Service Provider Experienced Threats

- 77% DDoS attacks towards your customers
- 49% DDoS attacks towards your services
- 49% Infrastructure outages
- 47% DDoS attacks towards your infrastructure
- 39% Bandwidth saturation
- 4% Other

Figure 7 Source: Arbor Networks, Inc.
What’s the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teenybopper you just pwned has you beat with the tiny botnet he leased with his allowance money.
Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen  February 4, 2009 | 12:13 pm  Categories: Cybarmageddon!

“Do you get annoyed all the time because of skids on xBox Live? Do you want to take down your competitors’ servers or Web site?,” reads the site’s ad, apparently recorded by this paid actor at Fiverr.com. “Well, boy, do we have the product for you! Now, with asylumstresser, you can take your enemies offline for just 30 cents for a 10 minute time period. Sounds awesome, right? Well, it gets even better: For only $18 per month, you can have an unlimited number of attacks with an increased boot time. We also offer Skype and tiny chat IP resolvers.”

What’s the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.
DDOS EM’
When In Doubt Knock Em’ Out!

Features

Resolvers
- Skype
- Steam
- Cloudflare

IP Tools
- Geolocation
- IP Logger
- Host to IP

MAX BOOT TIME OF
3600
UDP, SSYN, RUDY, UDP-LAG, ARME, GET, POST
Extortion via DDoS on the rise

By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05

Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.

Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving $4 million from firms that they threatened with cyberattacks.

The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for $10,000, was attacked and brought offline—which reportedly cost it more than $200,000 a day in lost business.
This link runs a slow SQL query on the RIAA's server. Don't click it; that would be wrong. (tinyurl.com)
814 points posted 8 days ago by keyboard_user 211 comments

Clicking this link loads 120,000 copies of the RIAA's captcha. Clicking would be wrong, don't do it. (antisocial.propagation.net)
452 points posted 4 days ago by mridlen 292 comments
‘Operation Payback’ Attacks Fell Visa.com
By ROBERT MACKEY

TARGET: WWW.VISA.COM :: FIRE FIRE FIRE FIRE!!! WEAPONS http://bit.ly/e6iR3X :::: SET YOUR LOIC TO irc.anonops.net :::: #DDOS #PAYBACK #WIKILEAKS

A message posted on Twitter by a group of Internet activists announcing the start of an attack on Visa’s Web site, in retaliation for the company’s actions against WikiLeaks.

Last Updated | 6:54 p.m. A group of Internet activists took credit for crashing the Visa.com Web site on Wednesday afternoon, hours after they launched a similar attack on MasterCard. The cyber attacks, by activists who call themselves Anonymous, are aimed at punishing companies that have acted to stop the flow of donations to WikiLeaks in recent days.

The group explained that its distributed denial of service attacks — in which they essentially flood Web sites site with traffic to slow them down or knock them offline — were part of a broader effort called Operation Payback, which
Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey†

The Berkman Center for Internet & Society at Harvard University

December 2010

9. In the past year, has your site been subjected to a denial of service attack, meaning an attacker prevented or attempted to prevent access to your site altogether?

<table>
<thead>
<tr>
<th>#</th>
<th>Answer</th>
<th>Bar</th>
<th>Response</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>yes</td>
<td></td>
<td>21</td>
<td>62%</td>
</tr>
<tr>
<td>2</td>
<td>no</td>
<td></td>
<td>8</td>
<td>24%</td>
</tr>
<tr>
<td>3</td>
<td>not sure</td>
<td></td>
<td>5</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td>34</td>
<td></td>
</tr>
</tbody>
</table>
Just as Internet users learn that clicking on a link in an e-mail purporting to come from their bank is a bad idea, phishers seem to be developing a new tactic -- launch a DDoS attack on the Web site of the company whose customers they are targeting and then send e-mails "explaining" the outage and offering an "alternative" URL.
The popular British anti-fraud site Bobbear.co.uk is currently under a DDoS attack (distributed denial of service attack), originally launched last Wednesday, and is continuing to hit the site with 3/4 million hits daily from hundreds of thousands of malware infected hosts mostly based in Asia and Eastern Europe, according to the site’s owner. Targeted DDoS attacks against anti-fraud and volunteer cybercrime fighting communities clearly indicate the impact these communities have on the revenue stream of scammers, and with Bobbear attracting such a high profile underground attention, the site is indeed doing a very good job.
BobBear, an anti-fraud site based in the UK is still (*first reported here at Infosecurity.US on November 19th*) under constant distributed denial of service attack (DDoS), reports The Shadowserver Foundation. More information regarding BobBear, and the unfortunate attacks they are being subjected to appears after the break.
Beyrouti, Babbo and Vitello worked with hackers who breached brokerage accounts at E-Trade and TD Ameritrade. The hackers then executed fraudulent sales of securities and transferred the proceeds from the sale to the mules’ accounts. The receiving accounts were set up in the names of shell companies and linked to the hacked accounts.

