Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

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

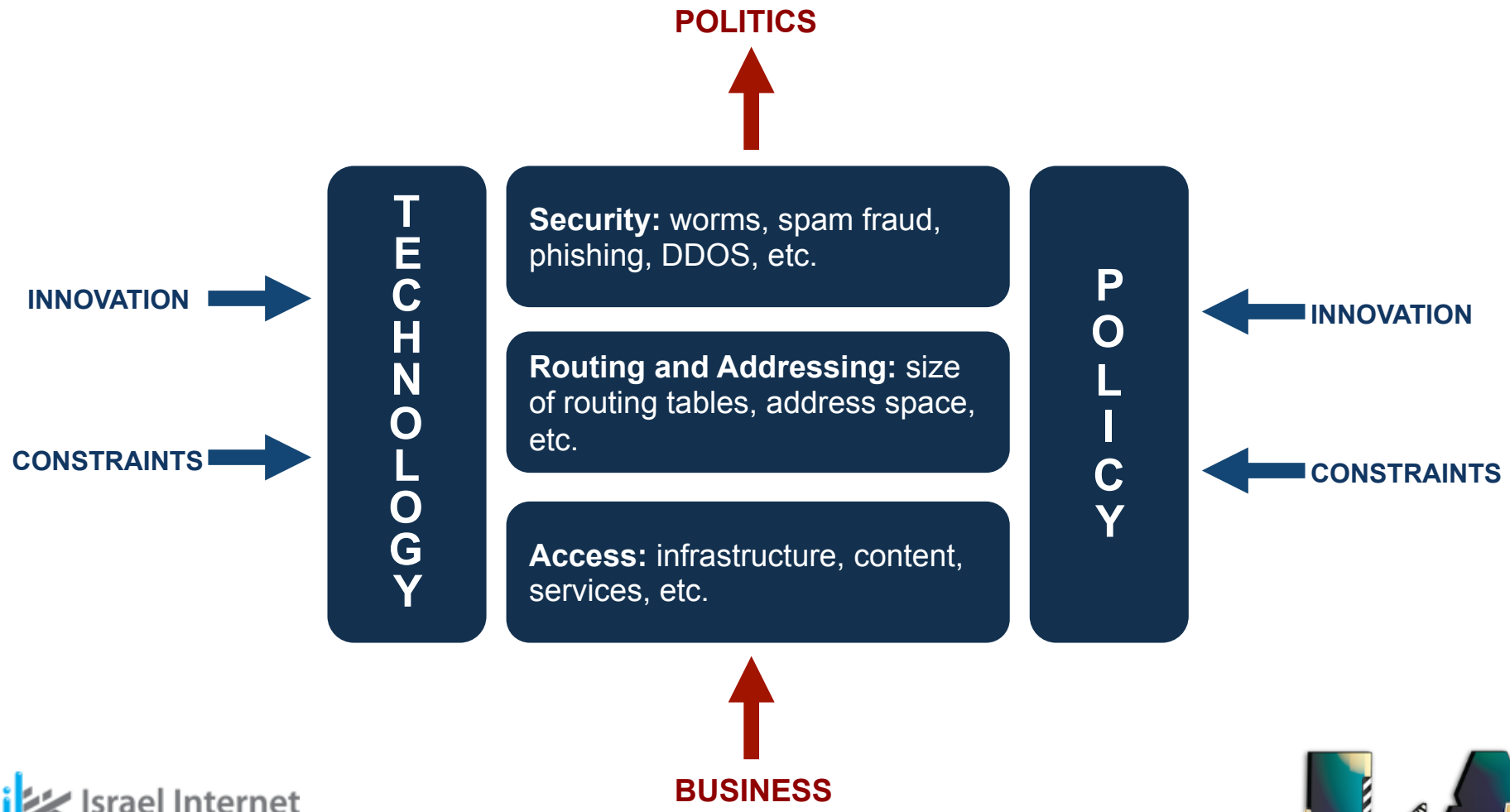
"Technology is moving so rapidly that… in the future, we anticipate that the cyber threat will pose the number one threat to our country."

