DDoS: Current and Evolving Frameworks

Presented by: David Fernandez and Terrence Gareau

NANOG 58
Global Statistics: Total Attack Types (Q1 2013)

Infrastructure (Layer 3 & 4): 76.54%
- DNS: 6.97%
- ICMP: 15.53%
- TCP Fragment: 0.00%
- SYN PUSH: 0.63%
- IGMP: 0.00%
- UDP Fragment: 7.77%
- ACK: 1.74%
- RIP: 0.00%
- FIN PUSH: 0.32%
- RESET: 1.43%

Application (Layer 7): 23.46%
- SSL GET: 1.43%
- SSL POST: 0.32%
- PUSH: 0.95%
- HTTP GET: 19.33%
- HTTP POST: 1.43%
- NTP: 0.00%

Global Stats:
- Total ASack Types (Q1 2013)
Global Statistics: Q1 2013 Bandwidth Attack Rates
Global Statistics: Q1 2013 Packets Per Second Rates

Bar chart showing the distribution of Q1 2013 average Mpps.
Top Ten Source Countries (Q1 2013)

- China: 40.68%
- United States: 21.88%
- Germany: 10.59%
- Iran: 5.51%
- India: 5.01%
- Brazil: 4.73%
- France: 3.50%
- Egypt: 3.30%
- Vietnam: 2.61%
- Canada: 2.19%
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.
Dirt Jumper V3: Criminal 101

http://hack-stars.ru/?p=4754
BroDoS Q1 2013: Enterprise Organization

Malicious Sourced Traffic Distribution
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
Bother 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

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

/*
 * 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> //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> <packetsize> <port> <delay> //udpflood attack
 * .raw <cmd> // raw IRC command
 * .rmdnick // change nickname
 * .pjson <host> //port scan
 * .safe // test safe_mode (dvl)
 * .inbox <to> // test inbox (dvl)
 * .conback <ip> // connect back (dvl)
 * .uname // return shell's uname using a php function (dvl)
 */
Booster Scripts: getDeLiRiUm asp

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

```csharp
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: \r\nConnection: Keep-Alive\r\n";

    while (loop <= times)
    {
        try
        {
            IPEndPoint endPoint = new IPEndPoint(Addr[0], port);
            Socket sock = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
            sock.Connect(endPoint);

            if (sock.Connected)
            {
                Encoding.ASCII = Encoding.ASCII;
                byte[] bytes = ASCII.GetBytes(data);
                sock.Send(bytes, length, 0);
            }
        }
        catch {}
        Response.Write("Attacker executed successfully. <br>");
        loop++;
    }
}
```
DrDoS: DNS/Amplification Reflection Overview

- DNS reflection campaigns are on the rise = < 200% over the last year
- Utilizes spoofed IP requests against legitimate DNS servers
- 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

Spoofed query (as primary target) sent to Victim Name Server

Attacker

Primary Target

Victim Name Server

Victim Name Server responds to Primary Target. RFC parameters are modified to amplify response and cause degradation of service.
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.,
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
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

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

[^_^]

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

Nope.
DNS Reflection Campaign: Reflector Graphs

**69.93.177.228 bps**
- Incoming Avg.: 5.83Mbps
- Outgoing Avg.: 5.95Mbps
- Outgoing Max: 11.87Mbps
- Incoming Max: 12.14Mbps

**74.122.121.230 bps**
- Incoming Avg.: 11.21Mbps
- Outgoing Avg.: 10.94Mbps
- Outgoing Max: 104.13Mbps
- Incoming Max: 100.34Mbps