Al-Jazeera web site under attack from pro-war hackers

Mick Ingram
1 April 2003

The web site of the Arab news agency Al-Jazeera has been under constant attack from hackers since the launch of its English language site on March 24.

The English language site was widely welcomed as an alternative to the official Western media, which is seen by many as a propaganda vehicle of the Pentagon. Devoted to news on the war against Iraq, it carries headlines such as "US 'precision' bomb destroys civilian bus", "Misinformation Basra" and "Hunger turns Iraqi civilians against US 'saviours'". Among the first articles in English was an eyewitness account of the assault on the Iraqi capital, Baghdad.

Immediately following the site's launch, it began to suffer from network outages. Internet monitoring service Keynote Systems reported on March 25 that Al-Jazeera and its English-language counterpart were only intermittently available for the second straight day. From approximately 12:30 p.m. Pacific Standard Time that day, the English news portion of the site seemingly dropped off the Internet, according to Roopak Patel, at Keynote's public services division.

While this was initially reported as simply being due to the popularity of the site and the inability of Al-Jazeera's hosting company to cope with demand, Patel stressed, "There's a whole host of reasons that the site could not be accessible. The server could be not able to serve up data as fast ... or it could be an attack."

Tom Ohlsson, a representative of network performance measurement service Matrix NetSystems, was quoted by CNET saying that in general the company hasn't seen signs of serious hacking since the start of the war.

"We were prepared to see malicious worms and viruses launched in conjunction with what's going on in Iraq, but we aren't seeing anything like that. There is no (widespread) disruption of traffic across the Internet," Ohlsson said.

As the sites remained inaccessible for the third day in a row, it was reported that Al-Jazeera had been hit by a distributed denial-of-service (DDOS) attack that began March 25. A DDOS attack involves the flooding of a network with data from any number of computers around the world. Hackers increasingly make use of compromised home PCs with permanent broadband connections to the Internet to launch the offending data packets. The attack is hard to detect as the data is nearly indistinguishable from that normally created by Web users.

By far the most serious problem for Al-Jazeera came on March 27 when the site was replaced with an American flag and a pro-US message which read, "Let Freedom Ring!" and "GOD BLESS OUR TROOPS!!!" The hacker signed the page "Patriot" and claimed to be part of a group called the Freedom Cyber Force Militia.

Defacement of web sites is a regular pastime for hackers. According to defacement tracker Zone-H.org, attackers who tag Web sites with digital graffiti normally want the world to know and so immediately notify sites like Zone-H.org of the defacement. Zone-H will immediately make a copy of the Web site and keep the copy as evidence of the defacement.

On an average workday, 350 sites are defaced, with as many as 1,000 sites defaced in an average weekend. After US strikes began on Iraq, those numbers increased significantly. Zone-H.org is now seeing as many as 2,500 sites defaced every day by both pro-war and antiwar hackers.

Such defacement is not normally difficult for a webmaster to deal with, involving only the restoration of the original data and the tracking down and fixing of the security hole used by the hacker to prevent it happening again. The attack on Al-Jazeera, however, was no ordinary defacement. The address of the site had been hijacked to point to another server carrying the hacker's message.

The actual defacement appeared on a free web site service provided by NetWorld Connections. Technically known as a "redirect," the hack caused web browsers that attempted to go to the domain name www.aljazeera.net—as well as the English-language site—to be surreptitiously redirected to the content hosted on NetWorld's servers.

Networld became aware of the attack on the morning of March 27 when it detected a spike in traffic. An email from

a security specialist confirmed that visitors to Al-Jazeera were being redirected to NetWorld's service, according to Ken Bowman, chief executive of the Salt Lake City company.

"We pulled down the content immediately," Bowman said, adding that VeriSign, which administers the domain registry, eliminated the redirect later in the morning. "They never even touched [Al-Jazeera's] site," he said.

The attack resulted from the compromising of Al-Jazeera's account with VeriSign subsidiary Network Solutions. The hacker changed the web site's nameservers to point to those of MyDomain.com, a free hosting service. In a press statement issued March 27, the company said, "MyDomain has learned from NavLink, the company that hosts the aljazeera.net web site from its data centres in France, that Al-Jazeera's domain name account at Network Solutions was compromised."

The problem was corrected by eliminating the redirect and reinstating the correct addresses for Al-Jazeera's sites. However, the changes take up to three days to filter throughout the Internet. Al-Jazeera's sites continue to come under DDOS attacks.

The FBI has said it has launched an investigation into the attack, but there is little chance that the perpetrators will be identified. The hackers had chosen their target for the hosting of the faked site well. NetWorld's Bowman explained that the site had been created using a free hosting service that the company offers. Because the service is free, the company does not keep rigorous watch on the activities of its users.

"All the supplied information was fictitious," he said. "It's a free site, so we don't track any data. We don't track the Internet addresses or anything else. It would take a staff of about 500 to do so." Bowman said NetWorld are analysing what happened and may change the way the free portion of the site is administered to prevent future incidents.

Far more worrying is the fact that the records of Verisign, one of the leading providers of secure web services, were compromised.

VeriSign maintains the Internet registry for the .com, .net, .cc and .tv top-level domains and administers the authoritative database for all domain names registered in those top-level domains after acquiring Network Solutions, the company originally given authority of the domains by the US government when the Internet became a public network.

The records from the *whois* database—the distributed directory that holds information about each domain—indicated early on March 27 that hackers had managed to forge new domain records. Such records typically describe the services that are offered by a particular domain, such as web, mail and file hosting. VeriSign's records for Al-Jazeera had been replaced by data that pointed to name servers hosted by MyDomain.com. Those name servers in turn referred web requests to the defacement site located at NetWorld.

The company boasts on its web site, "VeriSign's critical infrastructure services deliver an unmatched level of security and reliability to Internet and telecommunications customers around the world. Nearly all of the Fortune 500 companies, governmental bodies and other organisations, hundreds of thousands of small businesses, and hundreds of service providers rely on VeriSign to engage in digital commerce and communications." The site carries no explanation of how Al-Jazeera's records were forged.

Given the hostility of the US government towards Al-Jazeera, it is difficult to see anything coming from the investigation of the FBI. The way in which the attack was carried out indicates that this was no ordinary hack. While most defacements involve hacking into the server that hosts the site and changing the site's content, this one targeted the domain name itself, ensuring that administrators at NavLink could do nothing to restore the site.

To compromise the Verisign servers would take a high degree of specialist knowledge. It is a tradition among established hackers to use a known nickname in order to take credit for a hack. It is hard to believe that those responsible for such a prestigious achievement would not do the same, but security experts familiar with the defacement scene say they have never heard of a group called Freedom Cyber Force Militia—suggesting it may be a cover for some other organisation and/or individuals.