Keystroke crackdown

Army wants to monitor your computer activity to smoke out insider threats

By Joe Gould
jgould@militarytimes.com

In the wake of the biggest dump of classified information in the history of the Army, the brass is searching for ways to watch what every soldier is doing on his or her Army computer.

The Army wants to look at keystrokes, downloads and Web searches on computers that soldiers use.

Maj. Gen. Steven Smith, chief of the Army Cyber Directorate, said the software was one of his chief priorities, joking that it would take the place of a lower-tech solution: "A guy with a large bat behind every user as they go to search the Internet."

"Now we've been in the news — I don't know if you've seen it — with a little insider threat issue," Smith continued.

Smith did not mention Pfc. Bradley Manning by name. However, the effort comes in the wake of the former intelligence analyst's alleged leak of hundreds of thousands of pages of classified documents to the anti-secrecy organization WikiLeaks in 2009 and 2010. Manning faces a military trial on 22 counts, including aiding the enemy.

According to Smith, the Army will soon shop for software pre-programmed to detect a user's abnormal behavior and record it, catching malicious insiders in the act. Though it is unclear how broadly the Army plans to adopt the program, the Army has more than 900,000 users on its computers.

Smith explained how it might work.

"So I'm on the South American desk, doing intelligence work and all of a sudden I start going around to China, let's say," Smith said. "That might be an anomaly, it might be justified, but I would sure like to know that and let someone make a decision, almost at the speed of thought."

The scenario echoes the allegations against Manning: As an intelligence analyst charged with researching the Shiite threat to Iraqi elections, Manning raided classified networks for State Department cables, Afghanistan and Iraq war logs and video from a helicopter attack, according to courtroom testimony.

Software of the type Smith describes is at various stages of development in the public and private sectors. Such software could spy on virtually any activity on a desktop depending on its programming, to detect when a soldier searches outside of his or her job description, downloads massive amounts of data from a shared hard drive or moves the data onto a removable drive.

The program could respond by recording the activity, alerting an administrator, shutting down the user's access, or by feeding the person "dummy data" to watch what they do next, said Charles Beard, a cybersecurity executive with the defense firm SAIC's intelligence, surveillance and reconnaissance group.

"It's a giant game of cat and mouse with some of these actors," Beard said.

What's exciting, Smith said, is the possibility of detecting problems as they happen, on what cybersecurity experts call "zero day," as opposed to after the fact.

"We don't want to be forensics experts. We want to catch it at the perimeter," Smith said. "We want to catch this before it has a chance to be exploited."

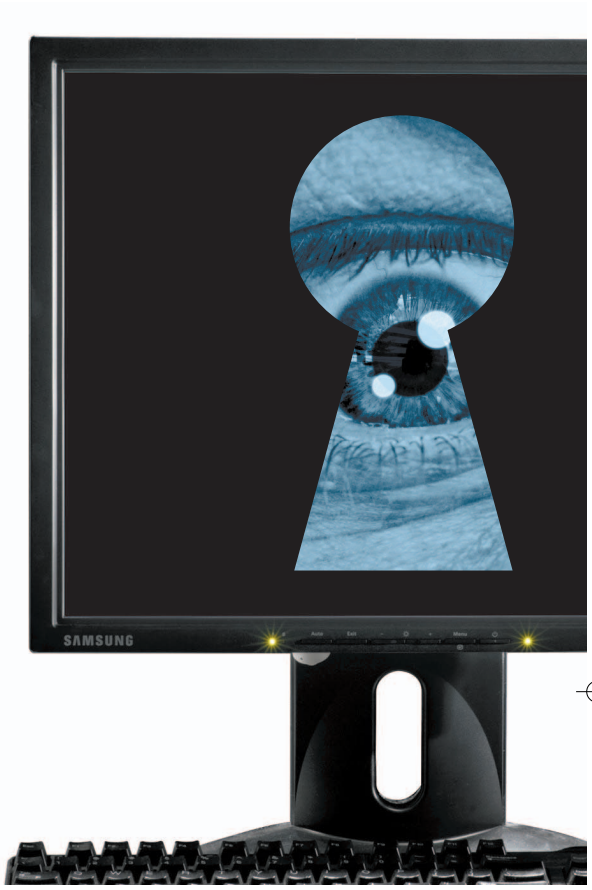
A governmentwide effort

The Army's efforts dovetail with a broader federal government initiative. President Obama signed an executive order last October that established an Insider Threat Task Force to develop a governmentwide program to deter, detect and mitigate insider threats.

Among other responsibilities, it would create policies for safeguarding classified information and networks, and for auditing and monitoring users.

In January, the White House's Office of Management and Budget issued a memo directing government agencies that deal with classified information to ensure they adhere to security rules enacted after the WikiLeaks debacle.

Beyond technical solutions, the document asks agencies to create their own "insider threat program" to monitor employees for "behavioral changes" suggesting they might leak sensitive information.



The interagency Insider Threat Task Force is aiming to complete work on the new standards by October. These standards may address training and employee awareness protocols, said John Swift III, senior policy adviser to a task force now working on the draft policy.

Deanna Caputo, lead behavioral psychologist for Mitre Corp., said both technical solutions and monitoring of human behaviors are needed for a successful detection and prevention program.

"To think that we can tackle the problem simply by technical solutions is a mistake," Caputo said.

A "culture of reporting" is essential, she said. "We need to up the ante and expect a little bit more from our people" to report abnormal behaviors among their coworkers. However, "there is a fine line with that [reporting]. People need to trust they are in a safe environment to do their job."

Carnegie Mellon's Software Engineering Institute has compiled 700 insider threat case studies, and come up with two broad profiles of insiders who steal intellectual property in business settings.

One is an "entitled independent" disgruntled with his job who typically exfiltrates his work a month before leaving. The other is an "ambitious leader" who steals information on entire systems and product lines, sometimes to take to a foreign country, such as China.

According to Patrick Reidy, who leads the FBI's insider threat program, such users may be conducting authorized activities for malicious ends, and their actions would not register on intrusion detection or anti-virus systems.

"People look at computers and