'Electronic Jihad' App Offers Cyberterrorism For The Masses

U.S. businesses would be greatly impacted by any large-scale cyberattacks because most of that infrastructure is run by companies in the private sector.

By Larry Greenemeier, InformationWeek
July 2, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=200001943

Although cyberterrorism has been around since the Internet reached the mainstream more than a decade ago, a relatively new Web-based application offers Islamic jihadis a way for even the relatively nontechnical to target and attack Web sites perceived to be anti-Islamic.

The "Electronic Jihad Program" is part of the long-term vision jihadi Web site Al-jinan.org has to use the Internet as a weapon, something that affects any organization that relies on the Web. Electronic Jihad allows users to target specific IP addresses for attack in order to take any servers running at those IP addresses offline. The application even includes a Windows-like interface that lets users choose from a list of target Web sites provided via the Al-jinan site, select an attack speed (weak, medium, or strong), and the click on the "attack" button.

The concept of "electronic jihad" is a relatively recent strain of cyberterrorism interested in very specific network and economic disruption, Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School, told InformationWeek. Its audience consists of malicious Islamic hackers aligned with Osama bin Laden, al-Qaida, and the extremist Islamic movement. "The attacks from jihadists are interested in taking Web sites down and disrupting economies that they don't like," she added. "It's something to be taken seriously."

U.S. businesses would be greatly impacted by any large-scale cyberattacks against either them or the country's critical infrastructure because most of that infrastructure is run by companies in the private sector. The government and the U.S. business community "are one-in-the-same target," Andrew Colarik, an information security consultant who holds a Ph.D. in information systems security from the University of Auckland, told InformationWeek. Even businesses that don't run critical infrastructure elements could be affected because "there's a cascading effect if you attack the infrastructure."

The latest version of Electronic Jihad software, 2.0, is designed to quickly update its list of target sites and to work with different Internet connection speeds. The application is also described as being capable of using different proxies to override government Web site blocking technology, Abdul Hameed Bakier, an intelligence expert on counterterrorism, crisis management, and terrorist-hostage negotiations, wrote in a recent report for the Jamestown Foundation, a Washington, D.C., think tank established on Sept. 11, 2003, to study and analyze global terrorism. "In the past, different jihadi groups practiced cyberattacks on anti-Islamic websites, but they were never able to sustain a long, organized campaign," Bakier wrote in the June 26 edition of Jamestown's weekly Terrorism Focus publication. He noted that Al-jinan is not only operating continuously but is developing new techniques to enhance the technology and methods of promoting electronic jihad. "With the spreading use of the Internet in the Arab and Islamic

world, the number of users engaged in some form of electronic jihad is likely to increase substantially," he added.

In addition to supplying the online weapons for cyberattack, the Al-jinan site also serves as a forum for learning attack techniques as well as other information that can be used in electronic jihad efforts. One emphasis is on the need for jihadis to organize synchronized mass cyberattacks on Web sites that they believe are critical of Islam. Electronic Jihad users set up an account name and password, which lets the site register the number of hours the user spends attacking targets and post the names of those who scored the highest. One attacker spent the equivalent of 70 days attacking sites.

Of course, the notion of "hactivism," which really lies at the heart of electronic jihad, has been around for years. In 1995, the Strange Communication Network, or Strano, launched what it called "the first global strike" on the Internet when it encouraged Web users to point their browsers at French government sites and repeatedly click on "reload" for an hour. "This was to disrupt French government sites, and it probably did back then," Denning said.

Since then, cyberterrorism has been a persistent threat that draws attention to itself only in extreme instances. The Baltic nation of Estonia was hit for two weeks at the end of April and early May with 128 cyberattacks launched against that country's computer infrastructure. While the source of those attacks is still being investigated, the results could have been dire for the country, where 97% of bank transactions are done via the Internet.

"When you are a highly Interneted country like we are, then these kinds of attacks can do very serious damage," Estonian President Toomas Hendrik Ilves said during a June 25 press conference with U.S. President Bush. "And I do think it's the wave of the future--not that it's a good wave, but it is something that we have to deal with more and more." Ilves added, "We know that the United States and Israel and Denmark have come under cyberattack before, and I think that it's an issue that will require much more attention in the future."

Estonia has linked the cyberattacks to a dispute with Russia over the relocation of a Soviet war memorial from the World War II era in the Estonian capital, Tallinn, shortly before the attacks began. Russia, however, has denied any involvement in the incident. The country has been at odds with Russia since regaining its freedom from the former Soviet Union in 1991.

The U.S. Defense Department is certainly not immune to cyberattacks. A cybersecurity breach on June 20 forced the Pentagon to take an estimated 1,500 computers offline. Secretary of Defense Robert Gates said at a press conference the following day that the e-mail system in the Office of the Secretary of Defense was penetrated by hackers, and "elements" of the unclassified e-mail system were shut down in response.

It's hard to tell if the attack on the Defense Department came from a terrorist cell or a political group or if it was an attack sanctioned by a foreign government, Colarik said, adding, "Or it could be a combination of these, with someone seeing that an attack was happening [against Pentagon computers] and jumping on the bandwagon."

However, security pros needn't get caught up in the distinctions between "cyberterrorism" and "electronic jihad" because they both rely heavily on a form of attack that IT security pros have been seeing for quite some time, Denning said, adding, "It's about DoS [denial-of-service] attacks, something that's been around for a while."

While companies that operate critical infrastructure must be especially wary of Internet-based attacks, "everyone has to pay attention to security," Denning said. "There may be some businesses that say no one will target us. But electronic jihad will target anyone if it creates economic disruption. Whoever's vulnerable gets attacked."