Special Report: U.S. cyberwar strategy stokes fear of blowback

www.reuters.com /article/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510

By Joseph Menn | WASHINGTON

WASHINGTON Even as the U.S. government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.

The strategy is spurring concern in the technology industry and intelligence community that Washington is in effect encouraging hacking and failing to disclose to software companies and customers the vulnerabilities exploited by the purchased hacks.

That's because U.S. intelligence and military agencies aren't buying the tools primarily to fend off attacks. Rather, they are using the tools to infiltrate computer networks overseas, leaving behind spy programs and cyber-weapons that can disrupt data or damage systems.

The core problem: Spy tools and cyber-weapons rely on vulnerabilities in existing software programs, and these hacks would be much less useful to the government if the flaws were exposed through public warnings. So the more the government spends on offensive techniques, the greater its interest in making sure that security holes in widely used software remain unrepaired.

Moreover, the money going for offense lures some talented researchers away from work on defense, while tax dollars may end up flowing to skilled hackers simultaneously supplying criminal groups. "The only people paying are on the offensive side," said Charlie Miller, a security researcher at Twitter who previously worked for the National Security Agency.

A spokesman for the NSA agreed that the proliferation of hacking tools was a major concern but declined to comment on the agency's own role in purchasing them, citing the "sensitivity" of the topic.

America's offensive cyber-warfare strategy - including even the broad outlines and the total spending levels - is classified information. Officials have never publicly acknowledged engaging in offensive cyber-warfare, though the one case that has been most widely reported - the use of a virus known as Stuxnet to disrupt Iran's nuclear-research program - was lauded in Washington. Officials confirmed to Reuters previously that the U.S. government drove Stuxnet's development, and the Pentagon is expanding its offensive capability through the nascent Cyber Command.

Stuxnet, while unusually powerful, is hardly an isolated case. Computer researchers in the public and private sectors say the U.S. government, acting mainly through defense contractors, has become the dominant player in fostering the shadowy but large-scale commercial market for tools known as exploits, which burrow into hidden computer vulnerabilities.

In their most common use, exploits are critical but interchangeable components inside bigger programs. Those programs can steal financial account passwords, turn an iPhone into a listening device, or, in the case of Stuxnet, sabotage a nuclear facility.

Think of a big building with a lot of hidden doors, each with a different key. Any door will do to get in, once you find the right key.

The pursuit of those keys has intensified. The Department of Defense and U.S. intelligence agencies, especially the NSA, are spending so heavily for information on holes in commercial computer systems, and on exploits taking advantage of them, that they are turning the world of security research on its head, according to longtime researchers and former top government officials.

Many talented hackers who once alerted companies such as Microsoft Corp to security flaws in their products are now selling the information and the exploits to the highest bidder, sometimes through brokers who never meet the final buyers. Defense contractors and agencies spend at least tens of millions of dollars a year just on exploits, which are the one essential ingredient in a broader cyber-weapons industry generating hundreds of millions annually, industry executives said privately.

Former White House cybersecurity advisors Howard Schmidt and Richard Clarke said in interviews that the government in this way has been putting too much emphasis on offensive capabilities that by their very nature depend on leaving U.S. business and consumers at risk.

"If the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users," Clarke said. "There is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn't."

Acknowledging the strategic trade-offs, former NSA director Michael Hayden said: "There has been a traditional calculus between protecting your offensive capability and strengthening your defense. It might be time now to readdress that at an important policy level, given how much we are suffering."

The issue is sensitive in the wake of new disclosures about the breadth and scale of hacking attacks that U.S. intelligence officials attribute to the Chinese government. Chinese officials deny the allegations and say they too are hacking victims.

Top U.S. officials told Congress this year that poor Internet security has surpassed terrorism to become the single greatest threat to the country and that better information-sharing on risks is crucial. Yet neither of the two major U.S. initiatives under way - sweeping cybersecurity legislation being weighed by Congress and President Barack Obama's February executive order on the subject - asks defense and intelligence agencies to spread what they know about vulnerabilities to help the private sector defend itself.

