THE DARK WEB REPORT

New Zealand Education Sector - 2022

CYBER SENTIENCE

Author
Tom Crisp

29 May 2023
Version 1.0

Contents

Foreword

The impact of cybercrime is far-reaching and indiscriminate in its targeting. Coupled with the increase in online activities during the COVID-19 pandemic, it poses a formidable challenge to all sectors in New Zealand. This is exacerbated by a global cybersecurity skills shortage, leading to cyber defense capability gaps. These gaps are key enablers for criminal activities against networks and infrastructure.

In recognition of these challenges, Cyber Sentience are supporting New Zealand and the global community by offering extensive visibility into areas of the internet-enabled criminal underground. Cyber Sentience offers managed and professional services to support targeted threat detection and intervention, with our Research and Development programme's being pivotal in combatting large scale, global cybercrime operations.

The education sector is of particular concern now as it is embracing digital technologies. The sector is becoming a prime target for malicious actors and criminals, where previously it had been taboo due to the innate vulnerability of young children looked after by the sector. Attacks against education providers have led to financial losses for both individuals and the education providers themselves. Students pursuing higher education have their learning outcomes impacted, with declines in enrollment numbers after significant cybersecurity events[1]. If these attacks continue, flow on effects will reduce the availability of skilled labour to the market and affect the safety and security of the millions of New Zealanders and foreigners who engage in the New Zealand education system.

With this in mind, Cyber Sentience have engaged in in-depth research over the last six months and have drawn up this report for education providers and the general public. The aim of this report is to accurately assess the threat landscape, provide tailored support, as well as promote awareness of insidious criminal activity impacting a massive cross-section of New Zealand society.

The research also reveals that there are systemic issues in the security construct applied to the sector. A monumental change in thinking is required for us to adequately shield our vulnerable education sector, and the individuals engaging in it.

Attacks against education providers have led to financial loses for both individuals and the education providers themselves.

1 https://www.forbes.com/sites/emmawhitford/2022/04/19/cyberattacks-pose-existential-risk-to-colleges-and-sealed-one-small-colleges-fate/

Research Background

This research looked to identify active cybersecurity threats facing the New Zealand education sector, using Cyber Sentience's visibility into areas of the internet where cyber criminals operate. This largely comprises of underground marketplaces and ecommerce locations, encrypted chat channels, forums, and information sharing sites.

The education sector services a particularly vulnerable cross-section of New Zealand society with 1 in 4 New Zealanders[2] enrolled with an education provider. Special support needs to be given to education providers, to ensure the safety and security of students pursuing an education. Through years of providing incident response and support services to organisations impacted by malicious cyber activity, Cyber Sentience employees are acutely aware of the financial and emotional impact these events can have.

This research is made public to support informed decision making with respect to cybersecurity for both education providers and consumers.

2 https://www.educationcounts.govt.nz/statistics/

2.1 Research Scope

To complete this research, the following scope was applied:

- Cyber Sentience reviewed intelligence collected between the 1st of January 2022 and the 31st of December 2022 for references to specific keywords.
- Keywords relating to education providers were selected, including the Top-Level Domain (TLD) "school.nz" which is used for many primary and secondary schools, as well as the primary domain names of key education providers.

This research is also subject to the following limitations:

- There is no assertion made for the 'totality' of the findings. Cyber Sentience have only reviewed intelligence made available through our partners and intelligence programmes.
- To protect the integrity of existing collection sources, detailed information about threat actors and sources is withheld from public release.
- While it is possible to take further investigation steps, such as determining the device and individual that is impacted by each malware infection, this could not be done at scale and lies outside the scope of this research.

