Hacking The Hill

HOW THE CHINESE -- OR SOMEONE -- HACKED INTO HOUSE OF REPRESENTATIVES COMPUTERS IN 2006, AND WHAT IT WILL TAKE TO KEEP OUT THE NEXT ELECTRONIC INVADER.

Saturday, Dec. 20, 2008
by Shane Harris

On October 26, 2006, computer security personnel from across the legislative branch were informed that the Congressional Budget Office had been hit with a computer virus. The news might not have seemed extraordinary. Hackers had been trying for years to break into government computers in Congress and the executive branch, and some had succeeded, making off with loads of sensitive information ranging from codes for military aircraft schedules to design specifications for the space shuttle.

Employees in the House of Representatives' Information Systems Security Office, which monitors the computers of all members, staffers, and committee offices, had learned to keep their guard up. Every year of late, they have fended off more than a million hacking attempts against the House and removed any computer viruses that made it through their safeguards. House computers relay sensitive information about members and constituents, and committee office machines are especially loaded with files pertaining to foreign policy, national security, and intelligence. The security office took the information from the CBO attack and scanned the House network to determine whether any machines had been compromised in a similar fashion.

They found one. A computer in one member's office matched the profile of the CBO incident. The virus seemed to be contacting Internet addresses outside the House, probably other infected computers or servers, to download malicious files into the House system. According to a confidential briefing on the investigation prepared by the security office and obtained by *National Journal,* security employees contacted the member's office and directed staffers to disconnect the computer from the network. The briefing does not identify the member of Congress.

Apparently worried that the virus could have already infected other machines, security personnel met with aides from the member's office and examined the computer. They confirmed that a virus had been placed on the machine. The member's office then called the FBI, which employs a team of cyber-forensic specialists to investigate hackings. The House security office made a copy of the hard drive and gave it to the bureau.

> "Somebody with a wireless device in China should expect it to be compromised while he's there." ***-- Joel Brenner***

Upon further analysis, the security office found more details about the nature and possible intent of the hack. The machine was infected with a file that sought out computers outside the House system to retrieve "malware," malicious or destructive

programs designed to spy on the infected computer's user or to clandestinely remove files from the machine. This virus was designed to download programs that tracked what the computer user typed in e-mail and instant messages, and to remove documents from both the hard drive and a network drive shared by other House computers. As an example of the virus's damage, the security office briefing cited one House machine on which "multiple compressed files on multiple days were created and exported." An unknown source was stealing information from the computer, and the user never knew it.

Armed with this information about how the virus worked, the security officers scanned the House network again. This time, they found more machines that seemed to match the profile -- they, too, were infected. Investigators found at least one infected computer in a member's district office, indicating that the virus had traveled through the House network and may have breached machines far away from Washington.

Eventually, the security office determined that eight members' offices were affected; in most of the offices, the virus had invaded only one machine, but in some offices, it hit multiple computers. It also struck seven committee offices, including Commerce; Transportation and Infrastructure; Homeland Security; and Ways and Means; plus the Commission on China, which monitors human rights and laws in China. Most of the committee offices had one or two infected computers. In the International Relations Committee (now the Foreign Affairs Committee) office, however, the virus had compromised 25 computers and one server.

The House security office contacted the committees' employees and all of the members' offices, and removed the infected computers and servers. The House's technical-support center sent an advisory to all systems administrators, reminding them of safe computing practices, such as not opening links in e-mails from unknown sources. The House security office determined that whoever infected the machines had probably tricked users into visiting a website or clicking on a link in an e-mail or instant message that downloaded an infectious file; the virus then exploited as many of the computer's vulnerabilities that it could detect. A diagram in the security briefing shows how the virus, once it penetrated the computer, made multiple attempts to download different kinds of malicious software.

The hacker or hackers -- it's unclear whether more than one was involved -- attempted to evade detection by using an array of attack methods and downloading malicious files from various Internet addresses. The hacker was likely using many other infected machines as launching pads, making it essentially impossible to stop the attacks completely and exceptionally difficult to know where the hacker was located. It's relatively easy for an attacker to mask his or her location by communicating through layers of infected computers and servers around the world.

The confidential briefing does not say where the hacker was, nor does it attribute the attack to a particular group or country. Such information is notoriously difficult for investigators to ascertain. But according to some members of Congress whose machines were infected, the attack described in the briefing emanated from China and

was probably designed to steal sensitive information from lawmakers' and committee offices.

Chinese Traces

That allegation and others about Chinese cyber-espionage lie at the heart of a simmering controversy over Chinese or China-supported hacking of U.S. government computer systems. As *National Journal* **reported earlier this year**, computer hackers, who several investigators and senior government officials believe are based in China and sometimes work on the Chinese government's behalf, have penetrated deeply into the information systems of U.S. corporations and government agencies.

The hackers have reportedly stolen proprietary information from executives and even one Cabinet secretary in advance of business meetings in China. Some sources contend, moreover, that Chinese hackers may have played a role in two major power outages in the United States. Power companies and outside investigators call such allegations demonstrably untrue, but many cyber-security professionals express considerable anxiety about the vulnerability of U.S. networks.

