Joshua Russell
CS 462

The Attack of Verkada Security Systems

Introduction

In recent years, cyber-attacks have become a regular occurrence; in 2023 alone, more than 340 million people were victims of cyber-attacks (St. John, 2024) and the numbers will continue to increase. Exploiting these vulnerabilities for monetary purposes, cyber warfare, revenge, or reconnaissance is becoming more common and more frequent. Data breaches and exploitations are increasing, as information is becoming the new currency. On March 9, 2021, cloud-based identity management service firm Okta was the victim of a hack that involved their security monitoring systems provided by cloud-based provider Verkada. Security footage from the Okta offices was downloaded from the camera systems and root shell access of the Okta networks was granted to hackers because of a faulty misconfigured server at a Verkada data center. This was just one of the companies that hacker collective “Advanced Persistent Threat 69420” penetrated in the attack of Verkada (Turton and Gretler, 2021). In addition, the culprits were able to access the cameras footage of a Tesla facility, a Virgin Hyperloop facility, Fortune 500 companies, schools, jails, hospitals, and homes. Overall, 150,000 surveillance cameras were exposed during this attack. In the digital age, the Verkada hack is one example of how third-party services and IoT devices are susceptible to exploitation, how cloud services are vulnerable to attacks, and how privacy is of utmost importance.

Background

Verkada is a Silicon Valley startup firm that was founded in 2016 by three Stanford University graduates, Filip Kaliszan, James Ren, and Benjamin Bercovitz. Verkada is a cloud-based company that provides security / monitoring and facial recognition services for businesses over the Amazon (AWS) networks. They offer a web-based interface for their clients to watch the feeds of the security systems, and they employ facial recognition software by way of software-as-a-service (SaaS), infrastructure-as-a-service (IasS), and platform-as-a-service framework models (Verkada, 2021). Cloud-based networks and systems are becoming more prevalent with companies looking for reduced infrastructure and lower costs, but these technologies are riddled with problems. With the increase usage of cloud-based technologies, these vulnerabilities become targets that hackers look to exploit. Companies such as Okta, Tesla, Cloudflare, Halifax Health, a Florida hospital; Sandy Hook Elementary School in Newtown, Connecticut; Madison County Jail in Huntsville, Alabama; and Wadley Regional Medical Center, a hospital in Texarkana, Texas all use their software for security monitoring (Gartenberg, 2021).

The Attackers

Advanced Persistent Threat 69420 (APT69420) was a hacker collective led by Swiss national Tillie Kottman also known as Maia Arson Crimew. Born in Lucerne, Switzerland, Tillie Kottman was a computer software developer and a self-described “white hat” hacker who worked in information technology. At the time, Kottman, who goes by they/them pronouns, was 21 years old and had experience hacking systems, releasing information and documents, and had been implicated in several earlier attacks (Miller, 2021). While Advanced Persistent Threat 69420 was a hacker collective, only Tillie was attributed to the attack against the Verkada network, as they are the public face of the group. Speaking to Bloomberg Magazine, Kottman says of the attack, "its lots of curiosity, fighting for freedom of information and against intellectual property, a huge dose of anti-capitalism, a hint of anarchism - and it's also just too much fun not to do it" (Turton and Gretler, 2021). Tillie considers themselves a hacktivist, and this attack was meant to shine a light on the practice of surveillance capitalism.

The Attack

In March of 2021, APT 69420 breached the Verkada network through a security weak point and failure. Hackers gained administrative privileges by to Verkada systems by using usernames and passwords found publicly on the internet. Hackers gained access through a misconfigured customer support server that was mistakenly exposed to the internet. Once that server was accessed, the hackers found customer support administrator usernames and passwords, and then logged into the customer support web interface. After that, the hackers were able to access Verkada’s network with root access to penetrate the cameras themselves, which allowed the group to access the internal networks of some of Verkada’s customers through an internal support function that mimicked emulated user sessions (Verkada, 2021). When APT 69420 infiltrated the network, they had access to the system for 36 hours. Once inside the network, the hackers stole source code, hard coded user credentials, git repositories, files, and access codes of over one hundred companies. In addition, several companies had their private networks penetrated through these stolen codes and credentials (Miller, 2021). Through the security infrastructure of Okta, hackers were able to gain root shell access of Okta's network and infiltrate their databases which held user credentials necessary for single sign on and multifactor authentication services. This is just one of the examples of how vulnerabilities of one system can lead to the access of another system that is connected by the network.

Effects

As understood, nothing is inherently secure in our increasingly online society. The attack of Verkada ushered in a wide range of vulnerabilities that many of the companies who implemented their services exposed. During the attack, more than 150,000 security cameras were accessed; downloaded and archived videos were also stolen and compiled to a hard drive. Prisons, psychiatric hospitals, clinics, and Verkada's own office security feeds were leaked. Video footage of a Florida hospital shows eight workers tackling and pinning a patient to a bed, another video shows a man in Stoughton, Massachusetts handcuffed and being questioned inside of a police station, and prisoners in Madison County Jail in Huntsville, Alabama were all stolen. Information security company Cloudflare and single-sign-on/multifactor authentication service provider Okta had their security systems leaked. Richard Branson's company Virgin Hyperloop facilities and Elon Musk's Tesla facilities in Shanghai were also victims of this attack (BBC, 2021). Additionally, cameras were found inside various Internet of Things (IoT) devices such as defibrillators and thermostats, and hidden cameras were exposed in ventilation systems. Many of these monitoring systems also provided audio access, which was also stolen and leaked including a police station interrogation. Subsequently, when the attack was discovered on March 9, 2021, Verkada executed mitigation techniques to regain control and evict the hackers from their systems. "We have disabled all internal administrator accounts to prevent any unauthorized access. Our internal security team and external security firm are investigating the scale and scope of this potential issue" (Gartenberg, 2021). By doing so, APT 69420 lost access to the company's live security feeds and the archival footage. Regarding Tillie, in March of 2021, Kottman was indicted by a grand jury in the Unted States with criminal charges relating to hacking attacking from 2019-2021. The charges included one count of conspiracy to commit computer fraud and abuse, several counts of wire fraud, one count of conspiracy to commit wire fraud, and one count of aggravated theft (Alder, 2021). In coordination with the United States, Swiss authorities raided the home of Kottman and seized equipment.

