Tech sector scrambles after CIA device-hacking allegations

March 8 2017, by Rob Lever

The CIA's hacking tools have targeted iPhones and Android systems such as the personal phone reportedly still used by President Trump, the WikiLeaks documents indicated

The tech sector was scrambling Wednesday to understand the implications of an alleged broad CIA hacking arsenal, capable of spying on phones and other connected devices.

Major tech firms said they were looking at the allegations raised in the documents released by WikiLeaks on Tuesday.

"While our initial analysis indicates that many of the issues leaked today were already patched in the latest iOS, we will continue work to rapidly address any identified vulnerabilities," Apple said in an emailed statement.

Samsung offered a similar response, saying: "We are aware of the report in question and are urgently looking into the matter."

Microsoft, meanwhile, said: "We're aware of the report and are looking into it."

Security analysts, however, said the documents, if authentic, were not on the same scale as the explosive 2013 revelations from former national security contractor Edward Snowden, who revealed mass surveillance tools used by the National Security Agency.

Targeted, not bulk spying

"These are targeted mechanisms, they can't be used for bulk intelligence," said Joseph Hall, a technologist with the Center for Democracy and Technology, a digital rights organization.

"It means they can't attack things in the middle and the core of the network, they have to go to the endpoints, and that's actually a nice thing. You have to be more precise about who you are targeting."

But Hall said the report raises questions about the US government's pledge to disclose security flaws to technology firms under a so-called "vulnerabilities equities process."

That pledge means "security flaws should get back to the companies so they can get fixed, and not languish for years," Hall said.

The WikiLeaks documents, the authenticity of which has not been verified, said the CIA tools could turn smart TVs into listening devices, bypass popular encryption apps, and possibly control connected automobiles.

The hacking tools have targeted iPhones, Android systems such as the personal phone reportedly still used by President Donald Trump, popular Microsoft software, and Samsung smart TVs, the documents indicated.

Open Whisper Systems, the company that developed the technology for the communications tool Signal, said the CIA documents showed its encryption works.

The WikiLeaks report "is about getting malware onto phones, none of the exploits are in Signal or break Signal Protocol encryption," the group said in a tweet.

Other encryption experts agreed.

Strength of encryption

"The existence of these hacking tools is a testimonial to the strength of the encryption," said Steve Bellovin, a Columbia University computer science researcher, in a blog post.

"It's hard or impossible to break, so the CIA is resorting to expensive, targeted attacks."

Robert Graham, a researcher with Errata Security, said most of these hacks are simply methods to "trick you into installing their software."

"Snowden revealed how the NSA was surveilling all Americans. Nothing like that appears in the CIA dump," Graham said in a blog post. "It's all legitimate spy stuff (assuming you think spying on foreign adversaries is legitimate)."

Bruce Schneier, chief technology officer at IBM Resilient and a frequent critic of government surveillance, said on his blog, "There is absolutely nothing illegal in the contents of any of this stuff. It's exactly what you'd expect the CIA to be doing in cyberspace."

Citation: Tech sector scrambles after CIA device-hacking allegations (2017, March 8) retrieved 7 May 2024 from https://phys.org/news/2017-03-tech-sector-scrambles-cia-hacking.html