Key Findings

This research detected a wide range of cybersecurity issues impacting the education sector, including:

- **Over 1,800+ malware infections** identified during 2022 **which impacted 191 New Zealand education providers**.
- **Unauthorised access to 556 web services** belonging to education providers **could be purchased underground** during 2022.
- **Malware observed on devices belonging to teachers, staff, parents, students, and corporate machines** within education provider networks.
- Discovering threat actors **sharing unconfirmed vulnerability information** for systems belonging to **7 out of 8 New Zealand universities**.
- Observing **attempted web exploitation** against 21 New Zealand education providers.
- **Finding access to email systems belonging to 31 New Zealand education providers** available for purchase.
- Finding a threat actor **selling backdoor access to compromised IT infrastructure** of a primary school.
- Finding that a **stolen database** belonging to a secondary school was being **openly shared underground**.
- **Targeting of a new Zealand education provider** by at least one **state nexus threat group**.
- Identifying opportunities to fix **systemic cybersecurity issues** impacting **over one million New Zealanders**.

Observations

4.1 Summary

This research is a window into the threats facing the education sector right now, and moderated conclusions can be drawn as a result. Our conclusions are drawn from our research coupled with Official Information Act requests and analysis of current government policies.

1. Inadequate controls

Cyber Sentience were able to discern what security tooling is currently deployed in the sector through information made available when machines were infected, as well as engaging with impacted education providers. Through the expertise developed by Cyber Sentience employees over years of combatting cybercrime activity and tracking evolutions in threat actor Tactics, Techniques and Procedures (TTP's), Cyber Sentience assess that wider security technology, service, and control adoption is required to defend against the threats identified by this research.

It is also clear that key security controls are not currently implemented by some education providers, as evidenced by the access to email systems that were identified as available for purchase. Compromised websites and the sharing of vulnerability information for education provider systems highlight improvement opportunities for patching processes that keep software up to date. The absence of detection controls for many threats detected by this research further impresses the need to provide increased cybersecurity support to the sector.

Cyber Sentience see a future where every family or individual engaging in the New Zealand education sector is provided a degree of cybersecurity protection from criminal activity.

2. A broken model

Ownership of IT policy in New Zealand is federated out to school boards. However, all 2,544 schools in New Zealand cannot be expected to have staff equipped with the expertise to protect against advanced cybersecurity threats, evidenced by the 82% of respondent schools in a survey who scored as having poor security awareness maturity. Nor can they be expected to know which technologies are suitable for the job, and standard commercial sensibilities do not allow for schools to acquire the necessary technology when procuring on an individual, 'per school' basis. The cost of advanced security technologies decreases dramatically when purchased in bulk. Schools are already priced out of acquiring the technologies required to fulfil their obligations as digital custodians for the safety and security of individuals within their care .

For a school to detect the threats outlined in this research, they must acquire a dark web monitoring service. While costs will vary between technologies and providers, an example licensing cost of $30,000 NZD annually per school will help illustrate the issue. To protect all 2,544 schools in New Zealand with a security control currently adopted by most private organisations, the cost to the New Zealand taxpayer would be 76 million dollars. When implemented as a central service, technology licensing may cost less than 0.1% of that to protect the entire sector.

This logic applies to procurement of security technologies across the board and illustrates that centralised implementation of cybersecurity functions, procurement and controls is the only way forward to adequately protect our vulnerable education providers, students, and families from criminal activity. Schools must also accept that a level of responsibility for the security of education networks should be ceded to a central, government supported provider.

The primary and secondary school sector, and many tertiary providers, are not currently protected by a security service that detects the threats identified by this research after traditional controls have failed.

3. Opportunity

Cyber Sentience see a future where every family or individual engaging in the New Zealand education sector is provided a degree of cybersecurity protection from criminal activity. Through monitoring for references to New Zealand schools, it is possible to detect when a personal computer is hacked, including those belonging to a parent or school child. Instead of allowing a cybercriminal to exploit this information, such as by draining bank accounts or stealing sensitive private information, it is possible to provide targeted support to victims and prevent significant harm from occurring.