Most companies, including Microsoft, Apple Inc and Adobe Systems Inc, on principle won't pay researchers who report flaws, saying they don't want to encourage hackers. Those that do offer "bounties", including Google Inc and Facebook Inc, say they are hard-pressed to compete financially with defense-industry spending.

Some national-security officials and security executives say the U.S. strategy is perfectly logical: It's better for the U.S. government to be buying up exploits so that they don't fall into the hands of dictators or organized criminals.

UNINTENDED CONSEQUENCES

When a U.S. agency knows about a vulnerability and does not warn the public, there can be unintended consequences. If malign forces purchase information about or independently discover the same hole, they can use it to cause damage or to launch spying or fraud campaigns before a company like Microsoft has time to develop a patch. Moreover, when the U.S. launches a program containing an exploit, it can be detected and quickly duplicated for use against U.S. interests before any public warning or patch.

Some losses occur even after a patch.

That happened to Microsoft and its customers with a piece of malicious software known as Duqu. Experts say it was designed to steal industrial-facility designs from Iran and that it used an exploit that tricked computers into installing malicious software disguised as a font to render type on the screen.

Those who dissected the program after its discovery in 2011 believe it was created by a U.S. agency. Though Duqu resembled Stuxnet in some respects, they couldn't say for sure how it was assembled, or whether the spying tool had accomplished its mission.

What's certain is that criminal hackers copied Duqu's previously unheard-of method for breaking into computers and rolled it into "exploit kits," including one called Blackhole and another called Cool, that were sold to hackers worldwide.

Microsoft had by then issued a patch for the vulnerability. Nevertheless, hackers used it last year to attack 16 out of every 1,000 U.S. computers and an even greater proportion in some other countries, according to Finland-based security firm F-Secure.

The flaw became the second-most frequently tried among tens of thousands of known vulnerabilities during the second half of 2012, F-Secure said. Hackers installed a variety of malicious software in cases when the exploit worked, including copies of Zeus, a notorious program for stealing financial login information that has been blamed for hundreds of millions of dollars in bank thefts. Microsoft won't say whether it has confronted U.S. officials about Duqu and other programs, but an executive said the company objects "to our products being used for malicious purposes."

THE BUSINESS OF "ZERO-DAYS"

Former NSA Director Hayden and others with high-level experience have boasted that U.S. offensive capabilities in cyberspace are the best in the world. But few outsiders had any idea what was possible before 2010, when a small laboratory discovered the worm called Stuxnet.

It took teams of security experts in several countries months to dissect the program. They discovered that it had been meticulously engineered to launch invisibly from a portable flash drive and spread through connected Windows-based personal computers in search of machines running a specific piece of industrial control software made by Siemens AG of Germany.

If Stuxnet found that software and a certain configuration, it changed some of the instructions in the program and hid its tracks. Eventually, the truth came out: The only place deliberately affected was an Iranian nuclear facility, where the software sped up and slowed down uranium-enriching centrifuges until they broke.

Stuxnet was unique in many ways, one of them being that it took advantage of four previously unknown flaws in Windows. In the industry, exploits of such vulnerabilities are called "zero-days," because the software maker has had zero days' notice to fix the hole before the tool's discovery.

It can take months for security patches to be widely installed after a vulnerability is reported, so even a "two-day" exploit, one released two days after a warning, is valuable.

But exploits can't be counted on to work once the holes they rely on are disclosed. That means contractors are constantly looking for new ones that can be swapped in to a particular program after the original vulnerability is fixed. Some security firms sell subscriptions for exploits, guaranteeing a certain number per year.

"My job was to have 25 zero-days on a USB stick, ready to go," said a former executive at a defense contractor that bought vulnerabilities from independent hackers and turned them into exploits for government use.