Concern about China is so great that, only hours before the opening ceremonies of the Olympic Games in Beijing last summer, the United States' top counterintelligence official, Joel Brenner, warned American visitors to leave their cellular phones and wireless handheld computers at home. "Somebody with a wireless device in China should expect it to be compromised while he's there," Brenner said on CBS News. "The public security services in China can turn your telephone on and activate its microphone when you think it's off." For those who were required or determined to take their electronic equipment, Brenner advised that they remove the batteries when they were not using the device.

Chinese sources were at the root of the hack on members of Congress in 2006, according to some lawmakers. In an interview with *National Journal* last summer, Rep. Mark Kirk, R-Ill., said that the virus described in the House's confidential briefing had infected a machine in his office. House security personnel informed him of the infection, Kirk said, and he called the FBI.

Kirk then co-chaired the House U.S.-China Working Group, whose members had met with 11 Chinese business leaders less than a year earlier to discuss bilateral trade issues. The group has held monthly meetings to foster a diplomatic dialogue between Chinese and U.S. officials. Kirk said that his office's infected computer was trying to contact Internet addresses that "eventually resolved themselves in China." He hastened to add, "Obviously, you don't know who is the real owner or operator of the [Internet] address."

"On these computers was information about all of the casework I have done on behalf of political dissidents and human-rights activists around the world." ***-- Frank Wolf***

The breach could be viewed through one of two lenses, Kirk said. "The bad view" is that Chinese intelligence sources were trying to spy on a member of Congress. The "good view" holds that Chinese citizens, who read about the commission's work in the media, hacked Kirk's computer out of frustration or retribution. But this attack profile, Kirk said, "looked toward the criminal side."

"Hacking into a congressional computer is a serious offense," he said. Although Kirk said he didn't know what files, if any, the hacker had pilfered, he assumed that the intruder wasn't looking for information about Kirk's constituents in Illinois. He concluded that the hacker was more interested in his China policy. "At that point," Kirk said, "it seemed what we had was a case of overseas espionage."

This past June, Rep. Frank Wolf, a Republican from Northern Virginia, took to the House floor and announced that four of his office's computers "were compromised by an outside source."

"On these computers," he said, "was information about all of the casework I have done on behalf of political dissidents and human-rights activists around the world." Wolf is an outspoken critic of China's human-rights policies.

"That kind of information, as well as everything else on my office computers -- e-mails, memos, correspondence, and district casework -- was open for outside eyes to see," Wolf said. And then, without naming names, he added, "Several other members were similarly compromised."

Wolf said he had met with staff from the House Information Resources office and with FBI officials. "It was revealed," he said, "that the outside sources responsible for this attack came from within the People's Republic of China." A spokesperson for Wolf told *NJ* that the intrusion he spoke of on the House floor is the same attack described in the confidential briefing obtained by *National Journal* and prepared by the House information security office. That briefing states that Wolf was one of the eight members affected, and that four of his machines were hit -- the same number that Wolf cited publicly. In his floor remarks, Wolf said that his computers were found to have been compromised in August 2006, two months before the House Information Systems Security Office scanned the network for possible infections.

Keeping It Secret

The pervasive nature of the 2006 attack begs a question: Why didn't members of Congress publicly disclose these breaches sooner? Wolf offered one answer.

"Despite everything we read in the press, our intelligence, law enforcement, national security, and diplomatic corps remain hesitant to speak out about this problem," Wolf said on the House floor. "Perhaps they are afraid that talking about this problem will reveal our vulnerability." He then added, "I have been urged not to speak out about this threat."

Wolf didn't say who urged him to remain silent. Kirk, whose office was also hit, said he spoke with Wolf before his remarks. Wolf wanted to publicly raise the issue of cyber-

security to bring more attention to the problem, Kirk said. Kirk was more interested in finding the culprits.

> "My objective was to get even with these guys and nail them. My objective was to tell the FBI as much detail as I can so we can go after them." ***-- Mark Kirk***

"My objective was to get even with these guys and nail them," he said. "My objective was to tell the FBI as much detail as I can so we can go after them."

In his speech, Wolf urged his colleagues to raise their level of awareness, and he exhorted the executive branch to open up. "I strongly believe that the appropriate officials, including those from the Department of Homeland Security and the FBI, should brief all members of Congress in a closed session regarding threats from China and other countries against the security of House technology, including our computers, BlackBerry devices, and phones," Wolf said.

Wolf's outspokenness met resistance, Kirk said. "I think a number of people came to Frank and said, 'Back off. Don't do this,' " Kirk said. He declined to say who had approached Wolf. But he said that "some parts of the government" favor keeping systems open to track attackers, but they aren't inclined to talk about it openly.

Both the intelligence community and the military use cyber-monitoring tools that are essentially the same as those directed against U.S. government systems. The Air Force, in particular, considers cyberspace to be a new battleground; the service has reportedly developed a formidable capacity to inflict damage on other nations' computers and electronic infrastructure.

Learning Curve

Many members of Congress, it seems, may also be uninterested in talking about their cyber-vulnerabilities -- not because they aren't concerned about them but because they don't understand them.

