N.S.A. Devises Radio Pathway Into Computers

By DAVID E. SANGER and THOM SHANKER JAN. 14, 2014

WASHINGTON — The National Security Agency has implanted software in nearly 100,000 computers around the world that allows the United States to conduct surveillance on those machines and can also create a digital highway for launching cyberattacks.

While most of the software is inserted by gaining access to computer networks, the N.S.A. has increasingly made use of a secret technology that enables it to enter and alter data in computers even if they are not connected to the Internet, according to N.S.A. documents, computer experts and American officials.

The technology, which the agency has used since at least 2008, relies on a covert channel of radio waves that can be transmitted from tiny circuit boards and USB cards inserted surreptitiously into the computers. In some cases, they are sent to a briefcase-size relay station that intelligence agencies can set up miles away from the target.

The radio frequency technology has helped solve one of the biggest problems facing American intelligence agencies for years: getting into computers that adversaries, and some American partners, have tried to make impervious to spying or cyberattack. In most cases, the radio frequency hardware must be physically inserted by a spy, a manufacturer or an unwitting user.

The N.S.A. calls its efforts more an act of “active defense” against foreign cyberattacks than a tool to go on the offensive. But when Chinese attackers place similar software on the computer systems of American companies or government agencies, American officials have protested, often at the presidential level.

Among the most frequent targets of the N.S.A. and its Pentagon partner, United States Cyber Command, have been units of the Chinese Army, which the United States has accused of launching regular digital probes and attacks on American industrial and military targets, usually to steal secrets or intellectual property. But the program, code-named Quantum, has also been successful in inserting software into Russian military networks and systems used by the Mexican police and drug cartels, trade institutions inside the European Union,

and sometime partners against terrorism like Saudi Arabia, India and Pakistan, according to officials and an N.S.A. map that indicates sites of what the agency calls “computer network exploitation.”

“What’s new here is the scale and the sophistication of the intelligence agency’s ability to get into computers and networks to which no one has ever had access before,” said James Andrew Lewis, the cybersecurity expert at the Center for Strategic and International Studies in Washington. “Some of these capabilities have been around for a while, but the combination of learning how to penetrate systems to insert software and learning how to do that using radio frequencies has given the U.S. a window it’s never had before.”

No Domestic Use Seen

There is no evidence that the N.S.A. has implanted its software or used its radio frequency technology inside the United States. While refusing to comment on the scope of the Quantum program, the N.S.A. said its actions were not comparable to China’s.

“N.S.A.'s activities are focused and specifically deployed against — and only against — valid foreign intelligence targets in response to intelligence requirements,” Vanee Vines, an agency spokeswoman, said in a statement. “We do not use foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of — or give intelligence we collect to — U.S. companies to enhance their international competitiveness or increase their bottom line.”

Over the past two months, parts of the program have been disclosed in documents from the trove leaked by Edward J. Snowden, the former N.S.A. contractor. A Dutch newspaper published the map of areas where the United States has inserted spy software, sometimes in cooperation with local authorities, often covertly. Der Spiegel, a German newsmagazine, published the N.S.A.'s catalog of hardware products that can secretly transmit and receive digital signals from computers, a program called ANT. The New York Times withheld some of those details, at the request of American intelligence officials, when it reported, in the summer of 2012, on American cyberattacks on Iran.

President Obama is scheduled to announce on Friday what recommendations he is accepting from an advisory panel on changing N.S.A. practices. The panel agreed with Silicon Valley executives that some of the techniques developed by the agency to find flaws in computer systems undermine global confidence in a range of American-made information products like laptop computers and cloud services.

Embracing Silicon Valley's critique of the N.S.A., the panel has recommended banning, except in extreme cases, the N.S.A. practice of exploiting flaws in common software to aid in American surveillance and cyberattacks. It also called for an end to government efforts to weaken publicly available encryption systems, and said the government should never develop secret ways into computer systems to exploit them, which sometimes include software implants.

Richard A. Clarke, an official in the Clinton and Bush administrations who served as one of the five members of the advisory panel, explained the group's reasoning in an email last week, saying that "it is more important that we defend ourselves than that we attack others."

"Holes in encryption software would be more of a risk to us than a benefit," he said, adding: "If we can find the vulnerability, so can others. It's more important that we protect our power grid than that we get into China's."

From the earliest days of the Internet, the N.S.A. had little trouble monitoring traffic because a vast majority of messages and searches were moved through servers on American soil. As the Internet expanded, so did the N.S.A.'s efforts to understand its geography. A program named Treasure Map tried to identify nearly every node and corner of the web, so that any computer or mobile device that touched it could be located.

A 2008 map, part of the Snowden trove, notes 20 programs to gain access to big fiber-optic cables — it calls them "covert, clandestine or cooperative large accesses" — not only in the United States but also in places like Hong Kong, Indonesia and the Middle East. The same map indicates that the United States had already conducted "more than 50,000 worldwide implants," and a more recent budget document said that by the end of last year that figure would rise to about 85,000. A senior official, who spoke on the condition of anonymity, said the actual figure was most likely closer to 100,000.