- FBI Director, March 2012

Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

Challenges and effects



Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

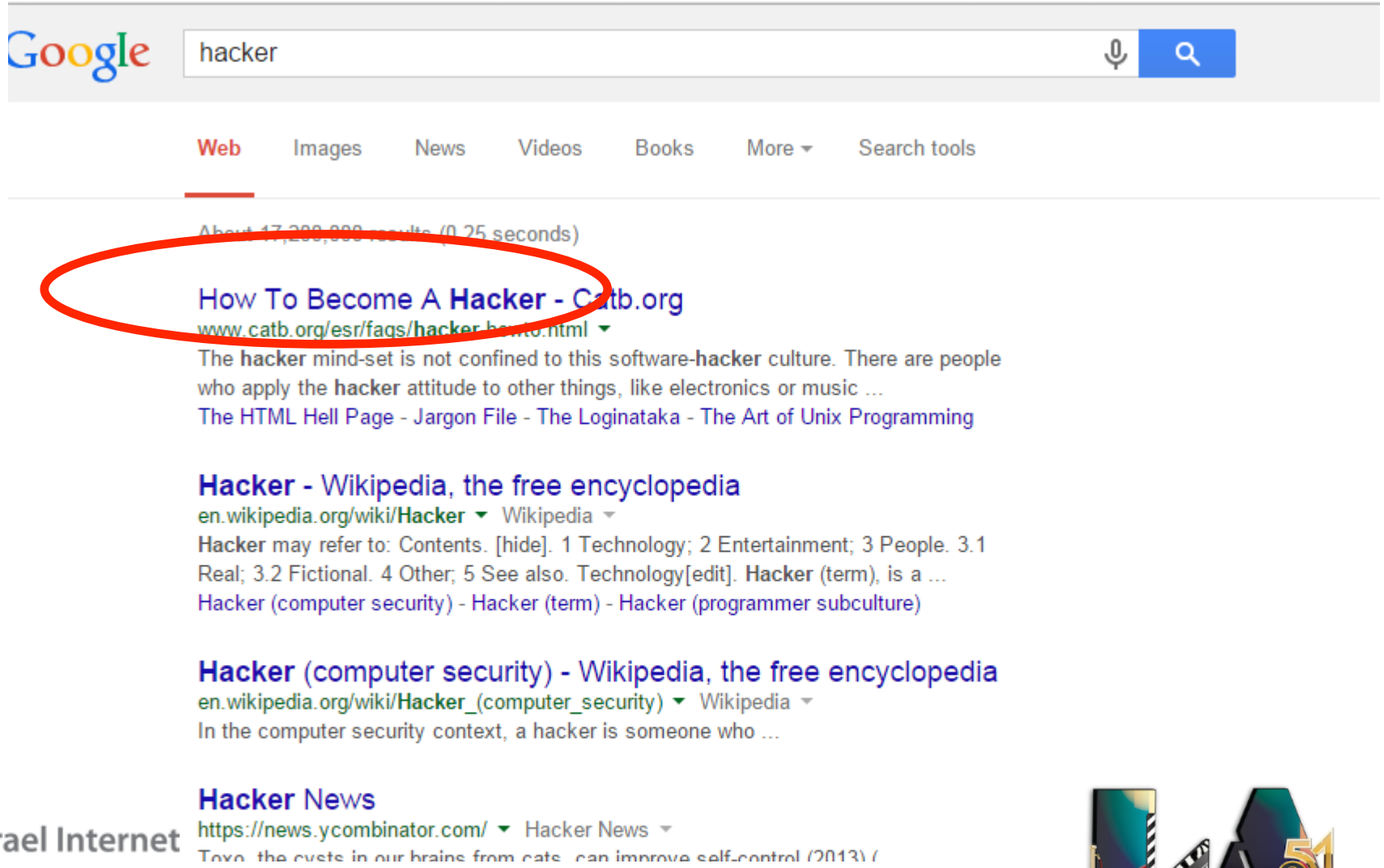
A few numbers…

- 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 dDos - 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

Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

How many hits does a search for the term **'Hacker'** in Google generate? **About 17,200,000**



Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

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

Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

How cyber attacks affected our lives

ARAB-ISRAELI CONFLICT

By YAAKOV LAPPIN | 08/17/2014 21:12

Iran attempted large-scale cyber-attack on Israel, senior security source says

- Israel, Iran wage cyber warfare in the battlefield of...
- Israel to intensify cyber security as end of Ramadan ...

Share on Facebook | Twitter | Google Plus

"This is not something we have seen before, both in terms of scope and the type of targets," source says; new, integrated military communications network was used in Gaza during the conflict.