Meanwhile, the victims’ phones received a barrage of calls to prevent the brokerage firms from contacting them to confirm the legitimacy of the transactions. When the victims answered their phone, they would hear silence or a recorded message. About $1.2 million was transferred to shell accounts opened by the suspects, who then transferred the money to other accounts in Asia or withdraw the money from ATMs in the New York area.
Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

August 11th, 2008

Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

Categories: Black Hat, Botnets, Denial of Service (DoS), Governments, Hackers...
Tags: Security, Cyber Warfare, DDoS, Georgia, South Ossetia...

In the wake of the Russian-Georgian conflict, a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia’s Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S., with Georgia’s Ministry of Foreign Affairs undertaking a desperate step in order to disseminate real-time
Kids responsible for Estonia attack

The distributed denial of service attack that took down Estonia was run by a bunch of kids, it has emerged.

Two years ago, the former Soviet satellite found its banking and government websites paralysed for several weeks by a distributed denial-of-service (DDoS) attack.

The incident prompted a massive reorganisation and upgrade of network security and early warning systems among Nato members, and Nato even set up a cyber-security research house in Estonia.

At the time Russia was suspected of orchestrating the attack, but Moscow always denied it, and indeed Estonian officials never accused the Kremlin directly.

Yesterday, Konstantin Goloskokov (22) claimed he and some friends set up the attack to protest the removal of a Red Army monument from a downtown site in Estonia’s capital Tallinn. The move had earlier led to rioting by pro-Soviet protesters.

Goloskokov told Reuters the attack was an act of civil disobedience, and, therefore, completely legal. "I was not involved in any cyber-attack," he said.
Row over Korean election DDoS attack heats up
Ruling party staffer accused of disrupting Seoul mayoral by-election

By John Leyden • Get more from this author

Posted in Security, 7th December 2011 09:23 GMT
Free whitepaper – IBM System Networking RackSwitch G8124

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Gong continues to protest his innocence, a factor that has led opposition politicians to speculate that he is covering up for higher-ranking officials who ordered the attack.

Democratic Party politician Baek Won-woo told The HankYoreh: “We need to determine quickly and precisely whether there was someone up the line who ordered the attack, and whether there was compensation.” ©
GREAT Firewall
INSPECTION
Banned content?
Yes: INJECT RST
No: REROUTED

Router

Target Traffic

Global Internet

Chinese Net

GREAT Cannon

ATTACK
Attack criteria met?
Yes: INJECT .js
No:
Figure 25 Source: Arbor Networks, Inc.
DDoS Attack Frequency

- 72% 1–10
- 12% 11–20
- 9% 21–50
- 2% 51–100
- 5% More than 100

Figure 97 Source: Arbor Networks, Inc.
DDoS Attack Frequency

Figure 97 Source: Arbor Networks, Inc.

- 72% 1–10 (Per month)
- 12% 11–20
- 9% 21–50
- 2% 51–100
- 5% More than 100

(2016 Report)
The clashes between Russia and Georgia over the region of South Ossetia have been shadowed by attacks on the Internet. As we noted in July, the Georgia presidential website fell victim to attack during a war of words. A number of DDoS attacks have

Raw statistics of the attack traffic paint a pretty intense picture. We can discern that the attacks would cause injury to almost any common website.

