Exclusive: National Security Agency helps banks battle hackers

Andrea Shalal-Esa and Jim Finkle, Reuters

The National Security Agency, a secretive arm of the U.S. military, has begun providing Wall Street banks with intelligence on foreign hackers, a sign of growing U.S. fears of financial sabotage.

The assistance from the agency that conducts electronic spying overseas is part of an effort by American banks and other financial firms to get help from the U.S. military and private defense contractors to fend off cyber attacks, according to interviews with U.S. officials, security experts and defense industry executives.

The Federal Bureau of Investigation has also warned banks of particular threats amid concerns that hackers could potentially exploit security vulnerabilities to wreak havoc across global markets and cause economic mayhem.

While government and private sector security sources are reluctant to discuss specific lines of investigations, they paint worst-case scenarios of hackers ensconcing themselves inside a bank's network to disable trading systems for stocks, bonds and currencies, trigger flash crashes, initiate large transfers of funds or turn off all ATM machines.

It is unclear if hackers have ever been close to producing anything as dire, but the FBI says it has already helped banks avert several major cyber attacks by helping identify network vulnerabilities.

NSA Director Keith Alexander, who runs the U.S. military's cyber operations, told Reuters the agency is currently talking to financial firms about sharing electronic information on malicious software, possibly by expanding a pilot program through which it offers similar data to the defense industry. He did not provide further details on his agency's collaboration with banks.

Alexander said industry and government were making progress in protecting computer networks, but "tremendous vulnerabilities" remained. The four-star Army general noted companies that have suffered damage from hackers, such as Google Inc, Lockheed Martin Corp and Nasdaq OMX Group, had among the best security systems in the world.

"If they're getting exploited, what about the rest? We have to change that paradigm," Alexander said.

NSA, which has long been charged with protecting classified government networks from attack, is already working with Nasdaq to beef up its defenses after hackers infiltrated its computer systems last year and installed malicious software that allowed them to spy on the directors of publicly held companies. A Nasdaq

spokesman confirmed the investigation into the attack continues, but declined to give further details.

OFFICIALS WORRIED

Hackers have targeted Wall Street investment banks for more than a decade, but recent attacks have been more sophisticated, coordinated and deliberate.

That makes security experts suspect the hackers were backed by countries such as China, and fueled concerns that cyber terrorists might someday use malware to wipe out crucial data and cripple networks across the financial sector.

China has repeatedly said it does not condone hacking, but experts say the evidence continues to mount against Beijing. In June, Google blamed China for an attempt to steal the passwords of hundreds of email account holders, the second major breach the Internet giant has blamed on the Chinese.

Earlier this year, security firm McAfee said hackers working in China broke into the computer systems of five global oil and gas companies to steal bidding plans and other critical proprietary information.

"We know adversaries have full unfettered access to certain networks," Shawn Henry, executive assistant director of the FBI, said without identifying the adversaries.

"Once there, they have the ability to destroy data," he said in an interview. "We see that as a credible threat to all sectors, but specifically the financial services sector."

The FBI has helped banks avert several potential attacks by alerting them to vulnerabilities in their computer networks, and by flagging possible hackers before they struck, he said.

Security experts interviewed by Reuters declined to identify any banks that may have data compromised, citing promises of confidentiality to clients, colleagues and employers that they would not to discuss the matter publicly.

Representatives of Wall Street's biggest banks including Bank of America Corp, Citigroup Inc, Goldman Sachs Group Inc and JPMorgan Chase & Co either declined to discuss security issues or were not available to comment.

TREASURE TROVE OF DATA

Former Deputy Defense Secretary William Lynn said cyber attacks could prove particularly devastating for financial institutions given the critical importance of the data stored on their networks and the need to maintain investor confidence in their security.

"You can't do transactions if you don't have reliable data," Lynn, who spearheaded the Pentagon's national cyber strategy released this summer, said in an interview.

He said more than 100 countries already have some hacking capabilities, and such tools could soon be available to rogue groups.

"You ultimately have to worry about terrorist groups gaining those capabilities, either by developing them themselves or just buying them on the open market," said Lynn, who retired earlier this month.

