Verkada Breach

Established in 2016, Verkada sells a full suite of physical security monitoring tools that will watch your everyday spaces with devices like indoor and outdoor cameras, door entry regulations, and tools for movement, heat, and sound. The hardware, provided by Silicon Valley, links to the web through Verkada's security cloud, granting clients the capability of storing and observing real-time feeds from anywhere with internet access.

Verkada's clients can also leverage the use of the corporation's AI characteristics to locate someone as they are doing their daily routines. Verkada's software allows clients to routinely follow anyone in their viewing areas—by facial recognition, the pigment of their wardrobe, whether they are carrying a bag, and or even their gender.

Businesses in this security vertical promote that their integrated exploration devices increase community protection as well as maintain citizens' safety through identifying hazards or preventing crime before it happens.

(GDPR, 2018)

On **March 10, 2021**, Bloomberg News reported that Verkada experienced an alarming discovery. At 4:17 PM CST, Verkada announced they had been breached, reporting that 140k+ cameras had been exposed.

So far forensic analysis indicates that attackers obtained admission on Monday, March 8th to view the footage.

Businesses are discovering the need to deliver added protection; however, this can result in outbreaks to their clients. It has become easier for hackers to steal information and view people without them knowing. For example, there have been several reports from the breach showing people doing their normal daily routines; the security officer on the night shift; individuals resting in a hospital waiting room; employees on the level of an industrial factory. Following the breach, the videos were quickly discovered by attackers, who had exploited high-ranking certificates to communicate as well as steal Verkada's massive network.

One of the hackers distributed some of the breached data to reporters at The Washington Post to highlight the security risk of extensive surveillance equipment that exposes society to a continuous view.

Verkada, which promotes that their cameras are "protected on or after the base up," has informed law administration and is currently examining the extent combined with the scale of the violation.

Switzerland-based Tillie Kottmann, main participant of the Hacktivist group responsible for the breach, indicated the group came across specifics from Verkada's "Super Admin" account which has been openly revealed. Once Kottmann hacked their system, she stated that the group was shocked by the amount of real-time footage they could see.

Kottmann says, "It still feels incredibly surreal the amount of foothold I was able to gain from this hit. That is the irony of this whole thing: All the cool features they provide for security are exactly why everything broke."

Verkada's Consumer Registry was also leaked to The Washington Post, providing more proof that the severity of the attack was serious as the registry contains more than twenty thousand associations.

Several of the breached snapshots revealed the isolated areas during the time of the pandemic. The hackers could see an empty school, offices, and more. A Cloudflare (Verkada's VPN) representative stated the Verkada recordings of the heavily guarded locations that must remain concealed from the public eye, were immediately disconnected when the breach was discovered.

The technology director for Surveillance Technology Development, a charitable activism unit, stated businesses' accumulation of private recordings as well as additional private information has left them under continuous attack. As technology grows, vulnerabilities grow as well. Hackers will always find a way to confiscate your sensitive data no matter how much technology changes. The director of this project confirmed exactly how some sites, for instance, Insecam, authorizes everyone to observe open and indiscreet cameras.

Ferguson, Verkada's Surveillance Technology Development director reports, "This is the hypocrisy of the surveillance network: Anything you create under the guise of making more safety is a tool that can be turned against you," and "The more we centralize power into the hands of a few tech companies, the more at risk we are of things like this,". Lastly "for every one of these you hear about, there are 10 others you don't."

(Creating a Company Data Breach Response Plan)

This attack has brought up additional questions specifically regarding how much the personnel at Verkada can view from their clients' recordings. Charles Rollet, the head of Verkada's surveillance division, stated that a source within the company admits that Verkada's personnel can access clients' records at any period, without the customers' permission.

Rollet says, "Verkada sold their system as particularly advanced in terms of privacy and security, which is ironic when you look at what happened,". Also, he said, "People do not realize what happens on the back end, and they assume that there are always these super-formal processes when it comes to accessing footage and that the company will always need to give explicit consent. But clearly, that's not always the case."

In the previous year, the corporation dismissed a few personnel per allegations that they have used the corporation's cameras to take snapshots as well as make erotic jokes regarding their female associates. This has continuously remained a problem at other tech companies, like the surveillance company Ring, which has also dismissed personnel for the same reason.

Ferguson expresses, "The breach is unusual and terrible, but we probably should be more concerned with what we think is normal and fine about digital surveillance technologies.". He continues, "Every video stream, sensor upload and the digital trail we create is vulnerable to illegal interception by hackers and lawful acquisition by police,".

March 12, 2021, Swiss agencies confiscated the electronics from Tillie Kottmann's home, the hacker pleaded guilty to distributing footage and sensitive data from Verkada's clients. Social media posts to Kottman's now-eliminated feed indicate the hacker as well as potential partners — utilizing the moniker "APT-69420 Arson Cats" — had pursued the enterprises apparently out of interest.

Organizations that do business with Verkada should be on the lookout for an increase in phishing attacks as the names and email addresses for the account administrators have been compromised. RAVENii recommends that you notify your employees to report any suspicious emails to your help desk.

RAVENii will continue to track and monitor this issue.

Harwell, D. (2021, March 10). *Massive camera hack exposes the growing reach and intimacy of American surveillance*. Retrieved from Washington Post: https://www.washingtonpost.com/technology/2021/03/10/verkada-hack-surveillance-risk/