THE TIMES OF ISRAEL | www.timesofisrael.com

Security 'situation room' stands ready to prevent 'cyber-holocaust'

In annual OpIsrael attack, hackers promise to 'eliminate Isra-Hell' from cyberspace; a Tel Aviv security firm aims to prevent that

BY DAVID SHAMAH | April 5, 2016, 6:01 pm |

Just how good is Israel's cyber-security technology?

This Thursday, the country will find out as it faces the yearly installation of the OpIsrael hack attack by the international group Anonymous.

Anonymous has released a scary-looking video with dramatic music, special effects, and a voice-over with a "message for the crazy murdering Zionist entity in Isra-Hell that we are coming back to punish you once again." A computer-generated voice promises to take down bank sites, company sites, government servers, and security networks "in an electronical (sic) holocaust that will not be soon forgotten, deleting them from cyber-space as we have done in the past."

Last year, OpIsrael hacktivists threatened an "electronic holocaust," and in fact the period around April 7, 2015, saw something of a spike in cyber-attacks against Israeli websites. To put it in context, though, according to Dr. Isaac Ben-Israel, head of the Tel Aviv University's Yuval Neeman Workshop for Science, Technology, and Security, Israeli sites are anyway subject to hundreds of thousands of attacks every day, "and on 'special occasions' like international organized cyber-attack events or when there is significant tension – like during Operation Protective Edge in 2014 – that number could rise to as many as a million a day."

Experts, pro-Israel hacktivists, and commercial protection services are gearing up to defend the country's networks. And Tel Aviv firm WhiteHat Security will operate a "cyber-situation room" on Thursday, offering free help to any organization or business that needs assistance in battling hackers.

Joining the company in the effort will be a consortium of security firms, government offices, and individual experts who will patrol the internet, zeroing in on attacks and repelling them. That could include, for example, mounting a counter-attack against the source of denial of service (DDOS) attacks – in which huge numbers of processing requests "gang up" on a server to overload and

disable it – by returning the favor.

Other interventions could include closing off communications to servers or websites that are identified as sources for malware, or even helping a group to ensure that its firewall is working properly.

Past OpIsraels have not been notably successful. Users reported that some websites were slow to load on past April 7s as servers attempted to cope with denial of service attacks, by far the most popular tactic used by the international hackers that target Israel on that day.

Attackers did manage to deface dozens of sites (most of them were moribund, having sat on servers for a long time without being updated by their owners or no longer being used). The hackers' greatest accomplishment last year included stealing some 400 names and email addresses off a government server, filching data from several dozen credit card accounts, acquiring a list of email addresses and passwords from the Israel Export Institute, getting access to login data to several dozen Facebook pages, and discovering details of about 10,000 government workers, including names, addresses, email accounts, and phone numbers.

Although it is no indication as to how many hackers will be participating in OpIsrael, the YouTube videos posted online announcing the event have not been popular. Two days before the attack is set to begin, the most-watched version of the dozen or so videos claiming to be from Anonymous, a German-language version, had a viewership of barely 2,000.

Of course, it's important to be prepared, according to Shaon Nemirovsky, CEO of WhiteHat, and he suggests doing the usual things – updating operating system software, anti-virus programs, and Javascript engines; making sure that firewalls are functioning properly; double-checking mail spam filters to keep malware out; impressing upon employees or family members the dangers of clicking on links or opening files from "suspect" sources (which could install destructive malware); and avoiding links to unfanmiliar sites.

"Each year April 7 merits more awareness on both sides, both among hackers and cyber-defenders," said Nemirovsky. "Actually the attacks begin months before April 7, when they reach their crescendo. In 2015 we saw the hackers using some innovative methods to attack Israeli servers and networks, and despite the fact that the impact of the attacks was quite modest, the hackers were able to affect service on several major websites, to deface sites, and to leak data. Being ready and preparing for these attacks can go a long a way toward preventing damage, and our situation room will be available to help out if needed."

© 2015 THE TIMES OF ISRAEL, ALL RIGHTS RESERVED