	1	No traffic w/e 25th Nov	Client -> Server only

Explore this server IP further!

Query by network range

FLYING PIG
TLS/SSL KNOWLEDGE BASE

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK ANT** - Tor events QFD

Prototype owner: [redacted] ICTR-NE

Query FLYING PIG

IP / network / certificate field [redacted].0/24

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)]

Run Query!

Network-specific panels

- General network info ☑
- SSL Clients present in network ☑
- SSL Servers present in network ☑
- HTTP requests to IPs in network ☑

Certificate field search: %mail.ru | Server IP: [redacted]184.14 | Client IP: [redacted].127 | **Network:** [redacted].0/24

General network info for [redacted].0/24

Geolocation (?):
Country: **KR** (M)
City: **SEOUL** (L)

WHOIS info (?):
Network: No results. Network type: No results.
Company: No results. Domain: No results.

AS info (?):
Advertised by AS: No results. Found within network: No results.
AS name: No results.

DNS (?):
No results

SSL clients in network [redacted].0/24: (?):

Tip 1: Right click on a client IP to explore it further!

1 - 20 of 57 items | 10 | 25 | 50 | 100 | 1 2 3

Client IP	Client company info (from GEOFUSION export)	First seen	Last seen	Total SSL traffic w/e 25th Nov	Total SSL traffic all time	Num. unique servers contacted w/e 25th Nov	Num. unique servers contacted all time
[redacted].9	Korea_Telecom;mailplug.co.kr	2011-09-04	2011-09-04	0	1	0	1
[redacted].23	Korea_Telecom;mailplug.co.kr	2011-10-26	2011-11-23	1	7	1	3
[redacted].29	Korea_Telecom	2011-10-22	2011-10-22	0	1	0	1
[redacted].32	Korea_Telecom	2011-11-16	2011-11-18	1	2	1	2
[redacted].36	Korea_Telecom;mailplug.co.kr	2011-11-19	2011-11-22	7	7	1	1
[redacted].38	Korea_Telecom;mailplug.co.kr	2011-10-14	2011-11-16	0	21	0	5
[redacted].41	Korea_Telecom;mailplug.co.kr	2011-10-24	2011-10-26	0	2	0	2
[redacted].42	Korea_Telecom;mailplug.co.kr	2011-10-21	2011-10-21	0	1	0	1
[redacted].57	Korea_Telecom;mailplug.co.kr	2011-11-09	2011-11-11	0	3	0	2
[redacted].62	Korea_Telecom;mailplug.co.kr	2011-09-09	2011-09-09	0	1	0	1
[redacted].64	Korea_Telecom;mailplug.co.kr	2011-10-12	2011-10-12	0	1	0	1
[redacted].70	Korea_Telecom;mailplug.co.kr	2011-10-08	2011-10-31	0	18	0	5
[redacted].76	Korea_Telecom;mailplug.co.kr	2011-10-14	2011-11-07	0	14	0	1
[redacted].82	Korea_Telecom;mailplug.co.kr	2011-11-15	2011-11-15	0	2	0	1
[redacted].86	Korea_Telecom;mailplug.co.kr	2011-11-18	2011-11-18	1	1	1	1
[redacted].87	Korea_Telecom;mailplug.co.kr	2011-11-12	2011-11-12	0	1	0	1
[redacted].93	Korea_Telecom;mailplug.co.kr	2011-11-04	2011-11-04	0	2	0	1
[redacted].99	Korea_Telecom;mailplug.co.kr	2011-10-25	2011-11-21	3	12	2	5
[redacted].103	Korea_Telecom;mailplug.co.kr	2011-09-05	2011-09-05	0	1	0	1
[redacted].105	Korea_Telecom;mailplug.co.kr	2011-11-03	2011-11-03	0	1	0	1

Explore this client IP further!

All SSL servers in network [redacted].0/24: (?)

Tip 1: Right click on a server IP to explore it further!

1 - 3 of 3 items | 10 | 25 | 50 | 100 | 1

Server IP	Server company info (from GEOFUSION export)	Last week seen:	% Paired clients that week	Num. unique clients that week	Num. unique clients all time
[redacted].18	Korea_Telecom;mailplug.co.kr	2011-11-11	0.0	1	1
[redacted].205	test	2011-12-09	0.0	1	1

HTTP requests to IPs in network [redacted].0/24 (top 100) (?)

Tip 1: Right click on a server IP to explore it as an SSL server!

