Cyber-intruder sparks response, debate

washingtonpost.com /national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html

By Ellen Nakashima

The first sign of trouble was a mysterious signal emanating from deep within the U.S. military's classified computer network. Like a human spy, a piece of covert software in the supposedly secure system was "beaconing" — trying to send coded messages back to its creator.

An elite team working in a windowless room at the National Security Agency soon determined that a rogue program had infected a classified network, kept separate from the public Internet, that harbored some of the military's most important secrets, including battle plans used by commanders in Afghanistan and Iraq.

The government's top cyberwarriors couldn't immediately tell who created the program or why, although they would come to suspect the Russian intelligence service. Nor could they tell how long it had been there, but they soon deduced the ingeniously simple means of transmission, according to several current and former U.S. officials. The malicious software, or malware, caught a ride on an everyday thumb drive that allowed it to enter the secret system and begin looking for documents to steal. Then it spread by copying itself onto other thumb drives.

Pentagon officials consider the incident, discovered in October 2008, to be the most serious breach of the U.S. military's classified computer systems. The response, over the past three years, transformed the government's approach to cybersecurity, galvanizing the creation of a new military command charged with bolstering the military's computer defenses and preparing for eventual offensive operations. The efforts to neutralize the malware, through an operation code-named Buckshot Yankee, also demonstrated the importance of computer espionage in devising effective responses to cyberthreats.

But the breach and its aftermath also have opened a rare window into the legal concerns and bureaucratic tensions that affect military operations in an arena where the United States faces increasingly sophisticated threats. Like the running debates over the use of drones and other evolving military technologies, rapid advances in computing capability are forcing complex deliberations over the appropriate use of new tools and weapons.

This article, which contains previously undisclosed information on the extent of the infection, the nature of the response and the fractious policy debate it inspired, is based on interviews with two dozen current and former U.S. officials and others with knowledge of the operation. Many of them assert that while the military has a growing technical capacity to operate in cyberspace, it lacks authority to defend civilian networks effectively.

"The danger is not so much that cyber capabilities will be used without warning by some crazy general," said Stewart A. Baker, a former NSA general counsel. "The real worry is they won't be used at all because the generals don't know what the rules are."

A furious investigation

The malware that provoked Buckshot Yankee had circulated on the Internet for months without causing alarm, as just one threat among many. Then it showed up on the military computers of a NATO government in June 2008, according to Mikko Hypponen, chief research officer of a Finnish firm that analyzed the intruder.

He dubbed it "Agent.btz," the next name in a sequence used at his company, F-Secure. "Agent.bty" was taken.

Four months later, in October 2008, NSA analysts discovered the malware on the Secret Internet Protocol Router Network, which the Defense and State departments use to transmit classified material but not the nation's most sensitive information. Agent.btz also infected the Joint Worldwide Intelligence Communication System, which carries top-secret information to U.S. officials throughout the world.

Such networks are typically “air-gapped” — physically separated from the free-for-all of the Internet, with its countless varieties of malicious code, such as viruses and worms, created to steal information or damage systems. Officials had long been concerned with the unauthorized removal of classified material from secure networks; now malware had gotten in and was attempting to communicate to the broader Internet.

One likely scenario is that an American soldier, official or contractor in Afghanistan — where the largest number of infections occurred — went to an Internet cafe, used a thumb drive in an infected computer and then inserted the drive in a classified machine. “We knew fairly confidently that the mechanism had been somebody going to a kiosk and doing something they shouldn’t have as opposed to somebody who had been able to get inside the network,” one former official said.

Once a computer became infected, any thumb drive used on the machine acquired a copy of Agent.btz, ready for propagation to other computers, like bees carrying pollen from flower to flower. But to steal content, the malware had to communicate with a master computer for instructions on what files to remove and how to transmit them.

These signals, or beacons, were first spotted by a young analyst in the NSA’s Advanced Networks Operations (ANO) team, a group of mostly 20- and 30-something computing experts assembled in 2006 to hunt for suspicious activity on the government’s secure networks. Their office was a nondescript windowless room in Ops1, a boxy, low-rise building on the 660-acre campus of the NSA.

ANO’s operators are among 30,000 civilian and military personnel at NSA, whose main mission is to collect foreign communications intelligence on enemies abroad. The agency is forbidden to gather intelligence on Americans or on U.S. soil without special authorization from a court whose proceedings are largely secret.

NSA, whose employees hold 800 PhDs in mathematics, science and engineering, is based at Fort Meade, an Army base between Baltimore and Washington that has the world’s largest collection of supercomputers as well as its own police force and silicon-chip plant.

The ANO operators determined that the breach was serious after a few days of furious investigation. On the afternoon of Friday, Oct. 24,Richard C. Schaeffer Jr., then the NSA’s top computer systems protection officer, was in an agency briefing with President George W. Bush, who was making his last visit to the NSA before leaving office. An aide handed Schaeffer a note alerting him to the breach.