HOW THE MARKET WORKS

Zero-day exploits will work even when the targeted software is up to date, and experts say the use of even a single zero-day in a program signals that a perpetrator is serious. A well-publicized hacking campaign against Google and scores of other companies in early 2010, attributed by U.S. officials and private experts to Chinese government

hackers, used one zero-day.

Many zero-day exploits appear to have been produced by intelligence agencies. But private companies have also sprung up that hire programmers to do the grunt work of identifying vulnerabilities and then writing exploit code. The starting rate for a zero-day is around $50,000, some buyers said, with the price depending on such factors as how widely installed the targeted software is and how long the zero-day is expected to remain exclusive.

It's a global market that operates under the radar, often facilitated by other companies that act as brokers. On the buy side are U.S. government agencies and the defense contractors that fold the exploits into cyber-weapons. With little or no regulation, it is impossible to say who else might be purchasing zero-days and to what end, but the customers are known to include organized crime groups and repressive governments spying on their citizens.

Even one of the four exploits used by Stuxnet may have been purchased. Swedish Defense Research Agency expert David Lindahl said the same trick employed by the exploit in question was used in a piece of Russian crime software called Zlob prior to Stuxnet's discovery. The same person may have sold the exploit to both the United States and to Russian criminals. However, Lindahl and other experts said simultaneous invention can't be ruled out.

The issue of rival countries or gangs using a flaw that U.S. officials have known about but decided to keep secret is a big concern. The National Security Agency declined to say whether or how often that happens, but researchers said simultaneous security discoveries occur often.

"It's pretty naïve to believe that with a newly discovered zero-day, you are the only one in the world that's discovered it," said Schmidt, who retired last year as the White House cybersecurity coordinator. "Whether it's another government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long."

China is thought to do a lot of its work on exploits in-house, relying on its own programmers, though Reuters has reviewed email from self-declared Chinese buyers offering large sums. "I really need some 0days,if you have some remote exploit 0days of windows system, I think I can buy it. you know, money is not the problem," one hopeful wrote in 2006.

ON THE FRONT LINE

Cesar Cerrudo, a researcher in Argentina and the recipient of the 2006 email, was among the first to sell zero-days in the open, targeting experts who wanted to test the security of networks for their employers or clients.

Cerrudo said he ignored some requests from China that seemed suspiciously detailed, such as one for an exploit for an out-of-date version of Microsoft Office. Cerrudo said he regrets selling to a research institution in Europe he won't name that he later realized received a great deal of funding from a national government. Now Cerrudo works at IOActive Inc, a Seattle-based consulting firm that advises corporate clients on security.

"Fewer people are publishing details about vulnerabilities and exploits," Cerrudo said, and that hurts overall safety. "People are trying to keep their techniques and exploits private so they can make a lot of money."

A Paris-based security company called Vupen sells tools based on exploits to intelligence, law-enforcement and military authorities in most of the world. It refrains from selling to countries such as Iran or North Korea, and says it voluntarily follows European and U.S. rules limiting arms exports, though others say it isn't clear whether exploits are subject to the most restrictive U.S. rules.

Until 2010, Vupen often notified software vendors for free when it found vulnerabilities, said chief executive Chaouki Bekrar. That has now changed. "As our research costs became higher and higher, we decided to no longer volunteer for multi-billion-dollar companies," Bekrar said. When software makers wouldn't agree to a compensation system, he said, Vupen chose to sell to governments instead. "Software vendors created this market by not decently

paying researchers for their hard work."

In Bekrar's estimation, Vupen is doing good. "Exploits are used as part of lawful intercept missions and homeland security operations as legally authorized by law," he said, "to protect lives and democracies against both cyber and real world threats."

The company is one of the most visible players in the business. Vupen sent a dozen researchers to an elite April conference on offensive hacking techniques at the luxury Fontainebleau Hotel in Miami Beach, where attendees eschewed nametags, dined on stone crab and heard such talks as "Advanced Heap Manipulation in Windows 8." The only larger contingents were one from the conference's organizer, zero-day reseller Immunity Inc, and one from the U.S. government.

