March 30th, 2021

Hacking Healthcare

TLP White

This week, *Hacking Healthcare* begins by breaking down how a fire experienced by a French cloud provider impacted millions, is a perfect example of cascading effects, and demonstrates how reliance on the cloud isn't foolproof. Next, we dive into the Verkada breach to examine third-party risk and how security services themselves can present security and privacy risks. Finally, we look at how a well-intentioned attempt to notify a company of its data leak led to the involvement of lawyers and the frustration of proponents of ethical reporting. Welcome back to *Hacking Healthcare*.

1. Fire at Cloud Provider's Data Center Impacts Millions

While cloud services undoubtedly offer significant security and productivity advantages, organizations using the cloud may have the tendency to fall into a trap of "out of sight, out of mind." This often happens despite attempts from some of the major cloud providers to make it clear that cloud customers themselves always retain responsibility for their data.[1, 2] However, as events in France at the beginning of March show, even organizations following such shared responsibility models can be unexpectedly caught out by physical threats to cloud infrastructure.

On March 10th, a fire broke out at a cluster of four OVHcloud data centers in Strasbourg, France. Despite whatever fire prevention was present in the building and a rapid response from firefighters, one of the data centers was completely destroyed and another was damaged.[3] The impact of the disaster was immediate, as "millions of websites, including government agencies, banks, shops, news websites and […] a chunk of the .FR webspace" were knocked offline.[4] In response, the cloud provider informed their customers they should begin to implement their own disaster recovery plans. Although OVHcloud hoped that some of the data lost could be reconstructed, some customers appear to have lost everything.[5, 6]

Recovery and investigative operations moved in tandem in the ensuing weeks, with early indications suggesting that an uninterruptible power supply (UPS) is the likely culprit behind the fire. Disconcertingly, OVHcloud confirmed a second incident just over a week later at one of the cluster's other data centers. Reportedly, smoke was found in a battery room, prompting a shutdown of the entire Strasbourg cluster of data centers as firefighters were called to clear the site.[7]

One small consolation to the sudden disruption of 3.6 million websites on 464,000 distinct domains was that the fire also disrupted a chunk of cybercriminal command and control servers. According to Costin Raiu, the director of the Global Research and Analysis Team (GReAT) at Kaspersky Lab, "[o]ut of the 140 known C2 servers we are tracking at OVH that are used by APT and sophisticated crime groups, approximately 64% are still online" "The affected 36% include several APTs: Charming Kitten, APT39, Bahamut and OceanLotus,"[8] he continued.

Action & Analysis
H-ISAC Membership Required

2. Verkada Breach Highlights Security and Privacy Concerns

One of the more startling news stories of the past month was the announcement from a group of hackers that they had access to roughly 150,000 live camera feeds due to their breach of security-camera startup Verkada. The breach exposed a wide range of Verkada clients, which included schools, prisons, pharmaceutical companies, hospitals and a host of others.[9, 10] The resulting media coverage has ignited debates around privacy and surveillance, facial recognition, and cybersecurity in general.

First reported by Bloomberg, the breach allegedly occurred after “Verkada exposed an unprotected internal development system to the Internet,” which “contained credentials for an account that had super admin rights to the Verkada network.”[11] The hackers behind the attack stated that this access allowed them to view Verkada client cameras and those clients’ full video archives, as well as let them exfiltrate 5GBs of data.[12]

While the hackers that perpetrated the attack allegedly did so “to show the pervasiveness of video surveillance and the ease with which systems could be broken into,” there is no doubt that a group with less of a public activist agenda could easily have gone undetected for an unknowable amount of time.[13] Worse, the hackers claim that they were “able to obtain ‘root’ access on the cameras, meaning they could use the cameras to execute their own code.”[14] Such access could potentially have let them expand access to the networks of the individual clients.

Fortunately, it appears at least one of the individuals behind the attack may face a penalty for doing so. The US Department of Justice filed charges against Tillie Kottmann, a Swiss national who has been vocal in describing her involvement. She was “indicted Thursday by a grand jury in the Western District of Washington on multiple counts of wire fraud, identity theft, and computer fraud and abuse.”[15] For the moment, Swiss authorities appear to be cooperating with US authorities on the matter.

Action & Analysis
H-ISAC Membership Required

3. Engineer Reports Data Leak to Nonprofit, Hears from the Police

Legal drama is unfolding after a computer engineer reported a data leak to a UK-based non-profit. The computer engineer, Rob Dyke, discovered a GitHub repository that exposed passwords, API keys, and other sensitive financial records belonging to the Apperta Foundation. Dyke then privately reported the leaked information to the foundation and received a thank you note for the notice. However, only a couple days later, he received legal correspondence from the Apperta Foundation followed by a note from the police in response to a report of computer misuse.

Dyke, in a recent interview, explained how he had worked with the Apperta Foundation in the past and was familiar with both the foundation's policies and industry best practices when it comes to reporting security vulnerabilities to vendors.[16] He explained how he had encrypted the data showing the exposed passwords, API keys, and other financial records to store it for 90 days as a step in the coordinated disclosure process. Furthermore, Dyke clarified his actions by stating that the information he found had been leaked publicly for two years and was not obtained by unlawful hacking.

Dyke's legal issues stem from the UK Computer Misuse Act of 1990, a 31-year-old piece of legislation which has broad and outdated language that could consider finding a data leak a violation of the Act. As technology has undergone tremendous transformations over the past several decades, older legislation that hasn't been updated is becoming increasingly problematic. In the UK, a recent survey found that 80% of security professionals were worried about violating the UK Computer Misuse Act of 1990 during their day-to-day professional duties.[17]

Action & Analysis
H-ISAC Membership Required

Congress –

Tuesday, March 30th:
- No relevant hearings

Wednesday, March 31st:
- No relevant hearings

Thursday, April 1st:
- No relevant hearings

International Hearings/Meetings –

- No relevant hearings

EU –

- No relevant hearings

Conferences, Webinars, and Summits –

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[2] https://aws.amazon.com/compliance/shared-responsibility-model/
[3] https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU
[4] https://www.reuters.com/article/us-france-ovh-fire-idUSKBN2B20NU
[5] https://www.datacenterdynamics.com/en/news/ovh-fire-ovhcloud-abandons-efforts-restart-sbg1-strasbourg/
[6] https://blog.malwarebytes.com/malwarebytes-news/2021/03/ovh-cloud-datacenter-destroyed-by-fire/
[7] https://www.datacenterdynamics.com/en/news/ovhcloud-firefighters-return-second-incident-strasbourg/
[8] https://www.infosecurity-magazine.com/news/ovh-data-center-fire-impacts/
[9] https://www.cyberscoop.com/verkada-breach-surveillance-facial-recognition-privacy/
[10] https://www.vice.com/en/article/wx83bz/verkada-hacked-facial-recognition-customers
[11] https://arstechnica.com/information-technology/2021/03/hackers-access-security-cameras-inside-cloudflare-jails-and-hospitals/
[12] https://arstechnica.com/information-technology/2021/03/hackers-access-security-cameras-inside-cloudflare-jails-and-hospitals/
[13] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
[14] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
[15] https://thehill.com/policy/cybersecurity/544063-justice-department-indicts-hacker-connected-to-massive-surveillance
[16] https://www.bleepingcomputer.com/news/security/engineer-reports-data-leak-to-nonprofit-hears-from-the-police/
[17] https://www.bleepingcomputer.com/news/security/engineer-reports-data-leak-to-nonprofit-hears-from-the-police/