Kate Vinton
Forbes Staff

FOLLOW

I write about the intersection between technology, security, and crime

full bio →

Comment Now

+ Follow Comments

Data Breach Bulletin: Anonymous Launches Cyber Attack on Israeli Websites

+ Comment Now + Follow Comments

Here's a roundup of the latest data breach news for the week of August 4, 2014:

CyberVor – If you follow security news, the announcement that a Russian cyber gang allegedly stole 1.2 billion passwords was arguably the biggest story of the week. Last Tuesday, the New York Times broke the news that Wisconsin-based Hold Security had discovered that a Russian hacker group they dubbed CyberVor had amassed a staggering 1.2 billion user names and passwords, believed to be the biggest data breach to date. Little detail was provided beyond that, leaving readers in the dark about who was affected and how exactly the hackers had collected such a large number of passwords. As the news of the heist broke, Hold Security made the oh-so generous offer to let site owners know if they were affected by CyberVor for a mere $120 per month, and then removed the page after Wall Street Journal reporter Danny Yadron tweeted a link to it (it's back now). Security blogger Brian Krebs wrote a post backing Hold Security but didn't originally disclose that he is on the company's advisory board. Buried under the speculation about who got hit (i.e., everyone) and criticism of Holden and its "offer" were some sober discussions about the role of passwords in society. Speaking of which, it's not a bad idea to change your passwords (it's really never a bad idea to update your passwords).

Hold Security

Home > Israel & the Region

Hamas attacked Israel's Internet during war, PM charges

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

BY STUART WINER AND RAPHAEL AHREN | September 14, 2014, 9:11 pm | 2

Recommend Share 65 Tweet 62 +1 0 Email Print Share

nber 2014. (photo credit: Kobi Gideon/GPO/Flash90)

Israel Internet Association ISOC-IL

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

Recommend 46 Tweet 11

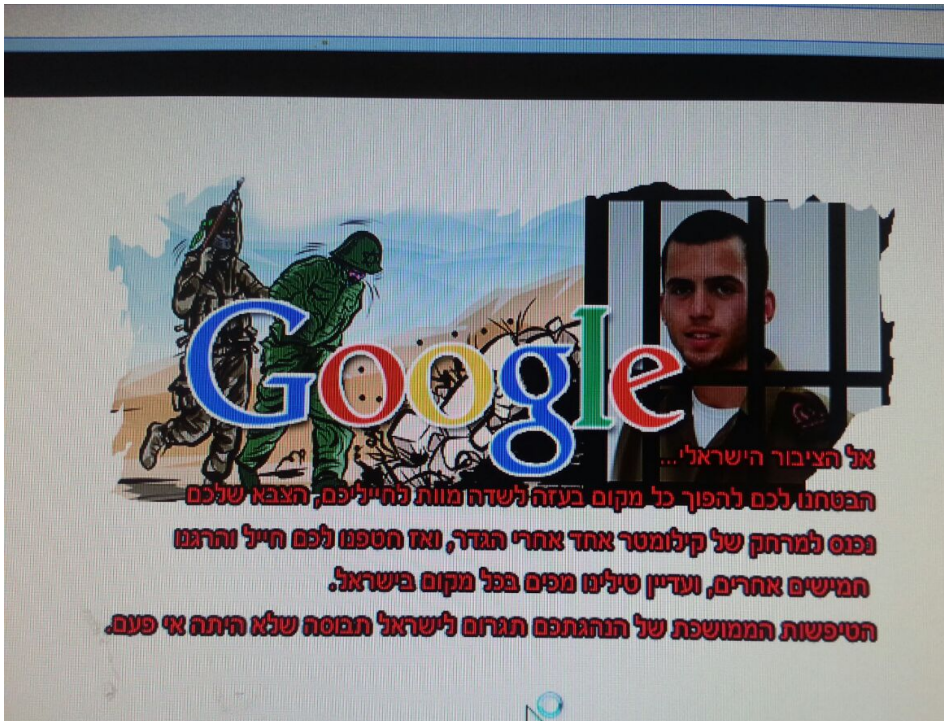
ynet news.com

Hackers from around the world,particularly in Arab launched mutiple cyber attacks on Israeli websites, the Shin Bet says, in protest of the IDF's ongoing operation in Gaza.