A newer entrant to the market is ReVuln, based in Malta. ReVuln says it specializes in crafting exploits for industrial control systems that govern everything from factory floors to power generators.

This is a major concern for governments because such systems are considered prime targets for terrorists and enemy nations, with the potential for high loss of life. Additionally, the software that controls them is much harder to patch than something like Windows, which Microsoft frequently fixes with updates over the Internet. Employees at several large makers of control systems say they don't know how to reach all their users, let alone convince them to make changes when holes are discovered.

ReVuln's founders, Italian researcher Luigi Auriemma and former Research in Motion vulnerability hunter Donato Ferrante, declined to say anything about their customers. In an email interview, they said they sold some exploits exclusively and others more widely. Asked if they would be troubled if some of their programs were used in attacks that caused death or destruction, they said: "We don't sell weapons, we sell information. This question would be worth asking to vendors leaving security holes in their products."

DEFENSE CONTRACTORS

Much of the work on offensive cyber-warfare is done by publicly traded U.S. defense contractors, now joined by a handful of venture capital-backed start-ups seeking government buyers for a broad array of cyber-weapons that use exploits. Defense contractors both buy exploits and produce them in-house.

Major players in the field include Raytheon Co, Northrop Grumman Corp and Harris Corp, all of which have acquired smaller companies that specialize in finding new vulnerabilities and writing exploits. Those companies declined to discuss their wares. "It's tough for us, when you get into the realm of offensive," said Northrop spokesman Mark Root.

Reuters reviewed a product catalogue from one large contractor, which was made available on condition the vendor not be named. Scores of programs were listed. Among them was a means to turn any iPhone into a room-wide eavesdropping device. Another was a system for installing spyware on a printer or other device and moving that malware to a nearby computer via radio waves, even when the machines aren't connected to anything.

There were tools for getting access to computers or phones, tools for grabbing different categories of data, and tools for smuggling the information out again. There were versions of each for Windows, Apple and Linux machines. Most of the programs cost more than $100,000, and a solid operation would need several components that work together. The vast majority of the programs rely on zero-day exploits.

Intelligence agencies have a good reason to leave a lot of the spyware development work to outsiders, said Alex Stamos, chief technology officer at an Internet security unit of NCC Group Plc. "It's just like munitions development," he said. "They don't purchase it until the vendors can demonstrate it works."

Another newcomer with U.S. agencies as clients is Atlanta-based Endgame Inc, which in March raised $23 million in

a second round of funding led by the blue-chip Silicon Valley venture capital firm Kleiner Perkins Caufield & Byers. Endgame is chaired by the chief executive of In-Q-Tel, a venture capital firm set up in 1999 at the request of the CIA to fund private companies developing technology that could be useful to the intelligence community.

Some of Endgame's activities came to light in purloined emails published by hackers acting under the banner Anonymous. In what appear to be marketing slides, the company touted zero-day subscriptions as well as lists of exactly which computers overseas belonged to specific criminal "botnets" - networks of compromised machines that can be mobilized for various purposes, including stealing financial passwords and knocking websites offline with traffic attacks.

The point was not to disinfect the botnet's computers or warn the owners. Instead, Endgame's customers in the intelligence agencies wanted to harvest data from those machines directly or maintain the ability to issue new commands to large segments of the networks, three people close to the company told Reuters.

Endgame declined to comment.

Ted Schlein, a Kleiner partner who sits on Endgame's board, said he couldn't comment on the company's classified business. But he defended the idea of captive botnets.

"If you believe that wars are going to be fought in the world of cyber in the future, wouldn't you want to believe you would have a cyber-army at your disposal? Why wouldn't you want to launch a cyber-army if needed?"

(Reporting by Joseph Menn; Editing by Jonathan Weber and Claudia Parsons)