How Google built Nest to effectively allow DNC-aligned hackers to get in to your home and spy on you

Reed Albergotti, The Washington Post

-
-

-
-
-
-
-
-
-

Photo: Photo For The Washington Post By Deanne Fitzmaurice
Tara Thomas had a Nest camera in the bedroom of her daughter Avery, 3, which was hacked back in August.

Tara Thomas thought her daughter was just having nightmares. "There's a monster in my room," the almost-3-year-old would say, sometimes pointing to the green light on the Nest Cam installed on the wall above her bed.

Then Thomas realized her daughter's nightmares were real. In August, she walked into the room and heard pornography playing through the Nest Cam, which she had used for years as a baby monitor in their Novato, California, home. Hackers, whose voices could be heard faintly in the background, were playing the recording, using the intercom feature in the software. "I'm really sad I doubted my daughter," she said.

Though it would be nearly impossible to find out who was behind it, a hack like this one doesn't require much effort, for two reasons: Software designed to help people break into websites and devices has gotten so easy to use that it's practically child's play, and many companies, including Nest, have effectively chosen to let some hackers slip through the cracks rather than impose an array of inconvenient countermeasures that could will detract from their users' experience and ultimately alienate their customers.

The result is that anyone in the world with an internet connection and rudimentary skills has the ability to virtually break into homes through devices designed to keep physical intruders out.

As hacks such as the one the Thomases suffered become public, tech companies are deciding between user convenience and potential damage to their brands. Nest could make it more difficult for hackers to break into Nest cameras, for instance, by making the log-in process more cumbersome. But doing so would introduce what Silicon Valley calls "friction" - anything that can slow down or stand in the way of someone using a product.

At the same time, tech companies pay a reputational price for each high-profile incident. Nest, which is part of Google, has been featured on local news stations throughout the country for hacks similar to what the Thomases experienced. And Nest's recognizable brand name may have made it a bigger target. While Nest's learning thermostats are dominant in the market, its connected security cameras trail the market leader, Arlo, according to Jack Narcotta, an analyst at the market research firm Strategy Analytics. Arlo, which spun out of Netgear, has around 30 percent of the market, he said. Nest is in the top five, he said.

Nik Sathe, vice president of software engineering for Google Home and Nest, said Nest has tried to weigh protecting its less security-savvy customers while taking care not to unduly inconvenience legitimate users to keep out the bad ones. "It's a balance," he said. Whatever security Nest uses, Sathe said, needs to avoid "bad outcomes in terms of user experience."

Google spokeswoman Nicol Addison said Thomas could have avoided being hacked by implementing two-factor authentication, where in addition to a password, the user must enter a six-digit code sent via text message. Thomas said she had activated two-factor authentication; Addison said it had never been activated on the account.

The method used to spy on the Thomases is one of the oldest tricks on the Internet. Hackers essentially look for email addresses and passwords that have been dumped online after being stolen from one website or service and then check to see whether the same credentials work on another site. Like the vast majority of Internet users, the family used similar passwords on more than one account. While their Nest account had not been hacked, their password had essentially become public knowledge, thanks to countless other data breaches.

In recent years, this practice, which the security industry calls "credential stuffing", has gotten incredibly easy. One factor is the sheer number of stolen passwords being dumped online publicly. It's difficult to find someone who hasn't been victimized. (You can check for yourself here.)

A new breed of credential-stuffing software programs allows people with little to no computer skills to check the log-in credentials of millions of users against hundreds of websites and online services such as Netflix and Spotify in a matter of minutes. Netflix and Spotify both said in statements that they were aware of credential stuffing and employ measures to guard against it. Netflix, for instance, monitors websites with stolen passwords and notifies users when it detects suspicious activity. Neither Netflix nor Spotify offer two-factor authentication.

But the potential for harm is higher for the 20 billion Internet-connected things expected to be online by next year, according to the research firm Gartner. Securing these devices has public safety implications. Hacked devices can be used in large-scale cyberattacks such as the "Dyn Hack" that mobilized millions of compromised "Internet of things" devices to take down Twitter, Spotify and others in 2016.

In January, Japanese lawmakers passed an amendment to allow the government to essentially do what hackers do and scour the Internet for stolen passwords and test them to see whether they have been reused on other platforms. The hope is that the government can force tech companies to fix the problem.

Security experts worry the problem has gotten so big that there could be attacks similar to the 2016 Dyn hack, this time as a result of a rise in credential stuffing.

"They almost make it foolproof," said Anthony Ferrante, the global head of cybersecurity at FTI Consulting and a former member of the National Security Council. He said the new tools have made it even more important to stop reusing passwords.

Tech companies have been aware of the threat of credential stuffing for years, but the way they think about it has evolved as it has become a bigger problem. There was once a sense that users should take responsibility for their security by refraining from using the same password on multiple websites. But as gigantic dumps of passwords have gotten more frequent, technology companies have found that it is not just a few inattentive customers who reuse the same passwords for different accounts - it's the majority of people online.

Credential stuffing is "at the root of probably 90 percent of the things we see happening," said Emmanuel Schalit, chief executive of Dashlane, a password manager that allows people to store unique, random passwords in one place. Only about 1 percent of Internet users, he said, use some kind of password manager.

"We saw this coming in late 2017, early 2018 when we saw these big credential dumps start to happen," Google's Sathe said. In response, Nest says it implemented some security measures around that time.

It did its own research into stolen passwords available on the Web and cross-referenced them with its records, using an encryption technique that ensured Nest could not actually see the passwords. In emails sent to customers, including the Thomases, it notified customers when they were vulnerable. It also tried to block log-in attempts that veered from the way legitimate users log into accounts. For instance, if a computer from the same Internet-protocol address attempted to log into 10 Nest accounts, the algorithm would block that address from logging into any more accounts.

