NIPC ADVISORY 00-058

"Cyber Attacks Against U.S. Web Sites in Ongoing Middle East Conflict"

November 03, 2000

This advisory updates NIPC Assessment 00-057, advising recipients of the ongoing cyber denial-of-service (DoS) attacks against Palestinian- and Israeli-related web sites.

The continued tension and increase in the number of cyber attacks shows no signs of abating and has reportedly resulted in attacks on two U.S. web sites. The attack against one of the sites, the American-Israel Public Affairs Committee (AIPAC), differs from previous attacks on other web sites in that it is the first of its kind to have experienced theft of information, including credit card information. All other attacks involving Palestinian and Israeli-related sites are believed to have consisted solely of a DoS type of attack. The attack against AIPAC resulted in the web site being replaced with one containing anti-Israel slurs. The site was reportedly out of service for approximately 15 minutes and those whose credit card accounts may have been compromised were notified by AIPAC. The FBI is currently investigating this matter.

At least three web sites have been identified as advocating the continuance of the ongoing cyber attacks in the Middle East, as well as including interfaces for the launching of automated e-mail flood, ping flood or other DoS attacks:

- http://members.tripod.com/irsa2000,
- www.ummah.net/unity/defend (relocated to www.defend.unity-news.com),
- www.wizel.com

The NIPC recommends that recipients remain vigilant to the possibility that other U.S. sites may come under attack. It is anticipated that as the conflict in the Middle East continues, the level and severity of cyber attacks being experienced may escalate and expand.

Based on NIPC review of previous activity and ongoing investigations, information system security professionals should be prepared to take recommended preventative measures, including but not limited to, the following: improve password discipline to prevent intrusions based on weak password protection; disable unneeded services that might permit remote re-authoring of web pages; take appropriate steps to limit ping flooding at border routers; block source e-mail IP addresses in the event of e-mail flooding. Ensure appropriate service packs and/or patches are installed to operating systems to limit vulnerability to other DoS attack methods.

Please report any illegal or malicious activities to your local FBI office or the NIPC, and to your military or civilian computer incident response group, as appropriate. Incidents may be reported online at http://www.nipc.gov/incident/cirr.htm.