**Average peak bits per second per attack** 211.66 Mbps
**Largest attack, peak bits per second** 814.33 Mbps
**Average attack duration** 2 hours 15 minutes
**Longest attack duration** 6 hours
Size of Largest Reported DDoS Attack (Gbps)

Figure 14 Source: Arbor Networks, Inc.

2014 Report
Figure 14 Source: Arbor Networks, Inc.
Real-time traffic from the DDoS attack. AKAMAI
IPv6 DDoS Attacks

Figure 26 Source: Arbor Networks, Inc.
• “Approximately $250,000 USD/incident.”
• “$8,000 USD/incident.”
• “Approximately 1,000EUR/incident.”
• “Roughly $1M USD to $1.5M USD/incident.”
• “$300,000 USD/incident.”
• “$1M USD/incident.”
• “More than $100,000 USD/month.”
• “Net revenue-generator—we offer commercial DDoS mitigation services.”
<table>
<thead>
<tr>
<th>Packet sent</th>
<th>Response from victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP SYN (to open port)</td>
<td>TCP SYN/ACK</td>
</tr>
<tr>
<td>TCP SYN (to closed port)</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP ACK</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP DATA</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP RST</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP NULL</td>
<td>no response</td>
</tr>
<tr>
<td>ICMP ECHO Request</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>ICMP TS Request</td>
<td>ICMP Echo Reply</td>
</tr>
<tr>
<td>UDP pkt (to open port)</td>
<td>ICMP TS Reply</td>
</tr>
<tr>
<td>UDP pkt (to closed port)</td>
<td>protocol dependent</td>
</tr>
<tr>
<td>...</td>
<td>ICMP Port Unreach</td>
</tr>
</tbody>
</table>

Table 1: A sample of victim responses to typical attacks.
Figure 4: Cumulative distributions of estimated attack rates in packets per second.
<table>
<thead>
<tr>
<th>Kind</th>
<th>Trace-1</th>
<th>Trace-2</th>
<th>Trace-3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attacks</td>
<td>Packets (k)</td>
<td>Attacks</td>
</tr>
<tr>
<td>Other</td>
<td>1,917 (46)</td>
<td>19,118 (38)</td>
<td>1,985 (51)</td>
</tr>
<tr>
<td>In-Addr Arpa</td>
<td>1,230 (29)</td>
<td>16,716 (33)</td>
<td>1,105 (28)</td>
</tr>
<tr>
<td>Broadband</td>
<td>394 (9.4)</td>
<td>9,869 (19)</td>
<td>275 (7.1)</td>
</tr>
<tr>
<td>Dial-Up</td>
<td>239 (5.7)</td>
<td>956 (1.9)</td>
<td>163 (4.2)</td>
</tr>
<tr>
<td>IRC Server</td>
<td>110 (2.6)</td>
<td>461 (0.91)</td>
<td>88 (2.3)</td>
</tr>
<tr>
<td>Nameserver</td>
<td>124 (3.0)</td>
<td>453 (0.89)</td>
<td>84 (2.2)</td>
</tr>
<tr>
<td>Router</td>
<td>58 (1.4)</td>
<td>2,698 (5.3)</td>
<td>76 (2.0)</td>
</tr>
<tr>
<td>Web Server</td>
<td>54 (1.3)</td>
<td>393 (0.77)</td>
<td>64 (1.7)</td>
</tr>
<tr>
<td>Mail Server</td>
<td>38 (0.91)</td>
<td>156 (0.31)</td>
<td>35 (0.90)</td>
</tr>
<tr>
<td>Firewall</td>
<td>9 (0.22)</td>
<td>7 (0.01)</td>
<td>3 (0.08)</td>
</tr>
</tbody>
</table>

Table 6: Breakdown of victim hostnames.

The majority of attacks are not classified by this scheme, either because they are not matched by our criteria (shown by “other”), or more likely, because there was no valid reverse DNS mapping (shown by “In-Addr Arpa”).
the probability of a given host on the Internet receiving at least one unsolicited response from the victim is \( \frac{m}{2^{32}} \) during an attack of \( m \) packets.