Eyes on you: Experts reveal police hacking methods (Update 2)

June 24 2014, by Raphael Satter

Malicious software expert Sergey Golovanov, with Moscow-based Kaspersky Lab, speaks during a "cyber self-defense course" hosted by his firm in east London on Tuesday, June 24, 2014. Kaspersky and University of Toronto-based Citizen Lab are publishing reports detailing the workings of software produced by Hacking Team, an Italian cyber surveillance company. The reports, which were released simultaneously on Tuesday, show how law enforcement agencies across the globe are taking a page out of the cybercriminal handbook, using targets' own phones and computers to spy on them with methods traditionally associated with the world's most malicious hackers.(AP Photo/Raphael Satter)

Law enforcement agencies across the globe are taking a page out of the hacker's handbook, using targets' own phones and computers to spy on them with methods traditionally associated with cybercriminals, two computer security groups said Tuesday.

Drawing on a cache of leaked documents and months of forensic work, two reports about the private Italian firm Hacking Team expose a global network of malicious software implants operated by police and spy agencies in dozens of countries.

"This in many ways is the police surveillance of the now and the future," said Morgan Marquis-Boire, a security researcher with Citizen Lab and a lead author of one of the reports. "What we need to actually decide how we're comfortable with it being used and under what circumstances."

Citizen Lab's work, paired with a report published simultaneously by Moscow-based Kaspersky Lab, helps complete the picture of state-sanctioned surveillance sketched by Edward Snowden's sensational revelations about the National Security Agency and its international allies.

While many of Snowden's revelations dealt with the mass monitoring of communication as it flows across the globe, Hacking Team brags about more aggressive forms of monitoring that let authorities turn people's phones and laptops into eavesdropping tools.

Hacking Team's chief spokesman, Eric Rabe, dismissed the reports as consisting of a lot of old news. Hacking Team's ability to break into iPhones and BlackBerrys is "well known in the security industry," he said in an email.

"We believe the software we provide is essential for law enforcement and for the safety of all in an age when terrorists, drug dealers and sex

traffickers and other criminals routinely use the Internet and mobile communications to carry out their crimes," he said.

Rabe invoked Hacking Team's customer policy, which says the company sells only to governments which it screens for human rights concerns. A company-established panel—whose membership Rabe declined to specify—checks out every potential client. While Hacking Team realizes that its software can be abused, the policy says the company takes "a number of precautions to limit the potential for that abuse."

Morgan Marquis-Boire, a senior security researcher and technical adviser with University of Toronto-based Citizen Lab, speaks during a "cyber self-defense course" hosted by Russian antivirus firm Kaspersky at an event in east London on Tuesday, June 24, 2014. Citizen Lab and Kaspersky are publishing reports detailing the workings of software produced by Hacking Team, an Italian cyber surveillance company. The reports, which were released simultaneously on Tuesday, show how law enforcement agencies across the globe are taking a page out of the cybercriminal handbook, using targets' own phones and computers to

spy on them with methods traditionally associated with the world's most malicious hackers. (AP Photo/Raphael Satter)

Those precautions haven't prevented copies of Hacking Team's malicious software from being used to target more than 30 activists and journalists, according to a tally maintained by Citizen Lab, a research group based at the University of Toronto's Munk School of Global Affairs.

Citizen Lab's report provided an unusual level of insight into how the malware operates, showing how devices can be compromised through booby-trapped emails or infected USB sticks, or even pushed onto handsets by a pliant telephone company.

Screenshots released by Citizen Lab appear to show a control panel complete with on-off switches for recording text messages, calls, keystrokes and visited websites. Other options open to Hacking Team's customers include the ability to force infected phones to take regular pictures or video and to monitor the position of an infected handset via Google Maps, effectively turning a target's phone into both a hidden camera and a tracking device.

Hacking Team built its programs for stealth. The spy software implanted on iPhones is calibrated to avoid draining the phone's battery, both Citizen Lab and Kaspersky said. On BlackBerrys, it can be programmed to ship stolen data via Wi-Fi to avoid jacking up the phone bill. The spyware even comes with a special "crisis" mode that will cause it to self-destruct if it's in danger of being detected.

"The victim's got almost no chances of figuring out that their iPhone is infected," said Kaspersky malware expert Sergey Golovanov, who

investigated the rogue program for his firm.

Hacking Team does not say who its customers are, but researchers can draw inferences from the network of servers tasked with controlling its spyware.

In its report, Kaspersky says its scans uncovered 326 Hacking Team command servers based in more than 40 countries, including 64 servers in the United States, 49 in Kazakhstan and 35 in Ecuador. Other countries hosting multiple servers include the United Kingdom, Canada and China.

Kaspersky's report cautions that hosting a Hacking Team command server doesn't necessarily mean officials in that country are using its software, although it said that would be logical due to the complications of controlling spyware from another nation's territory.

Hints about who is using these programs can also be found by studying how victims got infected.

Citizen Lab found Hacking Team software hiding in an Android phone application ostensibly designed to provide Arabic-language news from Saudi Arabia's Qatif region, the scene of protests in the wake of the 2011 Arab Spring revolutions. Saudi officials did not immediately return calls seeking comment.

Steven Bellovin, a Columbia University academic who has written about hacking in the law enforcement context, described the reports' findings as credible. In an email exchange, he said there was nothing inherently wrong about police using malware to infect their targets, noting that both police and criminals do carry guns.

"The hacking tools fall into the same category. They're dual use," he

said.

But Bellovin said there need to be strict rules - and open debate - about the law enforcement uses of malicious software before government-commissioned viruses are unleashed on the Internet.

"None of that seems to be present here," he said.

More information: Citizen Lab's report: citizenlab.org/2014/06/backdoo … raft-android-implant

Kaspersky's report: www.securelist.com/en/blog/823 … he_Story_Goes_Mobile

Hacking Team's video: www.hackingteam.it/index.php/remote-control-system