



Data breaches and malware

A cautionary tale for cyber security in the education sector

30 July 2021






 www.snode.com
 info@snode.com
 +27 12 880 0989

Table of contents

1. Introduction	2
<i>a. The risks of school data breaches</i>	2
2. A school under attack	2
3. Discoveries	3
4. Aggressive, military-grade malware	3
5. A global threat to minors' security	3
<i>a. Unforeseen cyber risks</i>	4
6. Response and remediation	4
7. Security assurance through a proactive approach	5
8. About Snode Technologies	5
9. Author	5
10. References	6

Introduction

The risks of school data breaches

In a rapidly digitised world as a consequence of COVID-19, institutions in both the private and public sectors are increasingly reliant on digital infrastructure to operate. Though the globe has been acclimatising to the Fourth Industrial Revolution for several years, many African countries have found it challenging to adapt to this developing digital ecosystem, particularly in the realm of cyber security.

No stranger to this transformation is the education sector, who have had to adapt to rapid technological advancements to both digitise their operations and support online learning. Schools have become increasingly reliant on digital means to provide a 21st century education, including interactive learning on tablets and laptops, completing online assessments and tests, or using software programmes for compiling student reports, and moving towards storing important information in electronic format (CFC, 2020). For all the benefits created from employing technology in schools, it also introduces new challenges: threats to the confidentiality, availability and integrity of their data systems and technology from parties both internal and external from the educational institution (Levin, 2020).

These often-unmonitored digital avenues mean that schools are vulnerable to cyber security breaches, whether they store their information on-site or on a cloud-based network. A data breach can occur through a variety of innocent sources, such as an educator unknowingly sharing information with a third party, publishing a password list on a publically accessible internal domain, or utilising a security system that is inadequately geared to defend against potential attacks.

As screen time is more prevalent than ever for children - both at school and at home - the potential threat for data breaches has increased exponentially. A cyber attack on a youth could result in the exposure of sensitive information such as ID numbers, home addresses, geolocations, online content, medical information and banking details - which could be used for insidious means.

A school under attack

In August of 2020, a prominent high school in Gauteng, South Africa noticed that their internal network was running extremely slowly, and at times was completely unavailable. This impacted the school's access to resources on the internal server, thus limiting students' access to textbooks on their tablet devices and computers within the school's laboratory and library, and rendering teachers unable to present learning materials via their digital whiteboards.

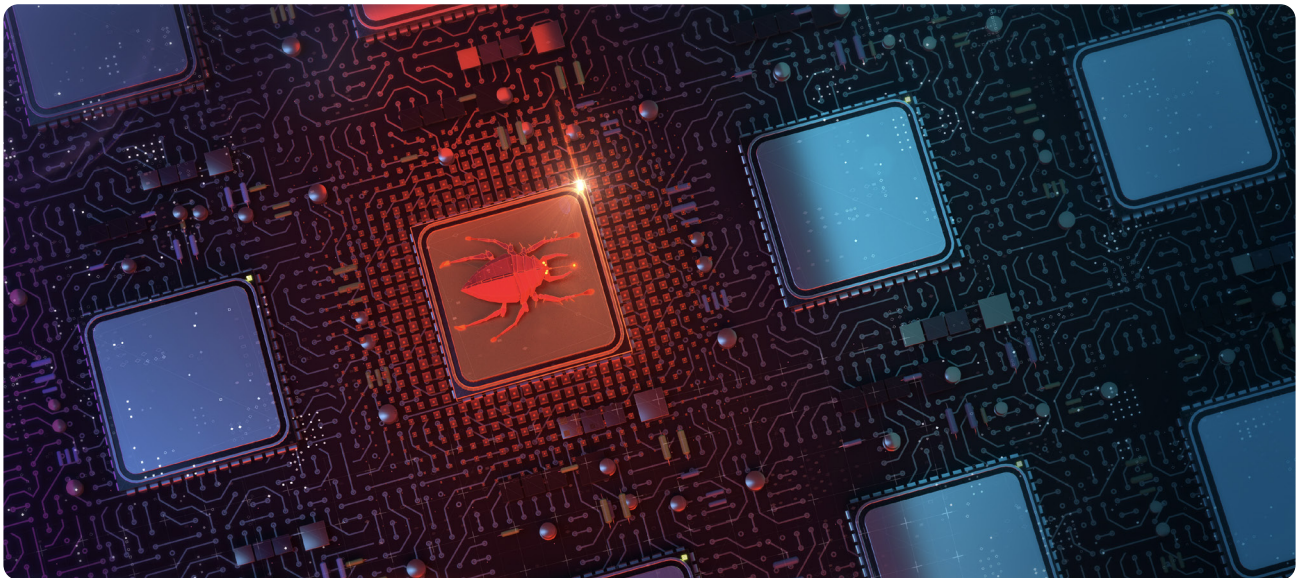
After conducting internal investigations, the school became aware that they were dealing with a bigger problem within the cyber realm that their infrastructure was not sufficient for.

