PITTSBURGH TRIBUNE-REVIEW

Hackers who attack U.S. in line for lucrative payoffs

By Adam Smeltz - Published: Saturday, October 27, 2012

Google wants a few Good Samaritans.

The Internet behemoth offers $100 to $20,000 in rewards for observers who find serious bugs compromising its users' data.

But corporate thank-yous may not pay the bills for independent Web gurus with the smarts to dig into sensitive electronic networks, digital security analysts said. Paid hacking for rogue groups and overseas governments can promise a much more lucrative alternative, complicating the rising global threats against the United States' cybersecurity.

“Hackers today have a choice: They can report bugs and problems to manufacturers of software” or sell their findings to foreign interests, said Albert Whale, senior security director at ABS Computer Technology Inc. in Ross.

He said prices per job can begin in the tens of thousands of dollars and reach hundreds of thousands.

“They're in it for the money,” said Whale, a consultant for the international software-security firm Cigital in Dulles, Va. “Name recognition isn't going to put food on the table.”

The cryptic nature of hacking makes it tough to gauge how often independent contractors, paid on the black market, snoop on behalf of overseas government interests and unofficial organizations. It's unclear how much of the hacking community they represent.

Some estimates suggest 4,000 people might belong to the Russian Business Network, among the largest networks of cybercriminals, said Norwich University faculty member M.E. Kabay.

In many dictatorships, “it's difficult to understand how criminal hackers could be working at all without tacit or explicit government support,” said Kabay, a professor in computer information systems at the Vermont school.

PREPARING FOR ATTACK

Defense Secretary Leon Panetta focused attention on domestic cybersecurity this month in New York, where he raised the prospect of a “cyber Pearl Harbor.”

He said thousands of “cyber actors ... probe the Defense Department’s networks millions of times per day.”

Panetta said Defense officials unearthed breaches of infrastructure networks that control chemical, electricity and water plants, along with transportation systems.

“We also know (these hackers) are seeking to create advanced tools to attack these systems and cause panic, destruction and even the loss of life,” Panetta said.

Worst-case scenarios would include near-simultaneous cyberattacks and conventional ground assaults, together crippling electrical, financial and communications systems in coordinated takedowns, technology scholars said.

The impact could knock out power generators, muddle medical systems and block access to banking.

“All they have to do is pick the right grid system somewhere and start knocking it out and we’d have a domino effect,” said E. Douglas Harris, associate dean at the Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas.

To safeguard the country in cyberspace, Panetta said, the Defense Department is investing more than $3 billion a year in “cutting-edge capabilities ... even in an era of fiscal restraint.” Additionally, the department is crafting policies and structuring better cooperation with industry and international partners, he said.

CHINA’S CYBERSNOOPING

Panetta mentioned China as a source of “growing cyber capabilities.” In interviews with the Tribune-Review, academic and industry leaders identified China and Russia as key sources of cyberthreats to the United States.

Both countries have integrated cyber-warfare capabilities into their military strategies, said Frank Cilluffo, director of the Homeland Security Policy Institute at George Washington University. China especially has engaged in cyberspying for at least a decade, probably mapping the United States’ electronic infrastructure and digging into private-sector intellectual property, analysts said.

They believe the large countries most committed to cybersnooping likely are developing in-house digital espionage teams instead of relying only on contractors.

“I think it’s a very disturbing trend but it’s probably also unstoppable,” said Gary McGraw, chief technology officer at Cigital and author of 12 books on software security.

McGraw said the United States has started to turn the tables on hackers, cyber-attacking the Iranian nuclear program in conjunction with Israel.

SMALL, BUT BOLD

Smaller adversaries such as Iran and North Korea present hacking threats on a less-sophisticated scale than China or Russia, but they can make up the difference with bold willingness to act, Cilluffo said. Investigators traced to Iran the denial-of-service attack at PNC Bank this month, the bank reported.

Iran, saddled with U.S. sanctions, might pursue cyberattacks as a way to push back and rattle the economy, analysts said. China probably uses its cyber prowess to sniff out trade secrets and prepare for possible confrontations. Rogue terrorists might attempt more crude attacks to drum up publicity and wreak havoc.

“Much of the infrastructure has never been designed to face an attack” through cyberspace, Kabay noted. Systems such as power grids were retrofitted to tie into the Internet but engineers added “trivial or no security” in the process, he said.

“Computers were never designed for cyberthreats,” Harris said. “They were designed as open networks.”

For technology professionals, that means a booming job market as businesses and other groups double down on safety.

The Bureau of Labor Statistics predicts the information technology job category that includes security workers will grow 22 percent in the next several years.

At the Cato Institute in Washington, Jim Harper said the private sector controls most digital data and is “best positioned to find problems related to cybersecurity.”

“The parties responsible for securing trade secrets are the owners of those trade secrets and intellectual property in the private sector,” said Harper, the director of information-policy studies. “It’s not the government.”