TechXplore

Security camera hack exposes hospitals, workplaces, schools

March 10 2021, by Matt O'brien and Frank Bajak

In this March 4, 2020 file photo, a security camera is shown on the second floor of a row of rooms at a motel in Kent, Wash. Hackers aiming to call attention to the dangers of mass surveillance said they were able to peer into hospitals, schools, factories, jails and corporate offices after they broke into the systems of a security-camera startup. That California startup, Verkada, said Wednesday, March 10, 2021, it is investigating the scope of the breach, first reported by Bloomberg, and has notified law enforcement and its customers. (AP Photo/Ted S. Warren)

Hackers aiming to call attention to the dangers of mass surveillance say they were able to peer into hospitals, schools, factories, jails and corporate offices after they broke into the systems of a security-camera startup.

That California startup, Verkada, said Wednesday it is investigating the scope of the breach, first reported by Bloomberg News, and has notified law enforcement and its customers.

Swiss hacker Tillie Kottmann, a member of the group that calls itself APT-69420 Arson Cats, described it in an online chat with The Associated Press as a small collective of "primarily queer hackers, not backed by any nations or capital but instead backed by the desire for fun, being gay and a better world."

They were able to gain access to a Verkada "super" administrator account using valid credentials found online, Kottmann said. Verkada said in a statement that it has since disabled all internal administrator accounts to prevent any unauthorized access.

But for two days, the hackers said, they were able to peer unhindered into live feeds from potentially tens of thousands of cameras, including many that were watching sensitive locations such as hospitals and schools. Kottmann said that included outdoor and indoor cameras at Sandy Hook Elementary School in Newtown, Connecticut, where 26 first-grade students and six educators were killed in 2012 by a gunman in one of the deadliest school shootings in U.S. history.

The school district's superintendent didn't return calls or emailed requests for comment Wednesday.

One of Verkada's affected customers, the San Francisco web infrastructure and security company Cloudflare, said the compromised Verkada cameras were watching entrances and main thoroughfares to some of its offices that have been closed for nearly a year due to the pandemic.

"As soon as we were notified of the breach, we proceeded to shut down the cameras in all our office locations to prevent further access," said John Graham-Cumming, the company's chief technology officer, in a blog post. "To be clear: this hack affected the cameras and nothing else."

Another San Francisco tech company, Okta, said five cameras it placed at office entrances were compromised, though there's no evidence anyone viewed the live streams. At Cloudfare, videos of an office lobby downloaded by the hackers actually date from last summer and had been saved for a theft investigation, Graham-Cumming said.

Twitter said it permanently suspended Kottmann's account, which posted materials gathered in the hack, for violating its rules against ban-evasion, which typically happens when users start a new account to circumvent an earlier suspension. Kottmann had earlier received a message from Twitter suspending the account for violating its rules against the distribution of hacked material, the hacker said.

The Verkada footage captured and shared by hackers appeared to include a Tesla facility in China and the Madison County Jail in Huntsville, Alabama. Madison County Sheriff Kevin Turner said in a statement Wednesday the jail has taken the cameras offline, adding "we are confident that this unauthorized release did not and will not impact the safety of staff or inmates." Tesla didn't respond to requests for comment.

Verkada, based in San Mateo, California, has pitched its cloud-based surveillance service as part of the next generation of workplace security. Its software detects when people are in the camera's view, and a "Person History" feature enables customers to recognize and track individual faces and other attributes, such as clothing color and likely gender. Not all customers use the facial recognition feature.

The company attracted negative attention last year when video surveillance industry news site IPVM reported that Verkada employees had passed around photos of female coworkers collected by the company's own in-office cameras and made sexually explicit comments about them.

Cybersecurity expert Elisa Costante said it's worrisome that this week's hack wasn't sophisticated and simply involved using valid credentials to access a huge trove of data stored on a cloud server.

"What is disturbing is to see how much real-life data can go into the wrong hands and how easy it can be," said Costante, vice president of research at Forescout. "It's a wake up call to make sure that whenever you are collecting this much data we need to have basic security hygiene."

Kottmann said the hacker collective, active since 2020, doesn't set out after specific targets. Instead, it scans organizations on the internet for known vulnerabilities and then works to "just narrow down and dig in on interesting targets."

Citation: Security camera hack exposes hospitals, workplaces, schools (2021, March 10) retrieved 1 May 2024 from
https://techxplore.com/news/2021-03-camera-hack-exposes-hospitals-workplaces.html