Discoveries

The Snode team was deployed, and through the Guardian platform, Snode's analysts could see both the symptoms and effects of untoward and malicious traffic on the school's network. This included an increase in the total quantity of concurrent connections and the total quantity of bandwidth across the entire network at repeatable specific times from one day to the next. Guardian also detected an increase in the total quantity of Indicators of Compromise across the environment.

As the investigation unfolded, Snode located two network devices connected to the network which compromised the environment. As a result, the school's internal servers were directly accessible from the Internet. The attackers had gained administrator access, giving them visibility into devices used by both teachers and students.

What the Snode team found next was disturbing.



Aggressive, military-grade malware

Within the school's network, among multiple pieces of malware, Snode discovered a three-year-old piece of military-grade malware called GlanceLove on android devices used by students and teachers. In 2017 GlanceLove, a bogus dating app, was used by Hamas to attack the Israeli Defense Forces by collecting the information of soldiers who downloaded the Android app. This sophisticated spyware is used for a multitude of underhanded means, such as eavesdropping on phone calls, perusing files, tracking locations, stealing SMS messages, contacts and photos, and turning on microphones and cameras to capture audio and images.

This begs the question: what was this malware doing in a high school's network? And how frequently is this war being waged against minor's privacy?

A global threat to minors' security

2020 has seen a rise in the exploitation of minors' information through digital means on a global scale; most notably through eavesdropping through home camera systems. The motivation: to commoditise the content of minors that is captured unawares.

In October 2020, almost three terabytes of footage from security cameras in Singaporean, Thai, North Korean and Canadian homes was stolen and disseminated to online sources, including pornographic sites. The videos feature minors, couples and women breastfeeding - in various states of undress or in compromising positions (Sun, 2020). This content was hacked from IP cameras, typically used for security purposes or to remotely monitor children, the elderly, domestic workers and pets.

The unnamed group responsible, which can be found on social messaging platform Discord, has an estimated 1 000 members worldwide. The group claims to have a network of over 50 000 hacked cameras that VIP subscribers can access to watch live, and even record.

Incidents such as this are only just beginning to enter the world's sphere of awareness; where seemingly innocuous technology intended to protect is being used as a vehicle for cyber surveillance to spur on social evils.

Unforeseen cyber risks

In the same month, hugely popular children's game Animal Jam was hacked, resulting in the breach of 46 million player accounts. The game ranks in the top five games in the 9-11 age category on Apple's App store, and has approximately 130 million users and over 300 million unique avatars. The game's creator, WildWorks, stated that a hacker was able to infiltrate the server of a third party vendor that the organisation used for intra-company communication.

The stolen data includes the email addresses of the parents managing the player accounts over the course of ten years, as well as other information that could be used to identify the parents of Animal Jam players. 32 million of those stolen records had the player's username, 23.9 million records had the player's gender, 14.8 million records contained the player's birth year and 5.7 million records had the player's full date of birth. The hacker also took 7 million parent email addresses used to manage their children's accounts. It also said that 12 653 parent accounts had a parent's full name and billing address, and 16 131 parent accounts had a parent's name but no billing address (Whittaker, 2020).

According to WildWorks, the company is aware that data was uploaded to raidforums.com, a well-known online forum for cyber criminals, and the investigation into the extent of the leaked information is ongoing.