At 4:30 p.m., Schaeffer entered the office of Gen. Keith Alexander, the NSA director and a veteran military intelligence officer.

Alexander recalled that Schaeffer minced no words. “We’ve got a problem,” he said.

Permanent slumber

That evening, NSA officials briefed top levels of the U.S. government: the chairman of the Joint Chiefs of Staff, the deputy defense secretary and senior congressional leaders, telling them about the incident.

Working through the night, the ANO operators pursued a potential fix. Since Agent.btz was beaconing out in search of instructions, perhaps they could devise a way to order the malware to shut itself down. The next morning, in a room strewn with empty pizza boxes and soda cans, they sketched out their plan on a white board. But before it could be put into action, the NSA team had to make sure it would not affect the performance of other software, including the programs that battlefield commanders use for intelligence and communications. They needed to run a test.

“Our objective,” recalled Schaeffer, “was first, do no harm.”

That afternoon, the team members loaded a computer server into a truck and drove it to a nearby office of the

Defense Information Systems Agency, which operates the department's long-haul telecommunications and satellite networks.

At 2:30 p.m. they activated a program designed to recognize the beaconing of Agent.btz and respond. Soon after, the malware on the test server fell into permanent slumber.

Devising the technical remedy was only the first step. Defeating the threat required neutralizing Agent.btz everywhere it had spread on government networks, a grueling process that involved isolating individual computers, taking them offline, cleaning them, and reformatting hard drives.

A key player in Buckshot Yankee was NSA's Tailored Access Operations (TAO), a secretive unit dating to the early 1990s that specialized in intelligence operations overseas focused on gathering sensitive technical information. These specialists ventured outside the military's networks to look for Agent.btz in a process called "exploitation" or electronic spying.

The TAO identified new variants of the malware and helped network defenders prepare to neutralize them before they infected military computers.

"It's the ability to look outside our wire," said one military official.

Officials debated whether to use offensive tools to neutralize the malware on non-military networks, including those in other countries. The military's offensive cyber unit, Joint Functional Component Command — Network Warfare, proposed some options for doing so.

Senior officials rejected them on the grounds that Agent.btz appeared to be an act of espionage, not an outright attack, and didn't justify such an aggressive response, according to those familiar with the conversations.

As the NSA worked to neutralize Agent.btz on its government computers, Strategic Command, which oversees deterrence strategy for nuclear weapons, space and cyberspace, raised the military's information security threat level. A few weeks later, in November, an order went out banning the use of thumb drives across the Defense Department worldwide. It was the most controversial order of the operation.

Agent.btz had spread widely among military computers around the world, especially in Iraq and Afghanistan, creating the potential for major losses of intelligence. Yet the ban generated backlash among officers in the field, many of whom relied on the drives to download combat imagery or share after-action reports.

The NSA and the military investigated for months how the infection occurred. They retrieved thousands of thumb drives, many of which were infected. Much energy was spent trying to find "Patient Zero," officials said. "It turned out to be too complicated," said one. "We could never bring it down to as clear as . . . 'that's the thumb drive.' "

The rate of new infections finally subsided in early 2009. Officials say no evidence emerged that Agent.btz succeeded in communicating with a master computer or in putting secret documents in enemy hands. The ban on thumb drives has been partially lifted because other security measures have been put in place.

'A great catalyst'

Buckshot Yankee bolstered the argument for creating Cyber Command, a new unit designed to protect the military's computer and communications systems. It gave NSA Director Alexander the platform to press the case, advocated by others, that the new command should be able to use the NSA's capabilities to obtain foreign intelligence to defend the military's systems.

"It was a great catalyst," said Alexander, although the effort later faced questions about whether the head of the largest and most secretive intelligence agency should also lead the new organization.

The new organization, which has a staff of 750 and a budget of $155 million, brings together the Joint Task Force-Global Network Operations, which carried out the bulk of the cleanup work under Buckshot Yankee, and the Network Warfare unit, the military's offensive cyber arm. It began full operations on Oct. 31, 2010, with Alexander as its head.

But the creation of Cyber Command did not resolve several key debates over the national response to cyberthreats. Agent.btz provoked renewed discussion among senior officials at the White House and key departments about how to best protect critical private-sector networks.

Some officials argued that the military was better equipped than the Department of Homeland Security to respond to a major destructive attack on a power grid or other critical system, but others disagreed.

"Cyber Command and [Strategic Command] were asking for way too much authority" by seeking permission to take "unilateral action . . . inside the United States," said Gen. James E. Cartwright Jr., who retired as vice chairman of the Joint Chiefs in August.

Officials also debated how aggressive military commanders can be in defending their computer systems.

"You have the right of self-defense, but you don't know how far you can carry it and under what circumstances, and in what places," Cartwright said. "So for a commander who's out there in a very ambiguous world looking for guidance, if somebody attacks them, are they supposed to run? Can they respond?"

