Cyber Protests Related to the War on Terrorism: The Current Threat

November 2001

This paper is an up-to-date companion to the information on cyber protests and hacktivism presented in the paper "Cyber Protests: The Threat to the U.S. Information Infrastructure" located at www.nipc.gov. This paper focuses on the events that occurred since the September 11 terrorist attacks and the resulting rise in threats to the U.S. information infrastructure, to include the potential for distributed denial-of-service (DDoS) attacks.

Since the terrorist attacks on September 11, 2001 the speculation of the potential for cyber attacks has varied, from low-level nuisances to an all out "cyber war." What has been seen thus far is on the low side of the threat spectrum. Both pro-U.S. protesters and anti-U.S. protesters have been active. However, the effects of their actions have not been particularly damaging. In reviewing these events, trend analysis indicates the continuing remote cyber threat to U.S. networks and web sites remains low. However, the threat is higher than before September 11.

PRO-U.S. HACKERS

Beginning on September 11, patriot hackers and hacking groups on Internet Relay Chat (IRC) and newsgroups called for attacks on Pakistani and Afghani web sites. They promoted active retaliation for the terrorist attacks on the World Trade Center and Pentagon. A web site dealing with Afghan dogs was reportedly the first victim of pro-U.S. cyber protesters. On September 12, the official web site of the Government of Pakistan was defaced. Other web sites defaced were those belonging to the Afghan News Network, Afghan Politics, Taleban.com, and Talibanonline.com.

Spam (unwanted mass e-mails) was also used to encourage hackers to join together in attacking web sites of Islamic fundamentalism and those supporting terrorism. Recipients were encouraged to further disseminate the message to persuade others to join the fight in any way they can, be it active hacking or in a support role such as information gathering. Denial-of-service (DoS) attacks were also used by hackers. E-mail bombing is a popular form of a DoS attack. Massive amounts of e-mail or web traffic are directed against a specific site, overloading it and causing it to crash. On September 12, the official web site of the Presidential Palace of Afghanistan was affected by a DoS attack that rendered it inaccessible. Usenet newsgroups dealing with Islam have also experienced DoS attacks. The newsgroup soc.religion.islam was e-mail bombed by hackers and subsequently crashed.

The call to hackers to join forces has been successful. A group calling itself the Dispatchers has taken up the task of striking out against Palestinian and Afghani web sites. Lead by a hacker named The Rev, who has defaced several sites since February, the group vowed to target those responsible for the September 11 terrorist attacks. Their first known defacement, committed on September 16, was the Iranian Ministry of the Interior. They stated their intentions to continue defacing and crashing sites in retaliation of the terrorist attacks and they have successfully done so, although they have not been heard from since late September.

A prominent pro-U.S. hacking group formed in late September. Founded by the wealthy, German hacker Kim Schmitz, Young Intelligent Hackers Against Terror (YIHAT) has as its goal to gather information on terrorists and give that information to the proper U.S. authorities. They claim to have hacked into a Sudanese bank and found records linking bank accounts to Al-Qaida and Osama bin Laden. They have also created a web site at www.kill.net for recruiting purposes which has suffered DoS attacks from opposing hackers and hacking groups supporting anti-U.S. sentiments, including Fluffi Bunni, a well-known hacker in the community. Subsequently, this has forced YIHAT to move its activities "underground" and operate covertly to protect their members. They have apparently discontinued use of the kill.net web site. Although YIHAT denounces web defacements there have been numerous defacements committed in its name. This appears to be a fringe element of the group, an outsider wishing to be accepted into the group, or someone wanting to discredit the organization. YIHAT also announced plans to seek state sponsorship from a nation that would legalize their hacking activities in their effort to fight terrorism. They also plan to open a hacking training center to better train their members. The group's expanding size has been listed at 800 registered members, although press accounts have placed the number at 25 to 35 active members.

ANTI-U.S. HACKERS

On September 14, Fluffi Bunni defaced web sites numbering in the thousands by compromising an ISP domain name server and redirecting those sites to a page created by himself. The message was "Fluffi Bunni Goes Jihad." This is believed to be the largest single defacement act regarding the terrorist protests. This event only lasted an hour but the number of sites affected was many. Also on September 14, the LifeStages computer virus was renamed to WTC.txt.vbs in order to infect computer users who were curious about the World Trade Center. The resulting effect on computer systems was minimal.