Detailed Findings

Cyber Sentience have audited all intelligence items collected during 2022 for references to specific keywords that relate to the sector. Each finding has been independently reviewed, and each threat categorised into one of the following sections. Where an item was determined to not constitute a security threat, the finding was categorised as ‘Not a Threat’ and removed from inclusion in this research.

In the following sections, Cyber Sentience have provided definitions, consequences, observed exposure and some commentary about each threat category.

Table showing the breakdown of identified threats

5.1 Summary

ID	Finding Type	Events	Notes
5.2	**Malware Infection**	1824	Access to 558 services in the education sector can be purchased.
5.3	**Credential Exposure**	200	Credentials (username and passwords) for 2359 Polytechnic, ITO and University users were found being shared underground. Primary/Secondary too large to quantify – single largest event affected 1221 schools with 6770 unique credentials exposed.
5.4	**Evidence of Website Compromise**	40	Evidence suggesting 6 education providers have (partially) compromised websites.
5.5	**Web Application Exploitation**	16	Threat actors shared technical vulnerability information for 24 systems in the education sector, likely to support database theft. Targeting observed by foreign government affiliated hacking group.
5.6	**Sale of Access - Webmail**	39	Access to email systems of 31 education providers can be purchased.
5.7	**Sale of Access - Backdoor**	1	A threat actor was found selling backdoor access to a primary school web server.
5.8	**Information Disclosure - PII**	8	Includes information about children, such as home address, family information and other PII.
5.9	**Database Leak**	1	A database belonging to a secondary school was found being traded underground.
5.10	**Service Abuse**	1	A threat actor was found sharing details about an education providers email system that could be abused to launch malicious email campaigns.
5.11	**Phishing Campaign**	1	A phishing campaign was identified impersonating an education provider to target victims.

5.2 Malware Infections

Definition

A malware infection is where a machine has been infected by malicious code, enabling a threat actor to take control of the device. A specific type of malware infection that is skyrocketing in popularity is a credential stealer, which steals saved passwords from the machine. Threat actors will often infect devices with credential stealers and sell the stolen credentials on an underground marketplace. Other threat actors will then purchase the bundle of credentials when they see an interesting service, such as internet banking or remote access to corporate networks. This finding category captures malware infections where a device has been infected with a credential stealer, and the subsequent listing of credentials on a marketplace which include New Zealand education sector services.

Consequence

A threat actor may purchase the credentials, pretend to be the victim and login to any web service, such as internet banking, email, or corporate systems accessible by the victim. For the individual, their personal internet ecosystem is compromised, and a threat actor has control of the device. For education providers, threat actors may now gain access to sensitive resources such as remote network access or systems containing protected technical and personal information.

This screenshot shows marketplace listings for credentials stolen from infected machines.

Exposure

Cyber Sentience were able to identify 1,824 devices that were infected during 2022 where the victim had interacted with an education provider in New Zealand. As a result of these malware infections, credentials for 558 different web services belonging to education providers were available for purchase.

Included in these malware infections were devices belonging to children, parents, teachers, staff, as well as internal corporate machines. Examples of the types of access available for purchase included remote access to networks, email systems, file storage, source code repositories and behavioural issue portals.

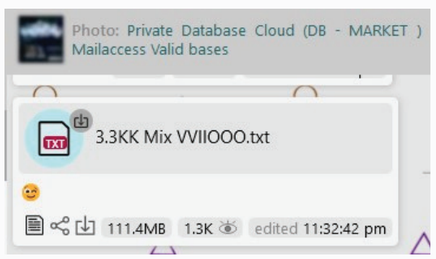
5.3 Credential Exposure

Definition

Cyber Sentience have identified an event where a threat actor has shared compromised credentials belonging to email addresses in the education sector. These are typically in large lists, containing large amounts of usernames and passwords in the format [username]@[educationdomain]:[password]. Often this is the result of 3rd party breaches where education email addresses have been used to sign up to external services, or as a result of phishing campaigns.