Societal Implications

This attack had broad implications for society on privacy and security, and of companies and individuals in government, public, and private sectors. The actions taken by Tillie Kottman cannot be considered an act of free speech, as they claim. Unauthorized access, stolen credentials, and stolen data are criminal acts under the Computer Fraud and Abuse Act of 1986 (CFAA). 18 U.S. Code § 1030 (a)states that "Whoever— intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— information from any department or agency of the United States; or information from any protected computer; shall be punished…" (U.S. Criminal Code). In the big picture, the attack on Verkada raised serious concerns for data security and privacy. One of the biggest concerns the Verkada hack exposed was privacy issues and ethical considerations. Because live feeds were exposed in sensitive areas like a hospital, a prison, and a police station interrogation room, it raises questions about privacy and the use of surveillance in sensitive settings. The question also raises thought, is it necessary that security systems need to be accessible online, or can they be just as effective as a closed-circuit, onsite monitoring system? Another concern exposed by this hack is the aspect of regulatory implications and corporate responsibilities, which highlights the need for stricter regulations regarding IoT devices, standards for security protocols, and compliance with data protection laws. Lastly, this attack had serious implications of exposing trade secrets and confidential practices of companies such as Tesla and Virgin in their production facilities. Overall, the hack of Verkada had widespread implications for privacy concerns, security of systems and networks, and regulations of devices used in settings understood as sensitive or confidential.

Joshua Russell
CS 462

Conclusion

In summary, the attack of Verkada systems and networks exemplifies the vulnerabilities and opportunities devices and IoT devices have that can be exploited. Cyber-attacks have become increasingly common, as hackers seek to exploit vulnerabilities for personal gain or for the greater good. With more devices entering the market that can connect to the internet and wireless networks, companies increase the risk of becoming victims to attacks. The example of the Verkada hack displays the importance of privacy and security of companies in the digital age, especially when it touches all sectors. Government entities, private businesses, and individuals all seeking services from third parties should ensure that policies and procedures are in place to reduce risk, maintain reputational standing with clients, and reinforce security and confidentiality. Whether it be a nation-state actor, foreign, or domestic terrorist attacks on the infrastructure of governments, companies, and individual citizens will continue to increase exponentially, but with careful planning and diligence threats can be limited and mitigated.

Joshua Russell
CS 462

Works Cited

Alder, S. (2021, March 22). *Verkada Surveillance Camera Hacker Indicted on Multiple Counts of Conspiracy, Wire Fraud and Aggravated Identity Theft*. Retrieved from www.hipaajournal.com: https://www.hipaajournal.com/verkada-surveillance-camera-hacker-indicted-on-multiple-counts-of-conspiracy-wire-fraud-and-aggravated-identity-theft/

BBC Technology. (2021, March 10). *Hack of '150,000 cameras' investigated by camera firm*. Retrieved from www.bbc.com: https://www.bbc.com/news/technology-56342525

Cornell Law School Legal Information Institute. (n.d.). *18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computers*. Retrieved from www.law.cornell.edu: https://www.law.cornell.edu/uscode/text/18/1030

Gartenberg, C. (2021, March 9). *Security Startup Verkada Hack Exposes 150,000 Security Cameras in Tesla Factories, Jails, and More*. Retrieved from www.theverge.com: https://www.theverge.com/2021/3/9/22322122/verkada-hack-150000-security-cameras-tesla-factory-cloudflare-jails-hospitals

Miller, M. (2021, March 19). *Justice Department Indicts Hacker Connected to Massive Surveillance Camera Breach*. Retrieved from www.thehill.com: https://thehill.com/policy/cybersecurity/544063-justice-department-indicts-hacker-connected-to-massive-surveillance/

St. John, M. (2024, August 28). *Cybersecurity Stats: Facts And Figures You Should Know*. Retrieved from www.forbes.com: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/#:~:text=The%20year%202023%20saw%20a%20notable%20increase%20in,cyberattacks%2C%20resulting%20in%20more%20than%20343%20million%20victims.

Turton, W., & Gretler, C. (2021, March 12). *Swiss Police Raid Apartment of Verkada Hacker, Seize Devices*. Retrieved from www.bloomberg.com: https://web.archive.org/web/20210315192331/https://www.bloomberg.com/news/articles/2021-03-12/swiss-police-raid-apartment-of-verkada-hacker-seize-devices

U.S. Attorney's Office, Western District of Washington. (2021, March 18). *Swiss Hacker Indicted for Conspiracy, Wire Fraud, and Aggravated Identity Theft*. Retrieved from www.justice.org: https://www.justice.gov/usao-wdwa/pr/swiss-hacker-indicted-conspiracy-wire-fraud-and-aggravated-identity-theft

Joshua Russell
CS 462

Verkada. (2021, March 9). *Summary: March 9, 2021 Security Incident Report*. Retrieved from www.verkada.com: https://www.verkada.com/security-update/report/

Wikipedia. (n.d.). *maia arson crimew*. Retrieved from www.wikipedia.com: https://en.wikipedia.org/wiki/Maia_arson_crimew#cite_note-:5-32