

Military Files Left Unprotected Online

Associated Press | July 12, 2007

GREENSBORO, N.C. - Detailed schematics of a military detainee holding facility in southern Iraq. Geographical surveys and aerial photographs of two military airfields outside Baghdad. Plans for a new fuel farm at Bagram Air Base in Afghanistan.

The military calls it "need-to-know" information that would pose a direct threat to U.S. troops if it were to fall into the hands of terrorists. It's material so sensitive that officials refused to release the documents when asked.

But it's already out there, posted carelessly to file servers by government agencies and contractors, accessible to anyone with an Internet connection.

In a survey of servers run by agencies or companies involved with the military and the wars in Iraq and Afghanistan, The Associated Press found dozens of documents that officials refused to release when asked directly, citing troop security.

Such material goes online all the time, posted most often by mistake. It's not in plain sight, unlike the plans for the new American embassy in Baghdad that appeared recently on the Web site of an architectural firm. But it is almost as easy to find.

And experts said foreign intelligence agencies and terrorists working with al-Qaida likely know where to look.

In one case, the Army Corps of Engineers asked the AP to promptly dispose of several documents found on a contractor's server that detailed a project to expand the fuel infrastructure at Bagram - including a map of the entry point to be used by fuel trucks and the location of pump houses and fuel tanks. The Corps of Engineers then changed its policies for storing material online following the AP's inquiry.

But a week later, the AP downloaded a new document directly from the agency's own server. The 61 pages of photos, graphics and charts map out the security features at Tallil Air Base, a compound outside of Nasiriyah in southeastern Iraq, and depict proposed upgrades to the facility's perimeter fencing.

"That security fence guards our lives," said Lisa Coghlan, a spokeswoman for the Corps of Engineers in Iraq, who is based at Tallil. "Those drawings should not have been released. I hope to God this is the last document that will be released from us."

The Corps of Engineers and its contractor weren't alone:

- The National Geospatial-Intelligence Agency - which provides the military with maps and charts - said it plans to review its policies after the AP found several sensitive documents, including aerial surveys of

military airfields near Balad and Al Asad, Iraq, on its server.

- Benham Companies LLC is securing its site after learning it had inadvertently posted detailed maps of buildings and infrastructure at Fort Sill, Okla. "Now, everything will be protected," said Steve Tompkins, a spokesman for Oklahoma City-based Benham.

- Los Alamos National Laboratory and Sandia National Laboratories, two of the nation's leading nuclear laboratories, closed public access to their file transfer protocol servers after the AP contacted them about material posted there. Both said the change was unrelated to the AP's inquiry.

The AP has destroyed the documents it downloaded, and all the material cited in this story is no longer available online on the sites surveyed.

The posting of private material on publicly available FTP servers is a familiar problem to security experts hired by companies to secure sites and police the actions of employees who aren't always tech-savvy. They said files that never should appear online are often left unprotected by inexperienced or careless users who don't know better.

A spokeswoman for contractor SRA International Inc., where the AP found a document the Defense Department said could let hackers access military computer networks, said the company wasn't concerned because the unclassified file was on an FTP site that's not indexed by Internet search engines.

"The only way you could find it is by an awful lot of investigation," said SRA spokeswoman Laura Luke.

But on Tuesday, SRA had effectively shut down its FTP server. The only file online was a short statement: "In order to mitigate the risk of SRA or client proprietary information being inadvertently made available to the public, the SRA anonymous ftp server has been shutdown indefinitely. In the coming months, a new secure ftp site will be introduced that will replace the functionality of this site."

Bruce Schneier, chief technology officer of BT Counterpane, a Mountain View, Calif.-based technology security company, said the attitude that material posted on FTP sites is hard to find reflects a misunderstanding of how the Internet works.

"For some, there's sort of this myth that 'if I put something on the Net and don't tell anybody,' that it's hidden," Schneier said. "It's a sloppy user mistake. This is yet another human error that creates a major problem."

File transfer protocol is a relatively old technology that makes files available on the Internet. It remains popular for its simplicity, efficiency and low cost. In fact, several agencies and contractors said the documents found by the AP were posted online so they could be easily shared among colleagues.

Internet users can't scour the sites with a typical search engine, but FTP servers routinely share a similar address as public Web sites. To log on, users often only need to replace "http" and "http://www" in a Web address with "ftp."

Some are secured by password or a firewall, but others are occasionally left open to anyone with an Internet connection to browse and download anonymously. Experts said that when unsophisticated users post sensitive information to the servers, they would not necessarily know it could be downloaded by people outside of their business or agency.

"What they don't realize is that every time you set up any type of server, you have that possibility," said Danny Allan, director of security research for Watchfire, a Waltham, Mass.-based Web security company. "Any files that you are putting on the server you want to monitor on a continuous basis."

Allan said he and others in the security industry have watched for more than a decade as files - including credit card information, sensitive blueprints of government buildings and military intelligence reports - spread through the public domain via unsecured FTP servers.

A spokeswoman for the U.S. Central Command, which oversees the war in Iraq, declined to say if material accidentally left on the Internet had led to a physical breach of security.

But among the documents the AP found were aerial photographs and detailed schematics of Camp Bucca, a U.S.-run facility for detainees in Iraq. One of the documents was password-protected, but the password was printed in an unsecure document stored on the same server. They showed where U.S. forces keep prisoners and fuel tanks, as well as the locations of security fences, guard towers and other security measures.