ICANN NO. 51 | 12-16 OCTOBER 2014
LOS ANGELES

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



Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

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

Israel Internet Association ISOC-IL

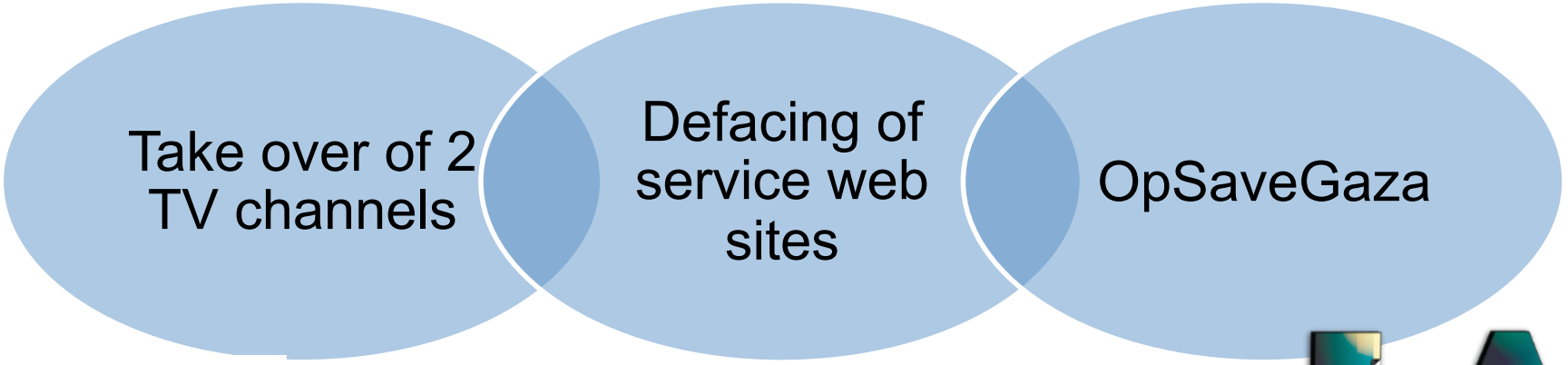
ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

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"