Consequence

Threat actors attempt to use these large numbers of compromised credentials to gain access to systems belonging to education providers. Depending on the objectives of the threat actors, this may lead to network compromise and ransomware attacks, data theft, or financial fraud.



This screenshot above is an example of a threat actor sharing a txt file containing education email addresses and passwords, in a private encrypted messaging channel.

Exposure

200 of these events were identified, exposing 2359 tertiary education staff and student credentials. The single largest credential exposure event impacting primary and secondary schools affected 1221 education providers and exposed 6770 accounts.

Not every username and password exposed in these events will provide access to education services. However, the risk is elevated through the highly parallelised and automated nature of these attacks, as well as the compounding issue of password reuse. The number of exposed accounts highlights a clear need for processes to be in place for detecting and mitigating the abuse of these credentials.

5.4 Evidence of Website Compromise

Definition

Cyber Sentience have observed a threat actor sharing information that indicates a website in the education sector has been attacked. This type of activity is usually the result of indiscriminate exploitation attempts of a vulnerable website component, with the threat actor then sharing lists of successfully exploited systems.

Consequence

A web application belonging to an education provider in New Zealand has been abused and at least partially compromised. Typical consequences include threat actors hosting illegal content on compromised systems, or luring victims into trusting malicious files that may infect end user devices.

Exposure

Cyber Sentience reviewed 40 events pertaining to website compromise that suggest 6 education providers New Zealand have partially compromised websites.

Examples of malicious content hosted on compromised or abused education provider websites include:

- Procurement guides for illegal drugs
- Gambling website advertisements
- Pirated media content; or
- Links to malware and phishing pages.

Typical consequences include threat actors hosting illegal content on compromised systems.

5.5 Web Application Exploitation

Definition

Cyber Sentience have observed a threat actor sharing information that indicates a vulnerability exists in an education provider's web application, such as the main website or learning and research portals. Threat actors who focus on computer exploitation will then use the knowledge of these vulnerabilities to exploit the web application for their own objectives.

Consequence

Threat actors will seek to exploit these vulnerabilities to steal databases containing personal information, as well as compromise the underlying IT infrastructure through more technical attacks. This personal information is often shared or sold to support other malicious activities, such as financial fraud. The backdoor access to IT infrastructure belonging to education providers may then be sold to other threat groups. These groups will then use the access to penetrate further into networks and often commit extortion activities like ransomware attacks.

Exposure

Cyber Sentience identified 16 events where threat actors shared unconfirmed vulnerability details for 24 different systems belonging to education providers in New Zealand. The majority of these fell into the web exploitation category 'SQL injection', which is used to target and compromise databases.

Threat actors shared vulnerability information that applied to the main websites of primary, secondary, and tertiary education providers. Also included were intranet sites, research portals and document archives.

Personal information is often shared or sold to support other malicious activities.

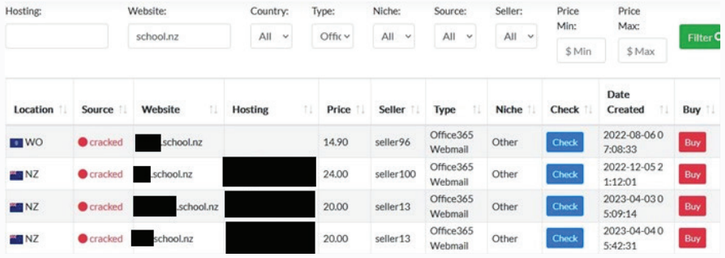
5.6 Sale of Access - Webmail

Definition

Cyber Sentience observed a threat actor claiming to have access to confirmed, legitimate email credentials for an education provider in New Zealand. The threat actor was advertising these credentials for sale on an underground marketplace.