Wolf has said that in discussing the threat with colleagues, he has found that members don't realize their computers are tantalizing targets. One cyber-security expert says that Wolf is probably right but that members' ignorance doesn't mean they're indifferent.

"As a member of Congress, you have so many issues competing for your attention and, historically, cyber-security hasn't been one that's won out," said Amit Yoran, who was the first director of the National Cyber Security Division in the Homeland Security Department. "It's not an issue that is particularly well tracked by their constituents."

Moreover, Yoran said, lawmakers can also fall victim to their own demands. "In Congress, you've got an organization full of a lot of senior executives." Just as in the executive branch or in the private sector, members want to be treated like CEOs. They have "very high support requirements," Yoran said. Put another way, if members of Congress want their computers to access a certain website or run a particular program, they don't ask for technical support -- they demand it.

That mind-set makes it exceptionally difficult to protect congressional computers in a uniform fashion. The House and Senate could enact the strictest security policies imaginable, but if members and their aides ignore the policies or ask for exceptions, security degrades.

No one understands that better than the office in charge of protecting members' computers -- the House Information Systems Security Office. "I can say, comfortably, that the level and quality of expertise within the security department, the IT department, of the House, is very strong," Yoran said. "The Senate as well." The confidential briefing on the 2006 breach bolsters Yoran's assessment. It is clearly written and demonstrates that the security office understands the dynamic nature of cyber-intrusions.

Yoran emphasized, however, that between expertise and adequate security, "there's a lot of ground." Members and their staffers must decide whether to follow security procedures -- and perhaps too often, they don't want to be bothered.

Who Should Lead?

Congress is more than a tempting and sometimes easy target. Lawmakers also have oversight responsibility for the security of executive branch networks, and they make decisions that affect all U.S. telecommunications systems.

Members make the laws that set security policies and standards for government systems. They issue an annual report card and other assessments on how well the government is meeting those standards. Slowly but increasingly, lawmakers are writing statutes aimed at stiffening the penalties for computer intrusion and at defining hacking more clearly as a crime.

Yet Congress's repeated run-ins with cyber-thieves and hackers don't appear to have focused lawmakers' oversight efforts. Last week, the Center for Strategic and International Studies, the Washington think tank noted for its defense policy research, released a highly anticipated **cyber-security assessment** for President-elect Obama. The study group included experts from a range of disciplines and industries, and was co-chaired by two members of Congress: Reps. Jim Langevin, D-R.I., and Michael McCaul, R-Texas.

The report, a year in the making, is almost entirely devoted to cyber-security recommendations for the next president. It devotes only one page to Congress's role, perhaps with good reason. The panel essentially concludes that Congress cannot manage cyber-security.

The root of the problem, the report said, lies in Congress's inconsistent, almost feudal, approach to oversight. "The fragmentation of oversight complicates efforts to improve homeland security, and cyber-security shares in this problem," the authors wrote. The Homeland Security Department, which is responsible for securing civilian government networks, "has far too many oversight committees -- more than 80 -- exercising jurisdiction."

The CSIS study group discussed whether that jurisdiction should be streamlined, a simple enough task on the surface. House and Senate rules don't explicitly give

jurisdiction over cyber-issues to any committees, and congressional leaders could limit responsibility to a more manageable number of lawmakers. The study group certainly thought that was a good idea. "Without rules changes that provide clear jurisdiction, responsibility for investigation, oversight, and policy development in cyber-security will depend largely on member interest and the ability of committees to coordinate with each other," the report stated.

The study group stopped short of formally recommending that Congress take that step, however. In large measure, that's because the CSIS recommendations were meant for the president-elect, not the speaker of the House and the majority leader of the Senate. But the panel also concluded that cyber-security -- protecting critical networks not only from espionage but also from tampering and potential control by outsiders -- was of such importance and magnitude that only the president could take charge of it. Indeed, the authors titled their report "Securing Cyberspace for the 44th Presidency."

"The president could engage [congressional] leaders in a discussion to streamline jurisdiction," the report said, "but jurisdictional consolidation would not produce the immediate improvement in cyber-security that our other recommendations offer." The panel wants Obama to take charge of cyber-security and make the White House its political nerve center. It recommended that he create a new office for cyberspace in the Executive Office of the President that would work closely with the National Security Council, "managing the many aspects of securing our national networks while protecting privacy and civil liberties." Any attempt to broadly secure cyberspace will, by necessity, involve close scrutiny of the information traveling through it, including e-mails, instant messages, and, increasingly, telephone calls.

The study group also recommended that Obama appoint an assistant for cyberspace and establish a Cyber-Security Directorate in the NSC. To support that directorate, the experts recommended a National Office for Cyberspace, which would be directed by the president's cyber-assistant.

"The new administration has to take rapid action to improve cyber-security, and streamlining congressional jurisdiction isn't one of those actions," said James Lewis, a CSIS senior fellow and the director of its public policy program. He led the study group.

"The legislative process is deliberative," Lewis said. "It has to move at its own pace on questions like jurisdiction, but there are things the executive branch can and should do without waiting."