The NSA's work with Wall Street marks a milestone in the agency's efforts to make its cyber intelligence available more broadly to the private sector. For years, the spy agency kept such a low profile that some joked that its name stood for "No Such Agency" or "Never Say Anything."

Greater cooperation with industry became possible after a deal reached a year ago between the Pentagon and the Department of Homeland Security, allowing NSA to provide cyber expertise to other government agencies and certain private companies.

Several people familiar with the NSA's assistance to Wall Street said the agency only gets involved when banks specifically ask for its help, so as not to violate laws that restrict its ability to operate within U.S. borders. These institutions get warnings about potential attacks and can ask questions on specific problems.

The NSA and big arms makers have a treasure trove of data on hacking, including intelligence on planned attacks and libraries of malicious software code used by foreign-government supported hackers that are not available elsewhere.

Such intelligence can be "gold" to a bank's security staff, said Shane Sims, a director in the forensics practice of PricewaterhouseCoopers.

"You can cash it in," said Sims, who is investigating attacks on several banks believed to be orchestrated by foreign governments. "It just allows you to turn your environment into an early warning system so you can intercede and take action before information goes out the door."

Banks need help from the NSA because they cannot keep up with increasingly sophisticated attacks just by using technology from traditional software security firms, experts say.

About eight out of ten Wall Street firms have been infiltrated by foreign-government backed hackers, according to Tom Reilly, who helps investment banks fight hackers in his role as the head of Hewlett-Packard Co's security business.

Hemanshu Nigam, a former federal prosecutor and cyber security expert, said enemy states could launch a cyber assault when their targets were particularly vulnerable. This could be during a major crisis, such as the financial crisis in 2008, the euro zone crisis now, or at the time of a key event such as the U.S. loss of its triple-A credit rating this summer.

Investors are already worried about how quickly markets can meltdown, as trading is almost completely electronic and reliant on hair-trigger software. The Dow Jones industrial average crashed nearly 700 points in about five minutes on May 6, 2010, an unprecedented plunge that regulators said was exacerbated by algorithmic trading, panic and vacuums of liquidity.

"What you're seeing is something that can cause a global tidal wave," said the cybersecurity expert Nigam, who had worked for News Corp and Microsoft Corp.

BANKS ALSO CONSULTING DEFENSE FIRMS

The NSA first started to worry about security of financial institutions about two years ago, and has held meetings with the Federal Reserve Bank of New York and banks to address those concerns, according to Jim Lewis, a cyber expert with the Center for Strategic and International Studies, a Washington-based think tank.

The New York Fed declined comment.

Lewis pointed the finger at China as a consistent threat. "Business espionage is a normal practice for Chinese businesses and for (government) agencies," he said.

U.S. financial institutions have also sought assistance from private defense contractors that help the U.S. government build cyber weapons and tools for defending military networks.

Companies such as Lockheed, General Dynamics Corp, Boeing Co, Northrop Grumman Corp and Raytheon Co are now competing with traditional security vendors to serve corporate America, including banks.

Defense industry executives say big Wall Street firms are asking arms makers for help in locking down critical data, including the algorithms used for trading shares, currencies and commodities.

"Other sectors are becoming increasingly concerned about such attacks and want to learn more about how we protect our data," said one defense industry executive, whose company has already worked with power companies and is now negotiating agreements with several major financial firms.

Earlier this year, the hacking of EMC Corp's RSA security division underscored the growing sophistication of hackers. RSA provides SecurID keys used by companies all over the world.

The hackers, likely backed by a foreign government, used data from the RSA breach, coupled with personal identifying information gleaned from other attacks, to break into Lockheed's computer networks.

Erin Nealy Cox, a former U.S. federal computer crimes prosecutor, said she tells banks that it's only a matter of time before their systems are breached.

"Our advice to our clients is -- it's not a matter of if, it's a matter of when," said Nealy Cox, managing director at Stroz Friedberg LLC. "We don't want to give anybody a false sense of security." (Reporting by Andrea Shalal-Esa and Jim Finkle, additional reporting by Tim McLaughlin in Boston, and Diane Bartz in Washington. Editing by Tiffany Wu and Martin Howell)