Consequence

A threat actor may buy these credentials and use them to gain access to a valid email account of an education provider. Any information held in this mailbox can be accessed by an unauthorised party. Compromised email accounts are commonly used to commit further attacks, such as attempting financial fraud or phishing campaigns using a trusted account. Often password reuse can be an issue, with these credentials able to be used across multiple services.



Exposure

Cyber Sentience identified 39 instances of threat actors selling confirmed email system access, impacting a total of 31 education providers in New Zealand. As the threat actor needs to provide proof that they can access the mailbox, there is a functionality offered by the marketplace that allows potential purchasers to 'test' the access to confirm its legitimacy. This indicates 31 email systems do not have appropriate security controls in place, such as two factor authentication.

The majority of instances where threat actors were found selling access to email systems applied to primary and secondary schools, however, tertiary education providers were also impacted.

5.7 Sale of Access - Backdoor

Definition

Cyber Sentience have observed a threat actor selling access to IT infrastructure of an education provider in New Zealand. The educator provider has been named directly, and the access type is either a backdoor on a web server or internal machine.

Consequence

IT infrastructure of an education provider has been compromised, and a backdoor is on a machine. Threat actors can purchase this access to commit further malicious activities, such as penetrating the network deeper and deploying ransomware. Any information held by the machine has likely already been stolen.

Exposure

Cyber Sentience identified one threat actor selling backdoor access to a web server belonging to a New Zealand secondary school. The listed access type was ‘webshell’, which suggests that the machine is a web server that likely had a backdoor dropped on it after successful exploitation of a vulnerable web component or application.

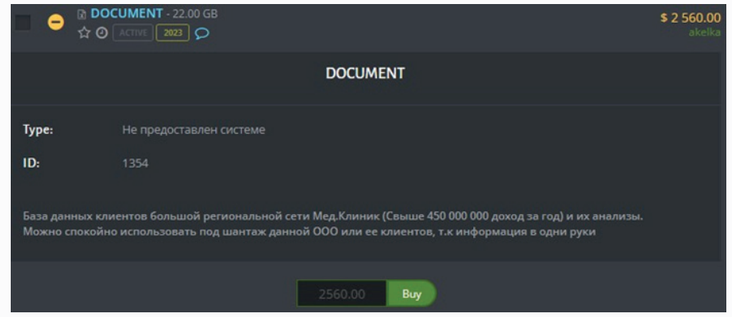
5.8 Information Disclosure – Personally Identifiable Information (PII)

Definition

Cyber Sentience have observed a threat actor sharing personal details of staff or students of the education sector. Any sharing of information which includes date of birth, home address, personal documents like legal identification or family information is included in this category.

Consequence

According to the privacy commissioner, stolen information such as passports and birthdates are often used by malicious actors to defraud people or steal their identities . This type of information can also be used to harass or blackmail victims.

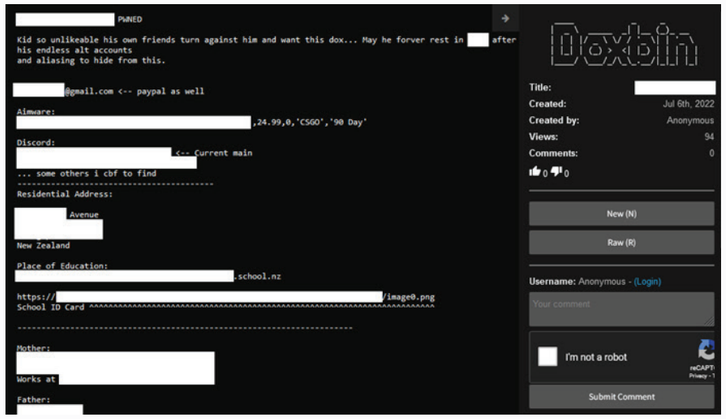


Translation:
Database of clients of a large regional network of Med.Clinics (Over 450,000,000 income per year) and their [..]. You can safely use this LLC or its clients for blackmail, because information is in one hand [sic]”

5.8 Information Disclosure – (continued)
Personally Identifiable Information (PII)

Exposure

Cyber Sentience discovered 8 events where threat actors disclosed personal information belonging to students or staff members of the education sector. These events ranged in severity. Smaller exposure events included threat actors sharing personal information held by LinkedIn which was stolen during a security breach. More serious exposure that we observed included a threat actor targeting a young child who had irritated them during an online game. The threat actor had 'doxed' (maliciously released personal information about) the student, revealing his school, personal address, identification documents, as well as pictures of his family and pets.



