US Target of Massive Cyber-Espionage Campaign

s.A InstallFlame
tacks.A InstallFlame Agen
ttacks.A InstallFlame Shoul
.bat
Attacks.A InstallFlame Command
Attacks.A InstallFlame Service
Attacks.A InstallFlame Attack
ttacks.A InstallFlame Delete
tacks.A InstallFlame Delet
acks.A InstallFlame Sam

Washington Post
February 10, 2013

By Ellen Nakashima

A new intelligence assessment has concluded that the United States is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness, according to individuals familiar with the report.

The National Intelligence Estimate identifies China as the country most aggressively seeking to penetrate the computer systems of American businesses and institutions to gain access to data that could be used for economic gain.

The report, which represents the consensus view of the U.S. intelligence community, describes a wide range of sectors that have been the focus of hacking over the past five years, including energy, finance, information technology, aerospace and automotives, according to the individuals familiar with the report, who spoke on the condition of anonymity about the classified document. The assessment does not quantify the financial impact of the espionage, but outside experts have estimated it in the tens of billions of dollars.

Cyber-espionage, which was once viewed as a concern mainly by U.S. intelligence and the military, is increasingly seen as a direct threat to the nation's economic interests.

In a sign of such concerns, the Obama administration is seeking ways to counter the online theft of trade secrets, according to officials. Analysts have said that the administration's options include formal protests, the expulsion of diplomatic personnel, the imposition of travel and visa restrictions, and complaints to the World Trade Organization.

Cyber-espionage is "just so widespread that it's known to be a national issue at this point," said one administration official, who like other current and former officials interviewed spoke on the condition of anonymity to discuss internal deliberations.

The National Intelligence Estimate names three other countries — Russia, Israel and France — as having engaged in hacking for economic intelligence but makes clear that cyber-espionage by those countries pales in comparison with China's effort.

China has staunchly rejected such allegations, saying the Beijing government neither condones nor carries out computer hacking.

Dating to at least the early 1980s, China has made the acquisition of Western technology — through means licit and illicit — a centerpiece of its economic development planning. The explosion in computer use has greatly aided that transfer of technology.

China's intelligence services, as well as private companies, frequently seek to exploit Chinese citizens or people with family ties to China who can use their insider access to U.S. corporate networks to steal trade secrets using thumb drives or e-mail, according to a report by the Office of the National Counterintelligence Executive.

The National Intelligence Estimate comes at a time when the U.S. government is making a concerted effort to develop policies that address cyberthreats against the nation.

"We need the NIE on cyber for a systematic and comprehensive understanding of what the most dangerous technologies are, who are the most threatening actors and what are our greatest vulnerabilities," said former deputy defense secretary William J. Lynn III, who requested the report in 2011 but has not seen or been briefed on the contents.

Some officials have pressed for an unclassified summary to be released publicly. Michael Birmingham, a spokesman for the Office of the Director of National Intelligence, declined to comment on the report, except to say that “as a matter of policy, we do not discuss or acknowledge the existence of NIEs unless directed to do so.”

A range of sectors

Much of China’s cyber-espionage is thought to be directed at commercial targets linked to military technology. In 2011, when Chinese hackers attacked network security company RSA Security, the technology stolen was used to penetrate military-industrial targets. Shortly after, the networks of defense contracting giant Lockheed Martin, which used RSA security tokens, were penetrated by Chinese hackers. The company said no data were taken.

Companies in other sectors also have been targeted, though the reasons for the espionage are not always related to economic interests. The New York Times, the Wall Street Journal and The Washington Post recently disclosed that they believe their networks were compromised in intrusions that originated in China.

Despite those disclosures and the growing prevalence of cyber-espionage, companies remain reluctant to report incidents.

“It’s harder for companies to suggest that they haven’t been attacked,” the administration official said. “The question is, how do they respond when they are asked about it? Is it in their interest to work with other companies and with the government to alleviate some of the problem?”

A watershed moment came in January 2010,when the tech titan Google announced that its networks had been hacked and that the intrusions originated in China. The intruders made off with valuable source code and targeted the Gmail accounts of Chinese human rights activists and dissidents, the company announced.

In a new book, Google chief executive Eric Schmidt says China is the world’s “most sophisticated and prolific” hacker, adding: “It’s fair to say we’re already living in an age of state-led cyberwar, even if most of us aren’t aware of it.”

Administration's response

In recognition of the growing problem, the State Department has elevated the issue to be part of its strategic security dialogue with China. Within the past year, the Justice Department has set up a program to train 100 prosecutors to bring cases related to cyber-intrusions sponsored by foreign governments.

In many ways, the moves are a response to what experts have described as the government's earlier passivity in tackling the problem.

"The problem with foreign cyber-espionage is not that it is an existential threat, but that it is invisible, and invisibility promotes inaction," a former government official said. The National Intelligence Estimate, he said, "would help remedy that" by detailing the scope of the threat.

Some experts have said that cyber-espionage's cost to the U.S. economy might range from 0.1 percent to 0.5 percent of gross domestic product, or $25 billion to $100 billion. Other economists, while viewing the problem as significant, have pegged the losses lower.

The White House is set to soon release a trade-secrets report, compiled by U.S. Intellectual Property Enforcement Coordinator Victoria Espinel, that highlights the need for companies to work with the government to stop the pilfering, said officials familiar with the report.

The government cannot mount a case on its own. A company needs to think it was wronged, have enough evidence that can be made public and be willing to burn bridges with the country accused of the hacking, officials said.

The White House is also expected this week to issue an executive order on cybersecurity that calls for voluntary standards for critical private-sector computer systems and for enhanced sharing of threat information by the government with companies to help secure private-sector systems against cyber-intrusions.