That map suggests how the United States was able to speed ahead with implanting malicious software on the computers around the world that it most wanted to monitor — or disable before they could be used to launch a cyberattack.

A Focus on Defense

In interviews, officials and experts said that a vast majority of such implants are intended only for surveillance and serve as an early warning system for cyberattacks directed at the United States.

“How do you ensure that Cyber Command people” are able to look at “those that are attacking us?” a senior official, who compared it to submarine warfare, asked in an interview several months ago.

“That is what the submarines do all the time,” said the official, speaking on the condition of anonymity to describe policy. “They track the adversary submarines.” In cyberspace, he said, the United States tries “to silently track the adversaries while they’re trying to silently track you.”

If tracking subs was a Cold War cat-and-mouse game with the Soviets, tracking malware is a pursuit played most aggressively with the Chinese.

The United States has targeted Unit 61398, the Shanghai-based Chinese Army unit believed to be responsible for many of the biggest cyberattacks on the United States, in an effort to see attacks being prepared. With Australia’s help, one N.S.A. document suggests, the United States has also focused on another specific Chinese Army unit.

Documents obtained by Mr. Snowden indicate that the United States has set up two data centers in China — perhaps through front companies — from which it can insert malware into computers. When the Chinese place surveillance software on American computer systems — and they have, on systems like those at the Pentagon and at The Times — the United States usually regards it as a potentially hostile act, a possible prelude to an attack. Mr. Obama laid out America’s complaints about those practices to President Xi Jinping of China in a long session at a summit meeting in California last June.

At that session, Mr. Obama tried to differentiate between conducting surveillance for national security — which the United States argues is legitimate — and conducting it to steal intellectual property.

“The argument is not working,” said Peter W. Singer of the Brookings Institution, a co-author of a new book called “Cybersecurity and Cyberwar.” “To the Chinese, gaining economic advantage is part of national security. And the Snowden revelations have taken a lot of the pressure off” the Chinese. Still, the United States has banned the sale of computer servers from a major Chinese manufacturer, Huawei, for fear that they could contain technology to penetrate American networks.

An Old Technology

The N.S.A.'s efforts to reach computers unconnected to a network have relied on a century-old technology updated for modern times: radio transmissions.

In a catalog produced by the agency that was part of the Snowden documents released in Europe, there are page after page of devices using technology that would have brought a smile to Q, James Bond's technology supplier.

One, called Cottonmouth I, looks like a normal USB plug but has a tiny transceiver buried in it. According to the catalog, it transmits information swept from the computer "through a covert channel" that allows "data infiltration and exfiltration." Another variant of the technology involves tiny circuit boards that can be inserted in a laptop computer — either in the field or when they are shipped from manufacturers — so that the computer is broadcasting to the N.S.A. even while the computer's user enjoys the false confidence that being walled off from the Internet constitutes real protection.

The relay station it communicates with, called Nightstand, fits in an oversize briefcase, and the system can attack a computer "from as far away as eight miles under ideal environmental conditions." It can also insert packets of data in milliseconds, meaning that a false message or piece of programming can outrace a real one to a target computer. Similar stations create a link between the target computers and the N.S.A., even if the machines are isolated from the Internet.

Computers are not the only targets. Dropoutjeep attacks iPhones. Other hardware and software are designed to infect large network servers, including those made by the Chinese.

Most of those code names and products are now at least five years old, and they have been updated, some experts say, to make the United States less dependent on physically getting hardware into adversaries' computer systems.

The N.S.A. refused to talk about the documents that contained these descriptions, even after they were published in Europe.

"Continuous and selective publication of specific techniques and tools used by N.S.A. to pursue legitimate foreign intelligence targets is detrimental to the security of the United States and our allies," Ms. Vines, the N.S.A. spokeswoman, said.

But the Iranians and others discovered some of those techniques years ago. The hardware in the N.S.A.'s catalog was crucial in the cyberattacks on Iran's nuclear facilities, code-named Olympic Games, that began around 2008 and proceeded through the summer of 2010, when a technical error revealed the attack software, later called Stuxnet. That was the first major test of the

technology.

One feature of the Stuxnet attack was that the technology the United States slipped into Iran's nuclear enrichment plant at Natanz was able to map how it operated, then "phone home" the details. Later, that equipment was used to insert malware that blew up nearly 1,000 centrifuges, and temporarily set back Iran's program.

But the Stuxnet strike does not appear to be the last time the technology was used in Iran. In 2012, a unit of the Islamic Revolutionary Guards Corps moved a rock near the country's underground Fordo nuclear enrichment plant. The rock exploded and spewed broken circuit boards that the Iranian news media described as "the remains of a device capable of intercepting data from computers at the plant." The origins of that device have never been determined.

On Sunday, according to the semiofficial Fars news agency, Iran's Oil Ministry issued another warning about possible cyberattacks, describing a series of defenses it was erecting — and making no mention of what are suspected of being its own attacks on Saudi Arabia's largest oil producer.

A version of this article appears in print on January 15, 2014, on page A1 of the New York edition with the headline: N.S.A. Devises Radio Pathway Into Computers.