User Info Safe After LoopPay Attack, Says Samsung

"This breach wasn't about LoopPay's corporate network or their customer data," said Dan Verton, executive editor of MeriTalk. "This was more likely an attempt to obtain information about the mobile payment technology the company developed so that exploits could be created." LoopPay's technology, called "Magnetic Secure Transmission," transmits information to a POS terminal via a magnet.

By John P. Mello Jr.
Oct 9, 2015 3:58 PM PT

Print
Email

Samsung on Thursday assured users that their information is safe following a computer intrusion of a key company linked to its mobile payment system.

The intrusion of LoopPay by a gang of hackers known as the Codoso or Sunshock Group may have occurred as early as March, according to a report in *The New York Times*.

Samsung purchased LoopPay for $250 million in February. Its technology -- which the company's newly launched mobile payment system, Samsung Pay, uses --

allows mobile phones to perform payment card transactions with older point-of-sale terminals that recognize only cards with magnetic strips.

"Samsung Pay was not impacted and at no point was any personal payment information at risk," Samsung said in a statement provided to TechNewsWorld by spokesperson Danielle Meister Cohen.

"This was an isolated incident that targeted the LoopPay corporate network, which is a physically separate network from Samsung Pay," the company explained. "The LoopPay corporate network issue was resolved immediately and had nothing to do with Samsung Pay."

Hunting for IP

Unlike widely publicized data breaches at Target, Home Depot and the U.S. Office of Personnel Management, in which intruders nicked information about individuals, the LoopPay bandits appear to have had another target in their crosshairs.

"This breach wasn't about LoopPay's corporate network or their customer data," said Dan Verton, executive editor of MeriTalk.

"This was more likely an attempt to obtain information about the mobile payment technology the company developed so that exploits could be created," the former U.S. intelligence officer told TechNewsWorld. LoopPay's technology, called "Magnetic Secure Transmission," transmits information to a POS terminal via a magnet. That allows devices using it to communicate with older card readers.

Samsung estimates that MST works with 80 percent of the existing card readers in the United States.

That's expected to give Samsung Pay an edge over competitors like Apple Pay that work only with newer systems that support near field communication wireless technology. It's estimated that only one in five POS terminals in the U.S. supports NFC. PR Problem While the LoopPay invaders may have been looking for intellectual property and not payment card information, the public might not make that distinction.

"That's a public relations question," said Leon Majors, senior vice president for Phoenix Marketing International.

"Will Samsung do enough to make sure customers know that? That's the key, but it's not something we will be able to answer for a month or two," he told TechNewsWorld. "This is about reputation rather than reality," said David Robertson, publisher of The Nilson Report.

Samsung Pay data could be perfectly safe, but the company has to disabuse the public of popular beliefs about its phones.

"There is a legacy notion [that] the safety and security of a Samsung device lags behind the safety and security of Apple devices," Robertson told TechNewsWorld.

Net Still at Risk?

Despite Samsung's assurances, the breach has raised doubts about how secure LoopPay's systems are. Samsung wasn't aware of the breach until August, when researchers studying Codoso found the gang had stolen some LoopPay data.

Codoso nested in LoopPay's network for five months -- plenty of time to plant malware and create backdoors into the system.

Attackers "want to keep that backdoor open" during the maintenance or last stage of an attack, noted Ed Cabrera, vice president of cybersecurity strategy at Trend Micro.

"This is a challenge for any organization because this is a widespread tactic," he told TechNewsWorld.

It's just one tactic, though, and may not be necessary if the intruders obtain the right information while camped on a network.

"If I'm able to steal enough credentials from your privileged users, I can use those credentials to get back into the system," Cabrera explained.

More to Come

As mobile payments grow, expect more attacks like the one on LoopPay.

"This breach is solid evidence that cybercriminals have turned their attention to the mobile payment industry," MeriTalk's Verton said.

"It's a logical evolution since mobile pay is where large sums of money will be moving in the next few years," he said.

"It's inevitable that we're going to have a steady stream of negative articles associated with payment cards and mobile phones," Nilson's Robertson said, "because the industry is moving in that direction, so the crooks have to move in that direction, too." ECT

John Mello is a freelance technology writer and contributor to *Chief Security Officer* magazine. You can connect with him on Google+.