1 - 1 of 1 items | 10 | 25 | 50 | 100 | 1

Server IP	Host name requested	First seen	Last seen	Count last week	Count all time
[redacted].40	[redacted].40	2011-10-30	2011-10-30	0	5

Cyber applications

NETWORK EXPLOITATION

- **Diginotar certificate authority compromise :**
  - **Private keys of legitimate certificate authority, Diginotar, stolen by hacker.**
  - **FLYING PIG was used to identify a FIS using them to launch a MITM against their own citizens.**

How the attack was done:

FLYING PIG screenshot showing fake certificate:

3082043030820392	2011-09-16 20:54:29	2011-10-20 17:14:05	0	3154	2011-09-05 06:05:49	2012-09-05 06:15:49	*.google.com	us	google inc	zscaler	us	www.zscaler.com	Y
3082052A30820492	2011-10-11 16:56:45	2011-11-25 15:41:29	5	1214	2011-09-20 06:07:12	2012-09-20 06:17:12	*.google.com			google internet authority			N
308204523082038	2011-11-11 02:30:27	2011-11-25 06:20:50	26	572	2011-11-02 21:08:36	2012-11-02 21:18:36	*.google.com	us	google inc	zscaler	us	www.zscaler.com	Y
308202DA30820242	2011-11-01 01:23:06	2011-11-25 17:48:58	71	547	2010-09-02 07:56:28	2011-09-02 08:06:28	*.google.com	us	google inc	sfibluecoat.sficorp.com	us	is	N
3082043030820392	2011-08-25 13:03:12	2011-10-13 07:51:24	0	467	2011-08-12 03:49:02	2012-08-12 03:59:02	*.google.com	us	google inc	zscaler	us	www.zscaler.com	Y
3082052830820412	2011-08-19 21:04:42	2011-08-26 19:51:50	0	441	2011-07-10 19:06:30	2013-07-09 19:06:30	*.google.com	us	google inc	diginotar public ca 2025	nl	diginotar	N
308204AA30820392	2011-11-08 09:35:22	2011-11-25 15:00:37	173	440	2011-09-20 06:07:12	2012-09-20 06:17:12	*.google.com	us	google inc	lorealinternetbrowsing	fr	loreal	N
308204643082030	2011-11-17	2011-11-25	436	438	2011-11-10	2012-11-10	*.google.com	us	google inc	zscaler	us	www.zscaler.com	Y

Cyber applications

NETWORK EXPLOITATION

- **Other Cyber applications:**
  - **Multiple examples of FIS data exfiltration using SSL have been found using FLYING PIG.**
  - **In particular, certificates related to LEGION JADE, LEGION RUBY, and MAKERSMARK activity were found on FLYING PIG using known signatures**
  - **These were then used to find previously unknown servers involved in exfiltration from US companies.**
  - **FLYING PIG has also been used to identify events involving a mail server used by Russian Intelligence.**

