US data mining system technical details murky

June 8 2013, by Rob Lever

A Google logo is seen on a monitor at the company's annual developer conference in San Francisco on June 28, 2012. The US government's vast online data collection system unveiled this week could tap into companies like Google and Facebook without the knowledge of top executives, experts say.

The US government's vast online data collection system revealed this week could tap into companies like Google and Facebook without the knowledge of top executives, experts said.

The so-called PRISM program could be so secret that only a small number of computer network administrators and company lawyers may have been aware of it, according to technical and legal specialists.

Still, many aspects of the program remain murky, according to people who follow issues related to online privacy and security.

The government has acknowledged tapping into servers of nine Internet giants—including Apple, Facebook, Google, Microsoft and YouTube —even though the companies deny giving direct "backdoor" access.

The Washington Post and The Guardian reported the system dates back to 2007.

"There is something deeply mysterious about this," said Joseph Hall, senior technologist with the Center for Democracy and Technology, a digital rights activist group. "We've been wracking our brains all night."

The program run by the top-secret National Security Agency with the FBI "could be doing things in ways the companies wouldn't know," Hall said.

Hall noted that many questions are unanswered, such as how the program handles encrypted communications.

Johannes Ullrich, chief research officer for the SANS Institute computer research center, said it would be technically possible to set up a "master account" to give government spies access but that many in the companies might be kept in the dark.

"Given the secrecy of these systems, I am not surprised that only few inside the respective organizations have knowledge about the access," Ullrich told AFP.

Ullrich said that "the exact nature of the backdoor is still not known" but that it would be hard to "filter" the data to target only non-US users, as the government insists is the case.

"It's not realistic to filter non-US data" in the collection process, he said, adding that the system must later exclude non-relevant data about Americans.

Ullrich said the program raises questions about the vulnerability of the companies if a so-called "backdoor" has been established.

"Not just the organization authorized to use the backdoor has access to the data, but anybody who penetrated that organization," he said.

"So the Chinese probably have access to the data as well."

Alex Halderman, a University of Michigan computer science professor who specializes in data security, said the company denials "seem quite broad and are hard to square with the supposed capabilities of PRISM."

Halderman said it is possible that "the gag orders were so restrictive that senior management was not told... arguably only a small group of attorneys and engineers would need to know in order to comply with a sweeping access request."

Sascha Meinrath, who heads the New America Foundation's Open Technology Institute, said companies are "trying to elide the truth" about their cooperation.

"I expect that when it comes to light, we will find a number of boxes at the data centers of these companies," he said.

"You need that because the amount of data is so huge that you have to have an infrastructure in place."

Facebook's logo is played on a laptop screen in Manila on May 15, 2012. The US government's vast online data collection system unveiled this week could tap into companies like Google and Facebook without the knowledge of top executives, experts say.

Although it is possible to tap into services remotely, Meinrath said this would be "a massive security risk" that could allow access from hackers or others.

Marc Rotenberg, president and executive director of the Electronic Privacy Information Center (EPIC), said he sees no contradiction between the public statement of the companies and the likely cooperation.

"What strikes the reader as a denial is not a denial," Rotenberg said.

"Google did not say they were not disclosing information to the NSA. They said they did not provide a backdoor."

Rotenberg, whose organization has sued unsuccessfully to get details of what was reported to be a cooperation agreement between Google and the NSA, said data orders might be known only by the legal staff and a technical expert.

"Much of this authority to disclose information is subject to the gag provisions which prevent companies from disclosing the existence of the obligation," he said.

"The spokespeople may be speaking accurately about what they know but it might not be an accurate statement. They could be punished for acknowledging it."

EPIC attorney Ginger McCall said the program appeared to be designed "to circumvent the need for a court order," and that as a result, "there is a strong possibility it was illegal."

But companies have "an incentive not to be forthright" because "if they were cooperating, there is a potential for liability," she noted.

Bruce Schneier, an author of books on computer security who is the chief security technology officer at BT, said the latest revelations are only providing a small amount of information on government snooping.

"All we have is shadows of information," he said. "We are finally learning some things. We need more whistleblowers."

Citation: US data mining system technical details murky (2013, June 8) retrieved 26 April 2024 from https://phys.org/news/2013-06-technical-murky.html