Analysis: The near impossible battle against hackers everywhere

Joseph Menn, Reuters

(Reuters) - Dire warnings from Washington about a "cyber Pearl Harbor" envision a single surprise strike from a formidable enemy that could destroy power plants nationwide, disable the financial system or cripple the U.S. government.

But those on the front lines say it isn't all about protecting U.S. government and corporate networks from a single sudden attack. They report fending off many intrusions at once from perhaps dozens of countries, plus well-funded electronic guerrillas and skilled criminals.

Security officers and their consultants say they are overwhelmed. The attacks are not only from China, which Washington has long accused of spying on U.S. companies, many emanate from Russia, Eastern Europe, the Middle East, and Western countries. Perpetrators range from elite military units to organized criminal rings to activist teenagers.

"They outspend us and they outman us in almost every way," said Dell Inc's chief security officer, John McClurg. "I don't recall, in my adult life, a more challenging time."

The big fear is that one day a major company or government agency will face a severe and very costly disruption to their business when hackers steal or damage critical data, sabotage infrastructure or destroy consumers' confidence in the safety of their information.

Elite security firm Mandiant Corp on Monday published a 74-page report that accused a unit of the Chinese army of stealing data from more than 100 companies. While China immediately denied the allegations, Mandiant and other security experts say the hacker group is just one of more than 20 with origins in China.

Chinese hackers tend to take aim at the largest corporations and most innovative technology companies, using trick emails that appear to come from trusted colleagues but bear attachments tainted with viruses, spyware and other malicious software, according to Western cyber investigators.

Eastern European criminal rings, meanwhile, use "drive-by downloads" to corrupt popular websites, such as NBC.com last week, to infect visitors. Though the malicious programs vary, they often include software for recording keystrokes as computer users enter financial account passwords.

Others getting into the game include activists in the style of the loosely associated group known as Anonymous, who favor denial-of-service attacks that temporarily

block websites from view and automated searches for common vulnerabilities that give them a way in to access to corporate information.

An increasing number of countries are sponsoring cyber weapons and electronic spying programs, law enforcement officials said. The reported involvement of the United States in the production of electronic worms including Stuxnet, which hurt Iran's uranium enrichment program, is viewed as among the most successful.

Iran has also been blamed for a series of unusually effective denial-of-service attacks against major U.S. banks in the past six months that blocked their online banking sites. Iran is suspected of penetrating at least one U.S. oil company, two people familiar with the ongoing investigation told Reuters.

"There is a battle looming in any direction you look," said Jeff Moss, the chief information security officer of ICANN, a group that manages some of the Internet's key infrastructure.

"Everybody's personal objectives go by the wayside when there is just fire after fire," said Moss, who also advises the U.S. Department of Homeland Security.

HUNDREDS OF CASES UNREPORTED

Industry veterans say the growth in the number of hackers, the software tools available to them, and the thriving economic underground serving them have made any computer network connected to the Internet impossible to defend flawlessly.

"Your average operational security engineer feels somewhat under siege," said Bruce Murphy, a Deloitte & Touche LLP principal who studies the security workforce. "It feels like Sisyphus rolling a rock up the hill, and the hill keeps getting steeper."

In the same month that President Barack Obama decried enemies "seeking the ability to sabotage our power grids, our financial institutions, our air traffic control systems," cyber attacks on some prominent U.S. companies were reported.

Three leading U.S. newspapers, Apple Inc, Facebook Inc, Twitter and Microsoft Corp all admitted in February they had been hacked. The malicious software inserted on employee computers at the technology companies has been detected at hundreds of other firms that have chosen to keep silent about the incidents, two people familiar with the case told Reuters.

"I don't remember a time when so many companies have been so visibly 'owned' and were so ill-equipped," said Adam O'Donnell, an executive at security firm Sourcefire Inc, using the hacker slang for unauthorized control.

Far from being hyped, cyber intrusions remain so under-disclosed — for fear leaks about the attacks will spook investors — that the new head of the FBI's cyber crime effort, Executive Assistant Director Richard McFeely, said the secrecy has become a major challenge.

"Our biggest issue right now is getting the private sector to a comfort level where they can report anomalies, malware, incidences within their networks," McFeely said. "It has been very difficult with a lot of major companies to get them to cooperate fully."

McFeely said the FBI plans to open a repository of malicious software to encourage information sharing among companies in the same industry. Obama also recently issued an executive order on cyber security that encourages cooperation.

The former head of the National Security Agency, Michael Hayden, supports the use of trade and diplomatic channels to pressure hacking nations, as called for under a new White House strategy that was announced on Wednesday.

"The Chinese, with some legitimacy, will say 'You spy on us.' And as former director of the NSA I'll say, 'Yeah, and we're better at it than you are," said Hayden, now a principal at security consultant Chertoff Group.

He said what worries him the most is Chinese presence on networks that have no espionage value, such as systems that run infrastructure like energy and water plants. "There's no intellectual property to be pilfered there, no trade secrets, no negotiating positions. So that makes you frightened because it seems to be attack preparation," Hayden said.

Amid the rising angst, many of the top professionals in the field will convene in San Francisco on Monday for the best-known U.S. security industry conference, named after host company and EMC Corp unit RSA.

Several experts said they were convinced that companies are spending money on the wrong stuff, such as antivirus subscriptions that cannot recognize new or targeted attacks.

RSA Executive Chairman Art Coviello and Francis deSouza, head of products at top vendor Symantec Corp, both said they will give keynote speeches calling for a focus on more sophisticated analytical tools that look for unusual behavior on the network — which sounds expensive.

Others urge a more basic approach of limiting users' computer privileges, rapidly installing software updates, and allowing only trusted programs to function.

Some security companies are starting over with new designs, such as forcing all of their customers' programs to run on walled-off virtual machines.

With such divergent views, so much money at stake, and so many problems, there are perhaps just two areas of agreement.

Most people in the industry and government believe things will get worse. Coviello, for his part, predicted that a first-of-its kind - but relatively simple - virus that deleted all data on tens of thousands of PCs at Saudi Arabia's national oil company last year is a harbinger of what will come.

And most say that the increased mainstream attention on cyber security, even if it fixes uncomfortably on the industry's failings and tenacious adversaries, will help drive a desperately needed debate about what do to internationally and at home.

(Reporting by Joseph Menn in San Francisco; Additional reporting by Jim Finkle in Boston and Deborah Charles in Washington; Editing by Tiffany Wu and Jackie Frank)

Source URL (retrieved on *09/21/2014 - 5:59am*):
http://www.ecnmag.com/news/2013/02/analysis-near-impossible-battle-against-hackers-everywhere?qt-video_of_the_day=0