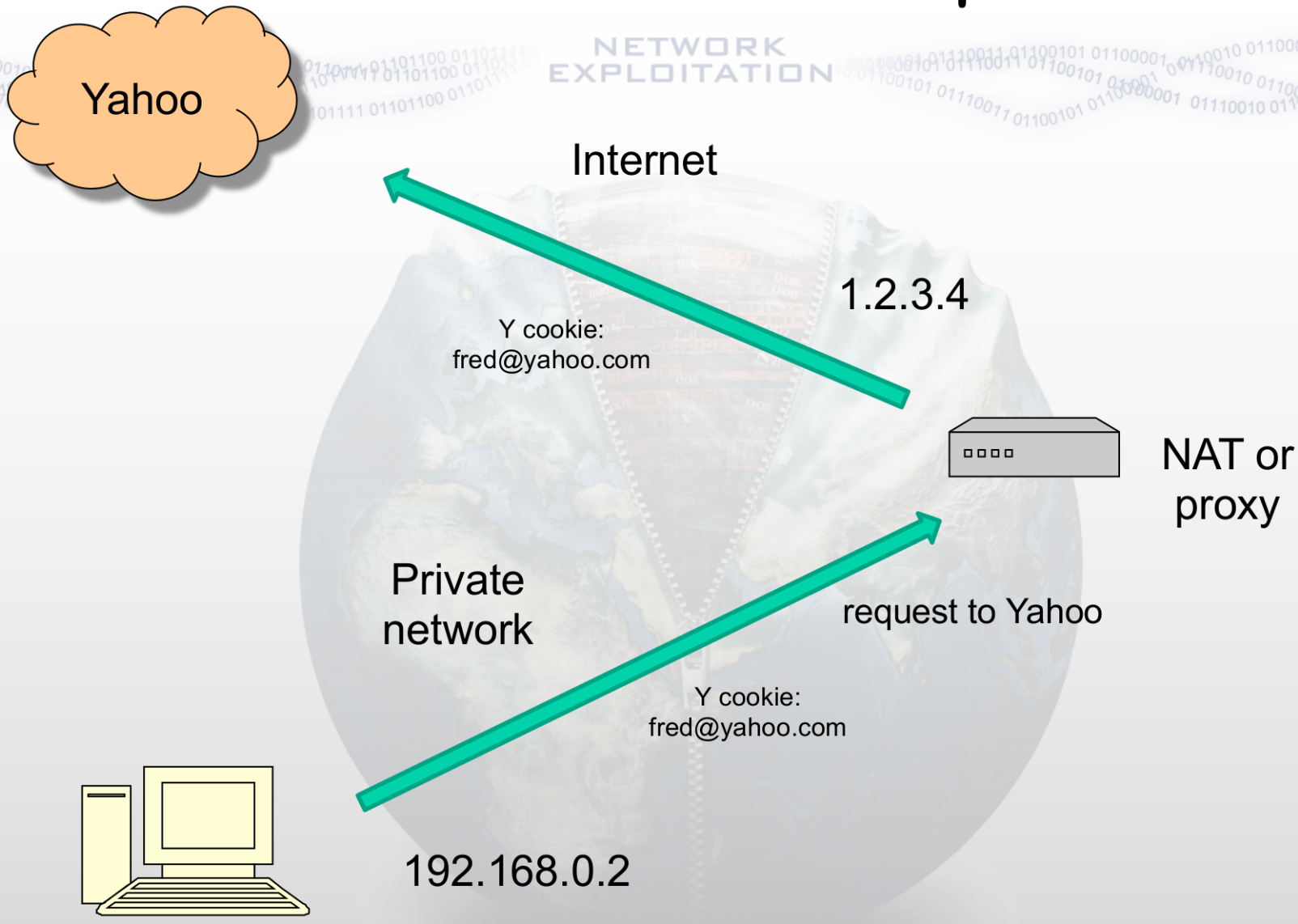
Identification of malicious TLS/SSL

- Can identify malicious TLS/SSL using signatures if known
- However this approach generally does not allow discovery of new threats
- Alternative is to use "behavioural" features to automatically identify potentially malicious traffic
- Features currently being investigated include:
  - Certificates with same subject but different issuers – may be indicative of Diginotar-style attack
  - Beaconing in TLS/SSL (indicative of botnets/FIS implants)
  - Number of client cipher suites offered
  - Repeated identical random challenges

HUSH PUPPY – motivation

- Much private network traffic seen but previously discarded
- If traffic could be attributed, potential high value – close access
- HUSH PUPPY is a bulk private network identification Cloud analytic
- Basic idea is to look for the same TDI being seen coming from a private address and then from a public address within a short time
- The private traffic can then be attributed to the owner of the public address
- Works for SSE & COMSAT

HUSH PUPPY – example



Other HUSH PUPPY datasets

- **HUSH PUPPY also makes use of Yahoo T-cookies to do correlations**
- **A T-cookie contains the IP address of the client as Yahoo sees it**
- **Hence a T cookie coming from a private IP can give the public IP of the NAT or proxy**
- **In addition, HUSH PUPPY uses the following data to help verify results**
  - Kerberos & Lotus Notes: Domains, organisations, departments, countries, machine names, user names
  - HTTP: Heuristic detection of Intranet web servers
  - SSL: Issuers, subjects, countries
  - SMTP: From & to domains

Results – what do we find?

NETWORK EXPLOITATION

- Foreign government networks
- Airlines
- Energy companies
- Financial organisations

- In cases of good collection, 50-80% of collected private network traffic has been attributed

- Some false positives can arise if few events correlated, due to factors such as TDIs not being completely unique and public internet proxies giving misleading public IP results

- Results can frequently be verified using Kerberos etc data

Examples of operational successes

NETWORK EXPLOITATION

- A large private network related to the Afghan government was identified, with ~800,000 events correlated.
- Examination of the case notations suggested it belonged to the Afghan MOD
  - A Kerberos domain mod.local
  - HTTP servers *.mod.local & mail
  - SSL certificates with the subject “Ministry of Defense” and the geo “AF”
- Results confirmed by analysis of content on XKEYSCORE
- A VSAT private network belonging to a Ministry of Foreign Affairs was identified
- NOSEY PARKER events were correlated with SSE

Contacts

NETWORK EXPLOITATION

- FLYING PIG – [redacted]
- HUSH PUPPY – [redacted]