September 15 saw the e-commerce web site belonging to First Responder Supplies hacked by a group claiming to be the Brazilian hacking group Illegal Crew. It is common for hacker groups not associated with a particular event or cause to take up arms in the cyber protests. Brazilian hackers have been involved in protests against the United States for a couple of years. The Pakistan Hackerz Club (PHC), including Doctor Nuker, and GForce Pakistan have also been active in hacking U.S. web sites. GForce Pakistan is a Pakistani hacker group, which formed in February 2000 and is primarily known for web page defacements of Israeli, Indian, and U.S. government web sites. The primary stated motive for their cyber activity to date is in protest of alleged violence and human rights violations against Muslims in Israel and Kashmir. On October 17 the National Oceanic and Atmospheric Administration's web server was hacked in the name of GForce Pakistan which threatened to attack other U.S. and British military web sites unless the demands posted on the defacement are met. Days later, on October 20, GForce allegedly defaced a U.S. Department of Defense (DoD) web site belonging to the Defense Test and Evaluation Processional Institute. This low-level web page defacement illustrates the ability of the hackers to compromise servers but it is unlikely any high-level DoD web servers will be successfully hacked. Other well known hackers have indicated they will join the attacks on U.S. web sites.

Web servers and other computer systems in foreign nations are vulnerable as well as those in the United States. An incident occurred on October 1, in Hungary, when hackers compromised the Hungarian National Security Office's web site and defaced a page with anti-U.S. propaganda. This indicates the hackers' willingness to go after those nations not directly involved in the current war on terrorism.

CALLS FOR AN END TO HACKING

Not all hacker groups have been supportive in the efforts to attack the United States. On September 14, a group of German hackers, the Chaos Computer Club, called for an end to the protests and for all computer enthusiasts to stop vigilante actions. They called for global communication to resolve the conflict. Their peaceful efforts were publicized but largely unheeded by the hacker community as indicated by the continuing defacements on both sides of the issue. Cyber Angels, a well-known group of hackers promoting responsible behavior, have also spoken against the hacking conflict. They sponsored television ads urging hackers not to get caught up in the over zealous fervor, rather, urging these same hackers to help gather intelligence and information on the criminals who are participating in this hacktivism.

CONCLUSION

Groups of Pakistani hackers have declared cyber jihad on the United States and are calling on all hackers of Muslim faith to participate. GForce Pakistan has taken on a large role in building a coalition to fight the United States as military operations are taking place. Their main targets are U.S. sites but they are also attacking Indian sites and foreign sites supporting the United States. They have stated that they will continue to target military sites and web sites that support critical infrastructure.

There has been a spillover effect of the protests. Several misdirected hacks have taken place including the defacements on September 16 of Aon Corporation, a Chicago-based insurance provider, because they have "terrorism" in the URLs. Aon lost approximately 200 employees in their World Trade Center office. A group calling itself "The Dispatchers" apologized for the mistake. Foreign nations are being affected as well. An Australian web site was compromised on September 27 by anti-U.S. hackers because it had "tradecenter" in its URL. This is a common occurrence in that hackers haphazardly target sites without investigating the company's background. Some sites are being attacked merely because their names sound vaguely Arabic. Pro-U.S. hackers will continue to respond to the conflict in cyberspace. There may be more misdirected action against U.S. web sites, those of U.S. allies, or those not involved in the military response to the terrorist attacks.

In the week following the terrorist attacks, web page defacements were well publicized. However, the overall number and sophistication remained rather low. Many of the sites that were defaced by pro-U.S. protesters had pictures of Osama bin Laden inserted in various poses, some with him burning in flames or with a gun to his head. Many of the sites defaced by anti-U.S. protesters had pictures of dead or dying Arab children with statements alleging the hypocrisy of the actions of the United States.

As many expert Information Technology security organizations have intoned since September 11, the potential for more serious cyber attacks does exist; however, they do not appear to be imminent. It is believed that the cyber protests, hacktivism, and on-line defacements will continue and may escalate as the United States continues military involvement. The potential for future DDoS attacks remains high. The protesters have indicated they are targeting web sites of DoD and organizations that support the critical infrastructure of the United States, but many businesses and other organizations-some completely unrelated to the events-have been victims. As such, infrastructure-related organizations should maintain a heightened defensive stance in regards to their web servers and networks connected to the Internet.