"It gets down to a level of detail that would assist insurgents in trying to free their members from the camp or overpower guards," said Loren Thompson, a military analyst with the Virginia-based Lexington Institute. "When you post ... the map of a high-security facility that houses insurgents, you're basically giving their allies on the outside information useful in freeing them."

The Corps of Engineers expressed a similar concern when it learned that the AP had downloaded the details about the fuel infrastructure upgrade at Bagram from a contractor's FTP site. Spokeswoman Joan Kibler said that kind of information "could put our troops in harm's way."

The AP's discovery led the agency to ask all its contractors to immediately put such material under password protection. In fact, all the agencies and contractors contacted by the AP have either shut down their FTP sites, secured them with a password or pledged to install other safeguards to ensure the documents are no longer accessible.

"We saw that there have been instances where some documents have been placed on FTP sites, and they haven't had any safeguarding mechanisms for them," Kibler said. "We've determined that those documents need to be safeguarded, so we've amended our practices here to require that any of those types of documents have restricted access when they're placed on FTP sites."

Documents found by the AP about Contingency Operating Base Speicher near Tikrit, Iraq, describe potential security vulnerabilities at the facility and paraphrase an Army major expressing concerns about a "great separation between personnel and equipment" as the base prepared for the military's current counterinsurgency push.

"For force-protection reasons and operational security, that's sensitive stuff," said Lt. Col. Michael Donnelly, a military spokesman based at Speicher. "That's for a need-to-know basis. The enemy regularly takes that stuff and pieces it together for their advantage."

The information about Camp Bucca, Bagram Air Base and Contingency Operating Base Speicher was found on the FTP server of CH2M Hill Companies Ltd., an engineering, consulting and construction company based in Englewood, Colo.

"None of the drawings are classified and we believe they were all handled appropriately per the government's direction," said CH2M Hill spokesman John Corsi. But the company added a password protection to its FTP site after the AP's inquiry and referred the direct request for the documents to the government.

Military officials said they could jeopardize troop security and refused to release them.

Other files found by the AP didn't appear to pose an immediate threat to troop security, but illustrated advanced military technologies. The National Geospatial-Intelligence Agency posted PowerPoint presentations outlining military GPS systems, including plans to combat GPS jammers. Files from Los Alamos give an early look at a developing technology to combat enemy snipers in urban environments, including one file describing the levels of security behind the new program.

Dean Carver, a counterintelligence officer with the federal Office of the National Counterintelligence Executive, part of the Office of the Director of National Intelligence, said at a recent security conference that such trade secrets - even those dealing with a basic technology - are often a common target for foreign espionage because they can be used to advance a country's own military technology.

"Every military-critical technology is sought by many foreign governments," said Carver, mentioning China and Russia as the leading culprits of snooping on the Internet.

Christopher Freeman believes he may have witnessed such hunting for secrets. While working on an internal security review at his job with the city of Greensboro, N.C., Freeman watched as a computer with an electronic address from Tehran, Iran, accessed the city's FTP server and downloaded a file that contained design drawings for the area's water infrastructure.

He said that while there's no way to know if there was malicious intent behind the download, "when you think of Iran, you think of all the bad stuff first."

"It could have been anyone," Freeman said. "It opened our eyes to show that we're not just little old Greensboro. We're a part of the global community."

That was years ago, and it led Freeman to start looking for FTP sites he thought should be secure. He found a manual describing how to operate a Navy encryption device on the server of the Space and Naval Warfare Systems Command. He also found photographs and graphics detailing the inner workings of missiles designed at Sandia.

"It's not something that had any business being on a FTP site," said Sandia spokeswoman Stephanie

Holinka of the material Freeman found. The agency has shut down its FTP site while a security upgrade is put in place, she said.

Many sites housed raw data, presentations and documents that didn't have security classifications, while other documents were clearly marked to prevent public release. The manual of the encryption device tells users to "destroy by any method that will prevent disclosure of contents or reconstruction of this document." A warning says exporting the document could result in "severe criminal penalties."

"The military is often criticized for making too many things secret, but when you're enabling an enemy to find out how you use encryption devices, you easily could be helping them to defeat America," said Thompson, the military analyst.

Freeman, who showed the AP the documents from Sandia and the Space and Naval Warfare Systems Command, said he made a conscious effort to avoid information labeled classified but still managed to accidentally download files from Sandia with "top secret" classifications, forcing him to wipe his computer hard drive clean and notify authorities.

Freeman passed along his findings to the FBI and the Department of Defense and later aided investigators in securing the Space and Naval Warfare Systems Command site. After getting calls from a contractor and the Army Materiel Command asking about what he found online, Freeman has sought legal representation from Denner Pellegrino, a Boston-based firm that specializes in cyber crime.

"This is a treasure trove for terrorists," Freeman said. "They can just waltz in and browse. I'm by no means a high-tech person. I'm not a programmer. I don't know hacking. I'm just a slightly above-average computer user."

FBI officials declined to specifically discuss Freeman and what he told the agency. But Mark Moss, a Charlotte-based FBI agent who focuses on online security, said foreign intelligence agencies spend a lot of time on the Internet because online intelligence-gathering is cheap, quick and anonymous.

"If they steal your technology through the Internet, it's overseas in an instant," Moss said. "It's the perfect conduit."

Copyright 2011 Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

<http://www.military.com/NewsContent/0,13319,142101,00.html?ESRC=topstories.RSS>