Though the compromised information contained few specifics about the children themselves, this is just one of many international incidents where minor's sensitive information is of special interest to attackers. As such, it is more pertinent than ever that both parents, schools and minors remain educated on cyber security best practices, and up the ante on data security across contexts.

Response and remediation

Snode's *modus operandi* was to shut down the incident as quickly as possible - as is necessary in circumstances around the abuse of minor's personally identifiable data, as was the case with Animal Jam.

After gaining visibility into the compromised school environment and identifying the magnitude of the threat within the network, Snode deployed multiple countermeasures to effectively respond to the breach and contain further identified incidents over four days.

The team launched Managed Detection and Response, utilising 8x5x365 monitoring and threat-hunting capabilities to rapidly identify further potential threats or suspicious activity. Devices used by the school were segmented and segregated to isolate the network from the devices owned by both students and teachers and reduce exposure.

The endpoint protection capabilities on all devices was upgraded to a later version, which included additional security features to protect the devices from advanced threats. This included a feature to enable school admins to account for and apply windows patches to 400 assets, from a central management console with automation. This enabled the administrators to close known vulnerabilities within Microsoft products on all devices in the shortest time period possible to reduce the window of exposure.

Administrator privileges were returned to the school admins only, limiting user accounts to only the level of rights required to use the device by teachers and learners. The use of advanced programming languages was also limited to a fixed number of school devices. External-to-internal and internal-to-internal network connections were reassessed, making existing connections stricter, and removing old, expired connections.



Security assurance through a proactive approach

Through their rapid response, Snode was able to contain the incident, minimise the business impact and assist the school in recovering from the security breach. Though the incident was mitigated successfully, the perpetrator's intentions remain unclear. Due to the sensitive nature of the information contained in the school's environment, it can be speculated that this data could be used for malicious means, should it fall into the wrong hands.

This case study is a cautionary tale that all institutions - businesses and schools alike - must have a robust, end-to-end cyber security approach in place to proactively manage and mitigate a risk event of this scale before it even occurs.

About Snode Technologies

Snode Technologies, a cyber defence firm based in Centurion, South Africa, has been a finalist and winner of some of Africa's most prestigious innovation awards, most recently, an overall winner at the SA Innovation Summit 2020 and the MEST Africa Challenge 2019. Snode was also listed, by Slingshot (Singapore), as one of the (2020) Top 100 Deep Tech innovations globally. Snode has over 80 global points of presence, protecting large industrial, agricultural, telecommunication and financial infrastructures.

Author



Nithen Naidoo

CEO & Founder of Snode Technologies

Nithen Naidoo is the CEO and founder of Snode Technologies. As a cyber security evangelist, with over 20 years of experience, Nithen provides cyber defence solutions globally, and most recently was recognised by the prestigious AfricArena tech accelerator as an Emerging Entrepreneur of 2021. Nithen is also a sought-after public speaker.

References

CFC Underwriting (2020). Education infiltration: Hackers access a school's systems through remote desktop protocol and hold data to ransom. Retrieved from:
https://www.cfcunderwriting.com/media/3142/cyber-case-study_education-infiltration_a5_gbp_digital.pdf?hsCtaTracking=0fda7f3b-6388-4e23-8553-c7bfff96ddf6%7C6dd41750-492f-4800-988d-d4a348719fd8

Levin, D.A. (2020). The State of K-12 Cybersecurity: 2019 Year in Review. Arlington, VA: EdTech Strategies, LLC/The K-12 Cybersecurity Resource Center. Retrieved from:
<https://k12cybersecure.com/year-in-review/>

Sun, D. (2020). Singapore home cams hacked and stolen footage sold on pornographic sites. The Newspaper. Retrieved from:
<https://www.tnp.sg/news/singapore/hackers-hawk-explicit-videos-taken-spore-home-cams>

Whittaker, Z. (2020). Animal Jam was hacked and data stolen; here's what parents need to know. Tech Crunch. Retrieved from:
<https://techcrunch.com/2020/11/16/animal-jam-data-breach/>



 www.snode.com

 info@snode.com

 +27 12 880 0989