

Publication: Financial Times (Europe); Date: Jun 3, 2015; Section: Companies & Markets; Page: 14

Software

Lookout targets 'bring your own' smartphone hacking risks

HANNAH KUCHLER — SAN FRANCISCO

Lookout, a cyber security start-up, is offering large companies a software platform to tackle the threat from hackers to smartphones.

The San Francisco-based company — which raised \$150m last year and counts Morgan Stanley, Goldman Sachs and Amazon founder Jeff Bezos among its backers — has trialled its system with 20 organisations, as concerns grow about the possibility of confidential data being stolen from employees' mobile devices.

Aaron Cockerill, vice-president of products at Lookout, said clients had previously focused on PCs and laptops. With hackers stealing \$1 off a phone's SMS bill, companies had dismissed the mobile threat as small, he said.

However, cyber criminals had started to target phones because employees sometimes "carry around next year's financial plan in their pocket", Mr Cockerill added. "Large companies are facing targeted, novel, unique attacks that either exfiltrate data or penetrate corporate networks."

Lookout's expansion comes after a widely followed report from Verizon found that just 100 mobile devices faced serious security breaches each day, contesting warnings about the vulnerability of smartphones.

Chris Spence, chief technology officer of the National Democratic Institute, a non-governmental organisation, has been using Lookout's software to try to protect employee smartphones across the world. "My guess is that the mobile threats are evolving," he said.

"As long as laptops and desktops are relatively easy to trick, easy for people to dominate, the bad guys don't need to get you on your mobile devices yet. [But] we want to be proactive and stay ahead of the game."

The NDI, chaired by former US secretary of state Madeleine Albright, faces targeted threats on its desktop computers, with hackers trying to obtain confidential information about the politically sensitive markets where it advocates democracy. So far it has seen little threat on mobile devices.

From its experience providing security software to more than 70m consumers and small businesses, Lookout has built up an expertise regarding the flaws in mobile apps. Its aim is to apply this knowledge to protect larger companies.

Mr Cockerill said that while the Apple ecosystem was prized as a safe environment online, enterprise apps developed for the operating system were not always subject to the iPhone maker's own stringent checks. "Developers can very easily make a mistake that does not get checked, and an employee device can be turned into an exploited device," he said.

The eight-year-old enterprise has used raised funds from groups including Deutsche Telekom and Andreessen Horowitz, the venture capitalist firm, to develop its salesforce and channels to sell into larger companies.

Jim Dolce, chief executive, said the company was ready to offer a security product that catered "beyond the singles and tens, and into the tens of thousands of users per account".

The adoption of consumer devices in the workplace, he said, meant tighter data security on smart technology was increasingly important.

"Chief information security officers are finding no choice but to support the 'bring your own device' model of risk exposure, even though it's an unknown brave new world," said Mr Dolce.

"[The model] is coming fast and furious and there's no stopping it because it is so convenient."



Twenty companies have been trialling a Lookout security product