Questions over the role of offense in cybersecurity deterrence began in the 1990s, if not earlier, said Martin Libicki, a Rand Corp. cyberwarfare expert. One reason it is so difficult to craft rules, he said, is the tendency to cast cyberwar as "good, old-fashioned war in yet another domain." Unlike conventional and nuclear warfare, cyberattacks generally are enabled only by flaws in the target system, he said.

Another reason it is so difficult, said James A. Lewis, a senior fellow at the Center for Strategic and International Studies, is the overlap between cybersecurity operations and the classified world of intelligence.

"The link to espionage is where the nuclear precedent breaks down and makes cyber closer to covert operations," Lewis said.

By the summer of 2009, Pentagon officials had begun work on a set of rules of engagement, part of a broader cyberdefense effort called Operation Gladiator Phoenix. They drafted an "execute order" under which the Strategic and Cyber commands could direct the operations and defense of military networks anywhere in the world. Initially, the directive applied to critical privately owned computer systems in the United States.

Several conditions had to be met, according to a military official familiar with the draft order. The provocation had to be hostile and directed at the United States, its critical infrastructure or citizens. It had to present the imminent likelihood of death, serious injury or damage that threatened national or economic security. The response had to be coordinated with affected government agencies and combatant commanders. And it had to be limited to actions necessary to stop the attack, while minimizing impacts on non-military computers.

"Say someone launched an attack on the U.S. from a known Chinese army computer — a known hostile computer," the official said. "You could maybe disable the computer, but you're not talking about making it explode and killing somebody."

Turf battles

But the effort to create such comprehensive rules of engagement foundered, said current and former officials with direct knowledge of the policy debate.

The Justice Department feared setting a legal precedent for military action in domestic networks. The CIA resisted letting the military infringe on its foreign turf. The State Department worried the military would accidentally disrupt a

server in a friendly country without seeking consent, undermining future cooperation. The Department of Homeland Security, meanwhile, worked to keep its lead role in securing the nation against cyberthreats.

The debate bogged down over how far the military could go to parry attacks, which can be routed from server to server, sometimes in multiple countries. “Could you go only to the first [server] you trace back to? Could you go all the way to the first point at which the attack emanated from? Those were the questions that were still being negotiated,” said a former U.S. official.

The questions were even more vexing when it came to potentially combating an attack launched from servers within the United States. The military has no authority to act in cyberspace when the networks are domestic — unless the operation is on its own systems.

In October 2010, Pentagon officials signed an agreement with the Department of Homeland Security pledging to work to enhance the nation’s cybersecurity. But in speeches, Alexander, the head of Cyber Command, has suggested that more needs to be done.

“Right now, my mission as commander of U.S. Cyber Command is to defend the military networks,” he said in an April speech in Rhode Island. “I do not have the authority to look at what’s going on in other government sectors, nor what would happen in critical infrastructure. That right now falls to DHS. It also means that I can’t stop it, or at network speed . . . see what’s happening to it. What we do believe, though, is that that needs to be accounted for. We have to have a way to protect our critical infrastructure.”

Homeland Security Secretary Janet Napolitano, in a speech in California that same month, made her preference clear. “At DHS, we believe cyberspace is fundamentally a civilian space.”

The execute order was signed in February. The standing rules of engagement limit the military to the defense of its own networks and do not allow it to go outside them without special permission from the president.

The next vulnerability?

Almost from the beginning, U.S. officials suspected that Russia’s spy service created Agent.btz to steal military secrets. In late 2008, Russia issued a denunciation of the allegation, calling it “groundless” and “irresponsible.”

Former officials say there is evidence of a Russian role in developing the malware, but some doubt whether the spy service created Agent.btz to infiltrate U.S. military computers.

Some say it could have been a product of Russia’s sophisticated mafia, with its extensive computer expertise, to collect all sorts of protected records worth stealing — or selling to the highest bidder. Or there could have been Russian involvement in one phase of the malware’s development before it was adapted by others. Others say they have no doubt that it was intentionally aimed at the Defense Department. New versions of Agent.btz continue to appear, years after it was discovered.

What is clear is that Agent.btz revealed weaknesses in crucial U.S. government computer networks — vulnerabilities based on the weakest link in the security chain: human beings. The development of new defenses did not prevent the transfer of massive amounts of information from one classified network to the anti-secrecy group WikiLeaks, an act that the government charges was carried out by an Army intelligence analyst.

NSA analysts know how to neutralize Agent.btz and its variants, but no one knows when the next vulnerability will be discovered or what kind of intrusion might ensue.

Richard “Dickie” George, who was the NSA information assurance technical director until his retirement this year, said that in the early days of Operation Buckshot Yankee, a four-star general asked when the danger from Agent.btz would pass and heightened security measures could end.

“We had to break the news to him,” George recalled, “that this is never going to be over.”

Staff researcher Julie Tate contributed to this report.