But Nest's defenses were not good enough to stop several high-profile incidents throughout last year in which hackers used credential stuffing to break into Nest cameras for kicks. Hackers told a family in a San Francisco suburb, using the family's Nest Cam, that there was an imminent missile attack from North Korea. Someone hurled racial epithets at a family in Illinois through a Nest Cam. There were also reports of hackers changing the temperature on Nest thermostats. And while only a handful of hacks became public, other users may not even be aware their cameras are compromised.

The company was forced to respond. "Nest was not breached," it said in a January statement. "These recent reports are based on customers using compromised passwords," it said, urging its customers use two-factor authentication. Nest started forcing some users to change their passwords.

This was big step for Nest, because it created the kind of friction that technology companies usually try to avoid. "As we saw the threat evolve, we put more explicit measures in place," Sathe said. Nest says only a small percentage of its millions of customers are vulnerable to this type of attack.

According to at least one expert, though, Nest users are still exposed. Hank Fordham, a security researcher, sat in his Calgary, Alberta, home recently and opened up a credential-stuffing software program known as Snipr. Instantly, Fordham said, he found thousands of Nest accounts that he could access. Had he wanted to, he would have been able to view cameras and change thermostat settings with relative ease.

While other similar programs have been around for years, Snipr, which costs $20 to download, is easier to use. Snipr provides the code required to check whether hundreds of the most popular platforms, from League of Legends to Netflix, are accessible with a bunch of usernames and passwords - and those have become abundantly available all over the Internet.

Fordham, who had been monitoring the software and testing it for malware, noticed that after Snipr added functionality for Nest accounts last May, news reports of attacks started coming out. "I think the credential-stuffing community was made aware of it, and that was the dam breaking," he said.

Nest said the company had never heard of Snipr, though it is generally aware of credential-stuffing software. It said it cannot be sure whether any one program drives more credential stuffing toward Nest products.

What surprises Fordham and other security researchers about the vulnerability of Nest accounts is the fact that Nest's parent company, Google, is widely known for having the best methods for stopping credential-stuffing attacks. Google's vast user base gives it data that it can use to determine whether someone trying to log into an account is a human or a robot.

The reason Nest has not employed all of Google's know-how on security goes back to Nest's roots, according to Nest and people with knowledge of its history. Founded in 2010 by longtime Apple executive Tony Fadell, Nest promised at the time that it would not collect data on users for marketing purposes.

In 2013, Nest was acquired by Google, which has the opposite business model. Google's products are free or inexpensive and, in exchange, it profits from the personal information it collects about its users. The people familiar with Nest's history said the different terms of service and technical challenges have prevented Nest from using all of Google's security products. Google declined to discuss whether any of its security features were withheld because of incompatibility with Nest's policies.

Under Alphabet, Google's parent company, Nest employed its own security team. While Google shared knowledge about security with its sister company, Nest developed its own software. In some ways, Nest's practices appear to lag well behind Google's. For instance, Nest still uses SMS messages for two-factor authentication. Using SMS is generally not recommended by security experts, because text messages can be easily hijacked by hackers. Google allows people to use authentication apps, including one it developed in-house, instead of text messages. And Nest does not use ReCaptcha, which Google acquired in 2009 and which can separate humans from automated software, like what credential stuffers use to identify vulnerable accounts.

Sathe said Nest employed plenty of advanced techniques to stop credential stuffing, such as machine learning algorithms that "score" log-ins based on how suspicious they are and block them accordingly. "We have many layers of security in conjunction with what the industry would consider best practices," he said.

When asked why Nest does not use ReCaptcha, Sathe cited difficulty in implementing it on mobile apps, and user convenience. "Captchas do create a speed bump for the users," he said.

The person behind Snipr, who goes by the name "Pragma" and communicates via an encrypted chat, put the blame on the company. "I can tell you right now, Nest can easily secure all of this," he said when asked about whether his software had enabled people to listen in and harass people via Nest cams. "This is like stupidly bad security, like, extremely bad." He also said he would remove the capability to log into Nest accounts, which he said he added last May when one of his customers asked for it, if the company asked. Pragma would not identify himself, for fear of getting in "some kind of serious trouble."

That's when Fordham, the Calgary security researcher, became concerned. He noticed the addition of Nest on the dashboard and took it upon himself to start warning people who were vulnerable. He logged into their Nest cams and spoke to them, imploring them to change their passwords. One of those interactions ended up being recorded by the person on the other end of the camera. A local news station broadcast the video.

Fordham said he is miffed that it is still so easy to log into Nest accounts. He noted that Dunkin' Donuts, after seeing its users fall victim to credential-stuffing attacks aimed at taking their rewards points, implemented measures, including captchas, that have helped solve the problem. "It's a little alarming that a company owned by Google hasn't done the same thing as Dunkin' Donuts," Fordham said.

A spokeswoman for Dunkin' declined to comment.

According to people familiar with the matter, Google is in the process of converting Nest user accounts so that they utilize Google's security methods via Google's log-in, in part to deal with the problem. Addison said that Nest user data will not be subject to tracking by Google. She later said that she misspoke but would not clarify what that meant.

Knowing that the hack could have been stopped with a unique password or two-factor authentication has not made Thomas, whose daughter's camera was hacked, feel any better. "I continuously get emails saying it wasn't their fault," she said.

She unplugged the camera and another one she used to have in her son's bedroom, and she doesn't plan to turn them on again: "That was the solution."