Judge Francis Bruty called Zboralski "a computer genius with a lamentable morality."

"He seems a little childlike, a dreamer. He doesn't appear to be someone who will end up a courtroom fixture," assistant prosecutor Georges Dobrouchkess told Reuters.

Kugutsumen

- Slashdot, Should MMOG Be Confined?; “I can think of very few people in EVE Online I would physically harm - this guy is one of them”, Seleene
- Ath5k Kugutsumen / Zerochaos illegal channel patch
NKILL
the internet kill board
The internet kill board

- Kill board are used to display physical damage from blast, fire or fragmentation expressed as a percentage of the target damaged.

- In Iraq, an Army commander was reported to have a whiteboard posted at his headquarters that showed the numbers of Iraqi casualties and served to keep track of enemy kills. "Let the bodies hit the floor," read a phrase at the bottom of the board. Allegedly, four Soldiers wanted to be on the "kill board" and impress the commander. They killed three unarmed detainees (and covered it up) to accomplish it.
profiling

- Non-intrusive activity
- DNS queries
- web search
- public databases (internic, apnic, ripe, edgar...)
- Network topology mapping
- host and service identification
input

- domain name
- host name
- IP address, network or AS
- random words
output

- related dns records
- ip address, networks, AS, routing prefix
- services
- banners
- network of trust
bscan

- We used to scan the whole internet with bscan on a regular basis back.
- 7 years later Fyodor announced at Defcon: “Nmap can now be used to scan the entire Internet.”
- bscan was able to scan the entire internet 0.0.0.0 - 239.255.255.255 for a single port in a matter of hours
- A typical TCP port scan of the internet took 8-16 hours
Loadable modules for telnet, bind, http handshakes

- ./bscan -s 10.2.6.6 -L "mod_banner.so" -X 10.3.0.0/16
  scans for ftp-banners [first line only unless '-a' specified] from spoofed source
  address '10.2.6.6' in spreadmode

- bscan’s README: You can scan with up to 10.000+ hosts/second on a 100mbit
  connection without any problems [see PROBLEMS].
The problem

- You end up with a bunch of IP address, banners, etc.
- It’s hard to tell who uses a particular IP address
Roelof’s Maltego

- Domains -> SOA, NS, MX, IP4, AXFR, brute force, search
- IP4 -> Netblock, AS, PTR, Shared virtual hosts (domain tools)
- It doesn’t work well with IP address
The solution

- profile all public domains names in advance
  - ns records
  - mx records
  - a records for www, ftp, smtp...
  - cnames
- grab all banners
first try and success

- Limited to Indonesia, Brunei, Singapore and the Philippines
- scan all IP addresses for vulnerabilities
- get all vulnerable domains
- in 2001, only 10 thousand IP addresses served all of Indonesia :)
- ISSUE: “How do we get all .com domains?”
first try
How do we get all .com?
From: VeriSign Customer Service
Subject: Re: pending tld agreement, no news for 2 weeks [REF:3612923067]
Date: 19 August 2005 21:13:04 GMT+04:00
To: Anthony C. Zboralski
Reply-To: tldzone@verisign-grs.com

Dear Anthony,

Your username is azboralski and the password is [REDACTED]. The server is rz.verisign-grs.com.

Best Regards,

Bryant, Bonnie
Customer Service
VeriSign, Inc
www.verisign.com
1 703.925.6999
1 703.421.5828 Fax
2nd try

- We extend the original proof of concept to all .com, .net and .org domains.

<table>
<thead>
<tr>
<th>Size</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1k</td>
<td>arpa.zone.gz</td>
</tr>
<tr>
<td>1.6G</td>
<td>com.zone.gz</td>
</tr>
<tr>
<td>226M</td>
<td>net.zone.gz</td>
</tr>
<tr>
<td>112M</td>
<td>org.zone.gz</td>
</tr>
<tr>
<td>25k</td>
<td>root.zone.gz</td>
</tr>
</tbody>
</table>
2nd try

- We extend the original proof of concept to all .com, .net and .org domains.

  4.1k  arpa.zone.gz
  1.6G  com.zone.gz
  226M  net.zone.gz
  112M  org.zone.gz
  25k   root.zone.gz
2nd try: scalability issues

- 102,359,087 domains
- 233,191,505 records just for NS and A glue records
- expands to 500 million records
- only 2 million name servers

- 52 arpa.data
- 187,029,891 com.data
- 28,706,090 net.data
- 17,452,806 org.data
- 2,666 root.data
- 233,191,505 total
2nd try scalability issues

- IO limits... 100 seek per second per hard disk
- tried mysql, berkeley db, postgres, posgres with patricia tri indexes...
- reverse engineering big tables
- hadoop
- budget issues...
google app engine

- 10,000 invites to the first beta and I missed it
- Lucky I had some friends

From: Tony Watson <watson@google.com>
Subject: Re: Google AppEngine
Date: 9 April 2008 10:04:47 GMT+04:00
To: Anthony C. Zboralski

You think just because I work at Google I can get special favors for you?

Well, your right. :)

Invite should be in your inbox now. Have fun and be sure to let me know what you think.

--
Tony
3rd try: app engine

- At first there were too many limitations
- The datastore is not a SQL database
- You can still follow the relational model
- google services (google accounts, memcache, google docs,
- Django with App Engine Patch
- It scales really well
3rd try: app engine
3rd try: app engine

The following symbols signify the most severe issue (if any) encountered during that day. Click a symbol in the table above to view a day's performance graphs.

- ✔️ No issues or minor performance issues
- 🔄 Investigating
- 🚨 Service disruption
- 🧟 Unknown

<table>
<thead>
<tr>
<th>Current Availability</th>
<th>Uptime (last 7 days)</th>
<th>Read latency (today)</th>
<th>Write latency (today)</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Datastore</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Images</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Mail</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Memcache</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Serving</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Urllib</td>
<td>🚨</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Users</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
3rd try: app engine
TODO

- iphone interface
- distributed scanner using boinc client
- DNS fingerprinting... version.bind is not popular
- geoip / google maps
- API to integrate with other tools (e.g. kismet)
- Internet simulator
- link to other databases (zone h, etc...)
thank you

- e-mail z@nkill.com for beta access
- Q/A?