COMPUTERWORLD An IDG company

Intelligence ops in Baghdad show need for physical security back home

By DAN VERTON
APRIL 08, 2003

The U.S. Central Command today declined to offer details on how U.S. military forces were tipped off to an alleged meeting of Saddam Hussein and his top aides yesterday. But sources indicated today that physical taps on telephone and fiber-optic landlines in the Iraqi capital of Baghdad may have played a role.

"We have a number of methods that we use to gain information," Brig. Gen. Vincent Brooks said during today's Central Command press briefing. "A single source is never adequate, so we have multiple sources."

Bombing missions near civilian targets also require that somebody on the ground "see" the target, he said.

The process by which the CIA and the military determined the likely location and time of an Iraqi leadership meeting is known in intelligence parlance as all-source fusion -- a process by which human intelligence, surveillance, imagery from satellites and aircraft and intercepted communications form pieces of a puzzle that help officials understand what's happening on the battlefield. It is the last piece, communications intelligence, that experts say may have played a key role in targeting Saddam.

"Tapping a fiber-optic cable without being detected, and making sense of the information you collect, isn't trivial but has certainly been done by intelligence agencies for the past seven or eight years," said John Pescatore, an analyst at Stamford, Conn.-based Gartner Inc. and a former National Security Agency analyst. "These days, it is within the range of a well-funded attacker, probably even a really curious college physics major with access to a fiber-optics lab and lots of time on his hands."

The importance placed on fiber-optic communications cables in Baghdad by the Iraqi regime dates to the first Gulf War in 1990. Saddam quickly realized that the U.S. was capable of intercepting most radio and wireless communications, and as a result, worked to avoid detection by hiring French and Chinese companies to install a fiber-optic backbone that is closely integrated with the civilian

telephone network. That makes it difficult for intelligence services to determine the separation point between civilian networks and the government's command-and-control networks.

U.S. intelligence agencies or their foreign adversaries have in the past employed physical taps on fiber-optic and telephone cables to gain intelligence. In 1955, during what was known as Operation Gold, the CIA tunneled under the border between East and West Berlin to tap phone lines used by Soviet intelligence. Likewise, during the early 1980s, the CIA's Operation TAW involved the tapping of a top-secret communications center outside Moscow by placing listening devices on cables in sewer tunnels.

Fiber-optic cables use light to transmit information and can be easily intercepted, interpreted and manipulated with standard off-the-shelf equipment that can be obtained legally throughout the world. More important, the vast majority of private and public fiber networks don't incorporate methods for detecting optical taps, offering an intruder a relatively safe way to conduct corporate espionage. Commercial intrusion-detection systems and other IT security systems operate at the data layer and offer no way to identify the existence of physical taps.

While there haven't been any high-profile public cases involving optical taps, experts and a former head of one of the major U.S. intelligence agencies warn that potential physical taps on fiber infrastructure should also be a concern for companies in the U.S.

Seth Page, CEO of Oyster Optics Inc. in Manhattan, has studied the threat of physical optical taps in detail and said they can be virtually impossible to detect. "Unless a field engineer happens to stumble upon a tapping device by accident you're not going to find optical taps," said Page. "Most CEOs and CIOs have no idea that optical taps are even technically feasible."

Not only are they feasible, but they may also be easier to conduct successfully than once thought. Web sites for metropolitan areas, such as San Diego, often post detailed maps of the entire citywide fiber backbone. In addition, the same high-speed fiber bundle sometimes serves a dozen or more office buildings, meaning criminals could gain access to wiring closets located in building basements or to cables that pass through public parking garages or elevator shafts, said Page.

In fact, standard testing and maintenance equipment is often used to either splice, split or passively capture a signal that's leaking from the cable, according to Page. Methods for using this equipment can now be found in the public domain.

"The vulnerability is entirely dependent on how the provider of services handles segmentation of the channels, multiplexing," said the former intelligence agency chief. "If the fiber-optic transport is a loop, if there is a common multiplexing

scheme and no virtual private network or encryption protection for each user, which is usually the case with fiber, then access to a wiring closet is an easy way into a target," the former intelligence official said.

"This layer of security -- not just for fiber, but for standard LAN and telephone wiring also -- isn't really thought out by companies," said Pescatore. "I'd estimate that 75% of enterprises have some network cabling in public access space."

According to Page, while some banks in the U.S. have dedicated fiber running directly from a central switching office, other companies pay for a share of bandwidth where virtual channels are built. All that's required after identifying the location of the cables is an optical packet sniffer and a PC to pull out the information you want, he said.

"This has serious security implications for users of fiber-optical communication systems, especially those with sensitive data such as financial institutions, insurance firms and health care corporations, as well as R&D facilities, global manufacturers and government agencies," said Page.

Source: Computerworld

Dan Verton is a Senior Writer at Computerworld and the author of Black Ice: The Invisible Threat of Cyber-Terrorism (McGraw-Hill, Summer 2003) & The Hacker Diaries (McGraw-Hill, 2002).