CYBER-DOME: DEFENDING A DNS ENVIRONMENT

ISCOC .IL
WORKING FOR AN OPEN, NEUTRAL, SECURE AND GLOBAL INTERNET

Tuesday, October 14, 2014
Let’s talk about the Internet

• The Internet has become the foundation of the 21st century way of life

• Countries today are investing huge budgets to promote and secure technology

"Technology is moving so rapidly that… in the future, we anticipate that the cyber threat will pose the number one threat to our country."

- FBI Director, March 2012
Challenges and effects

- **Security**: worms, spam fraud, phishing, DDOS, etc.
- **Routing and Addressing**: size of routing tables, address space, etc.
- **Access**: infrastructure, content, services, etc.

---

Israel Internet Association ISOC-IL

---

ICANN - NO. 30, 30 DECEMBER 2014
LO S ANGELES
A few numbers…

• More than 150,000 cyber attacks are recorded on a regular day in Israel
• There is a 40% annual increase in successful data breaches
• Phishing, Defacement and dDdos - the most common attacks
• During last summer’s military operation against Hamas - an increase of 1000% in the number of cyber attacks
• Targeted attacks were carried out during a period of two weeks
How many hits does a search for the term 'Hacker' in Google generate? **About 17,200,000**
The advise we got....

- Be prepared:
  - carry out analyses
  - deploy appropriate equipment
    - purchase special equipment and prepare tools for
      - intrusion detection,
      - data-mining,
      - blacklist management and exchange,
      - filtering,
      - Logging
  - configure the equipment properly
  - reserve some resources for any case,
- Have trained staff (education)
- Simulate attacks beforehand
How cyber attacks affected our lives

Hamas attacked Israel’s Internet during war, PM charges

Netanyahu blames Iran for backing cyber-attacks; speaks out against intelligence unit objectors

Hackers step up cyber attacks on Israel to protest Gaza operation

NetVision customers hit by foreign hackers; Anonymous threatens ‘day of solidarity and resistance’ in cyber attacks on Friday.

Michal Margalit
Published: 07.23.14, 18:02 / Israel Culture

Hackers from around the world particularly in Arab countries launched multiple cyber attacks on Israeli websites, the Shin Bet says, in protest of the IDF’s ongoing operation in Gaza.
Not just rockets

- Defacing web sites: Existing web pages or web servers are modified or replaced with new text or graphics, or content per the attacker’s choice is installed
More than 300 GB ...

dDoS attacks: Distributed Denial of Service attack, or DDoS, is an online service that is flooded with bogus traffic, trying to prevent honest users from using the service.
How did it work…

• Recruiting
  • Multiple agents (slaves, zombies) machines

• Exploiting
  • Utilize discovered vulnerability, exploit a bug of some specific protocol

• Infecting
  • Plant attack code
  • wide deployment

• Acting
  • Send attack packets via agents
July 11th, 2014 - “Israhell”

06/07/2014 - First Alerts
08/07/2014 – First Officials Meeting
11/07/2014 - Small attack with no consequences

July 12-19 – the “silent” week

- Take over of 2 TV channels
- Defacing of service web sites
- OpSaveGaza
July 21\textsuperscript{th}, 2014 - “OpGaza”, phase one

\textit{Shut down .il}

- Alerts of the attack: 09:30
- Blackhole: 10:30
- Proactive disconnect of intl. lines: 11:30
- Overload of the Internet infrastructure: 12:30
- Re-connect: 13:00
- Proactive disconnect of intl. lines: 15:00
- Re-connect: 15:10
- Status meeting: 16:00
- Stream of packets and Malformed packets
- 21\textsuperscript{st}. of July
- 22\textsuperscript{nd}. of July

\textit{July 21}\textsuperscript{th}, 2014 - “OpGaza”, phase one

\textit{Shut down .il}

- Alerts of the attack: 09:30
- Blackhole: 10:30
- Proactive disconnect of intl. lines: 11:30
- Overload of the Internet infrastructure: 12:30
- Re-connect: 13:00
- Proactive disconnect of intl. lines: 15:00
- Re-connect: 15:10
- Status meeting: 16:00
- Stream of packets and Malformed packets
- 21\textsuperscript{st}. of July
- 22\textsuperscript{nd}. of July
UDP Flood Attack

A connectionless protocol that does not require any connection setup procedure to transfer data.
What we did...

- We tried to relieve the impact of the attack while minimizing collateral damage to legitimate queries
- We imposed a rate limit on a stream that has been characterized as malicious
- We filtered our attack streams
- Traffic redirection and traffic analysis
- We isolated the IP unique addresses
- We connected to anti-dDos services
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06:50</td>
<td>dDos Attack to ISP</td>
</tr>
<tr>
<td>11:50</td>
<td>Direct attack on DNS servers .il</td>
</tr>
<tr>
<td>13:00</td>
<td>More than 300,000 .il websites down</td>
</tr>
<tr>
<td>14:00</td>
<td>3 biggest ISP’s are attacked at once</td>
</tr>
<tr>
<td></td>
<td>There is no access to the biggest hosting sites</td>
</tr>
<tr>
<td>16:00</td>
<td>ISP’s DNS servers are attacked</td>
</tr>
<tr>
<td>18:45, July 26th.</td>
<td>End of the attack</td>
</tr>
</tbody>
</table>
Lessons learned:

- Scan the infrastructure and Web resources
- Initiate network-level volumetric attack
- Test if Web Presence is impacted
- Maintain Flood – spoof all source IPs
- Initiate DNS reflective/amplified attacks
- Simultaneously launch as many types of attacks as possible
- Not relent or subside – they stand very firm in their resolve
- A combined attack that simply increases the chance of success!
Top Ten Tips

• Known malicious IP addresses - constantly update reputation intelligence
• Unwanted countries where you do not do business – current geolocation information
• Botnet infected machines and DDoS’ers – allow yet monitor all real users
• Application abusers and unwanted activities – enforce usage standards
• All unnecessary ports and protocols – deep packet inspect all allowed services
• Protocol anomalies and violations - enforce RFC & industry standards
• Advanced evasion techniques - manage fragmentation/segmentation policies
• Exploits designed for data exfiltration – stop focused attackers at the perimeter
• Brute-force password attempts – log and alert any suspicious activity
• Lack of information about the state of your perimeter – increase your visibility
Conclusion

• Add anti-dDos attacks software
• Susceptibility to attacks could be alleviated with better Internet Architectures
• Don’t leave all the decision making to the machines on either end of a connection
• Provide ‘intelligent’ support along the path
• Create “Hardened” networks
Questions?