July 12-19 – the "silent" week

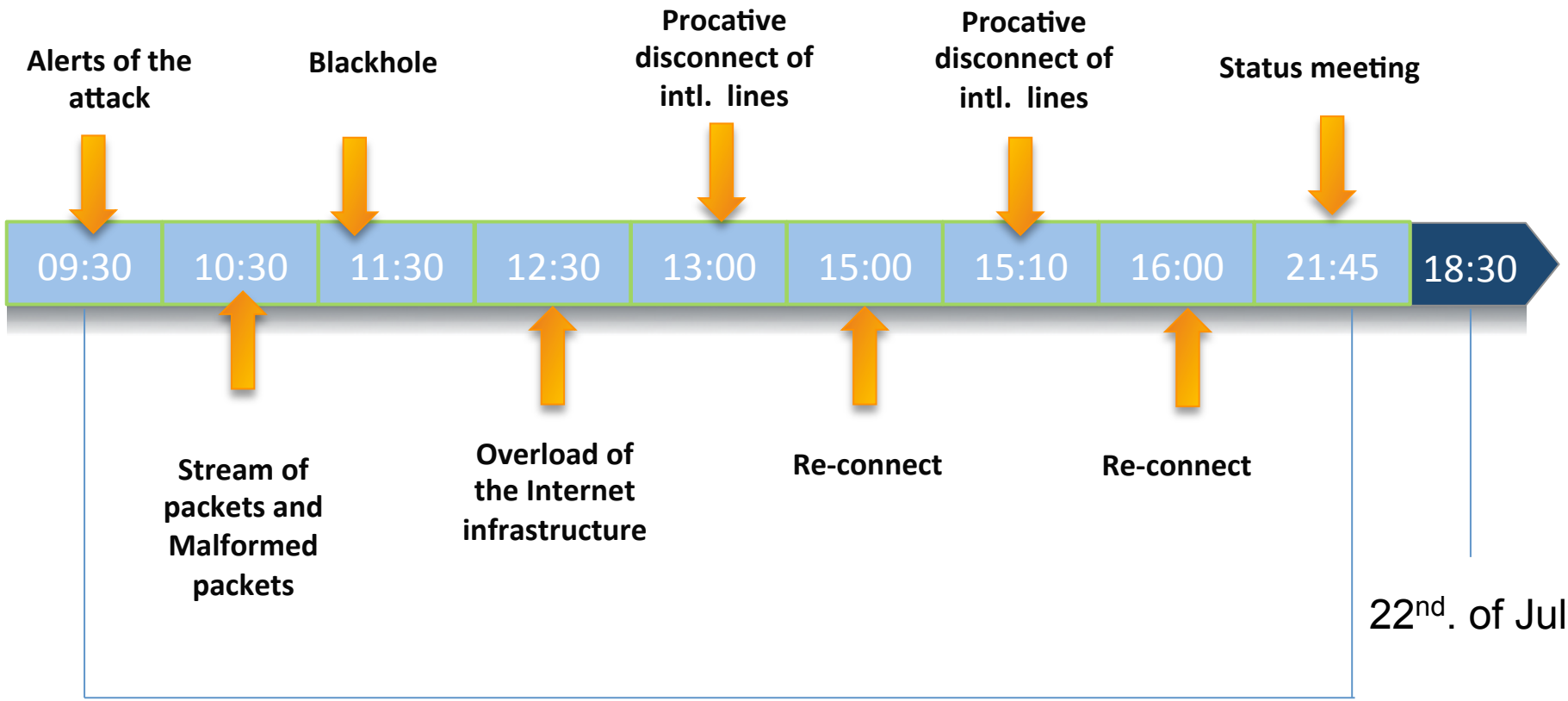


Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

July 21th, 2014 - "OpGaza", phase one

Shut down .il

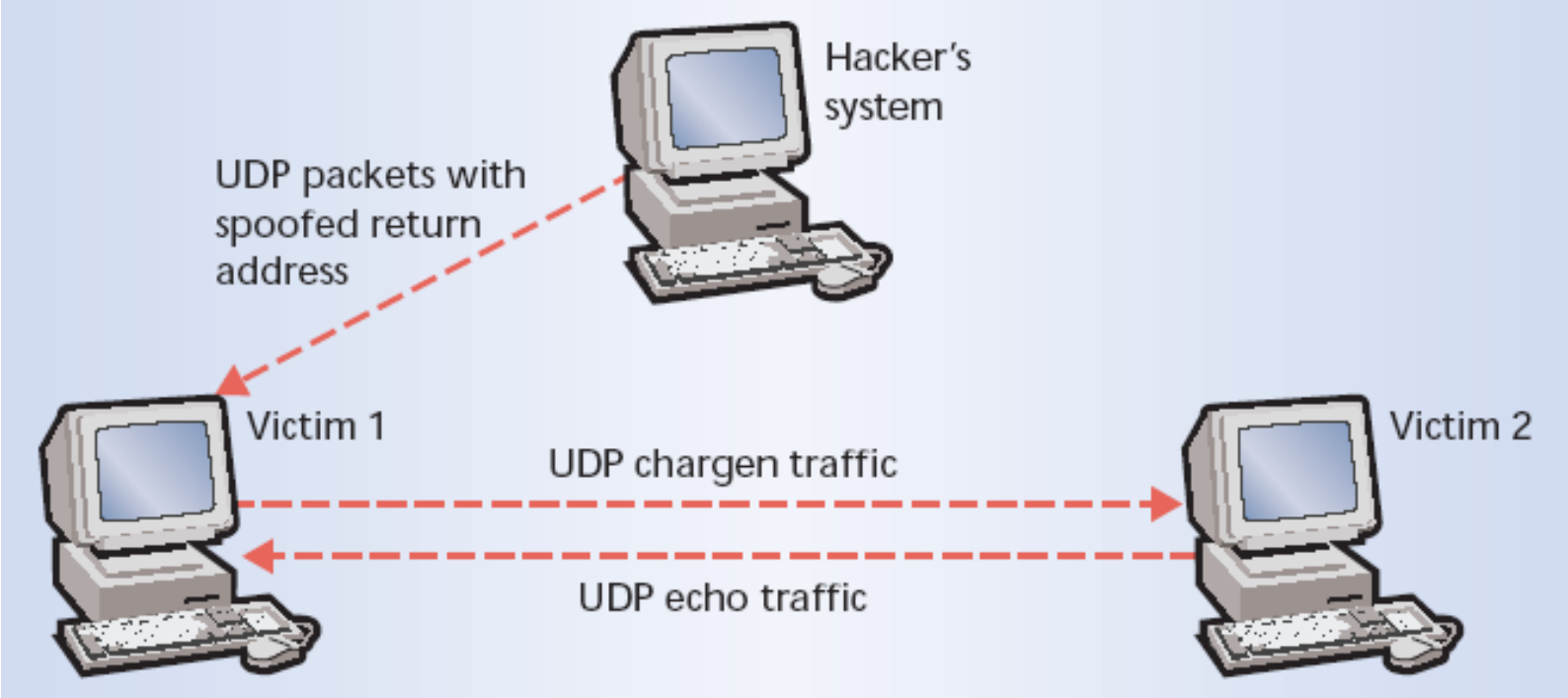


Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

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

July 25th, 2014 - "OpGaza", phase two
Shut down ISP's service

06:50 – dDos Attack to ISP

11:50 – Direct attack on DNS servers .il

13:00 – More than 300,000 .il websites down

14:00 – 3 biggest ISP's are attacked at once

There is no access to the biggest hosting sites

16:00 – ISP's DNS servers are attacked

18:45, July 26th. – End of the attack

Israel Internet Association ISOC-IL

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!

Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

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

Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014 LOS ANGELES

Questions?

Israel Internet Association ISOC-IL

ICANN NO. 51 | 12-16 OCTOBER 2014
LOS ANGELES