With respect to harm mitigation, the Harmful Digital Communications (HDC) Act 2015 addresses some of the ways people use technology to hurt others, and aims to prevent and reduce the impact of online harassment. Capabilities now exist where many of these threats can be proactively identified and discouraged, instead of waiting until it is self-reported. The HDC Act can be utilised to provide legal consequences for illegal activity of this type.

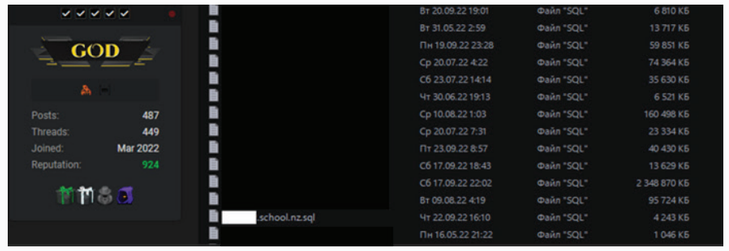
5.9 Database Leak

Definition

Cyber Sentience have observed a threat actor sharing a database likely stolen from an education provider during a cybersecurity breach. This database is either being listed for sale, or freely distributed within an underground community.

Consequence

The confidentiality of any information contained by the database has been compromised and is now accessible to threat actors. This information is typically used by other threat actors to perpetuate other crimes, such as identity and financial fraud. Any credentials held in the database are likely compromised and can be used for further criminal activities.



The screenshot above shows a threat actor sharing dozens of stolen databases with their community, including one belonging to a New Zealand secondary school

Exposure

Cyber Sentience discovered a database belonging to a New Zealand secondary school being shared freely underground on a forum dedicated to sharing information and databases stolen during cyber security breaches. It was found amongst 28 databases stolen from various entities across other sectors.

Cyber Sentience were also able to observe the proliferation and distribution of these stolen databases. In the months following this initial event, the database was observed being traded on various other underground communities and in encrypted chat groups.

5.10 **Service Abuse**

Definition

Cyber Sentience have observed a threat actor sharing technical information about a system belonging to an education provider that may be abused to support malicious cyber activity.

Consequence

Threat actors may be abusing these services to further their own objectives. Often abusing legitimate web services can leverage the trust of that organisation to target victims more successfully. Some examples of this would be hosting phishing pages on education provider websites, or abuse email relays belonging to an education provider to bypass email filtering controls.

Exposure

Cyber Sentience observed one threat actor sharing information about an open email relay (SMTP) belonging to a tertiary education provider in an underground community specialising in phishing. The mail server is likely being used to send malicious emails to a range of victims. As the email is coming from a legitimate, trusted source, many email gateway filters will allow the phishing email to be successfully delivered to the target, increasing the effectiveness of the campaign.

Their mail server is likely being used to send malicious emails to a range of victims.

5.11 **Phishing Campaign**

Definition

Cyber Sentience have found evidence of a phishing campaign impersonating an education provider to target victims.

Consequence

Credential phishing campaigns are more likely to be successful due to victims trusting the content and believing it to be from a local education provider. Victims may also be more likely to download and execute malicious files.

Exposure

Cyber Sentience identified a single phishing campaign impersonating a New Zealand tertiary education provider.

Steps can be taken to protect potential victims, such as requesting takedowns of infrastructure used in the malicious campaigns.

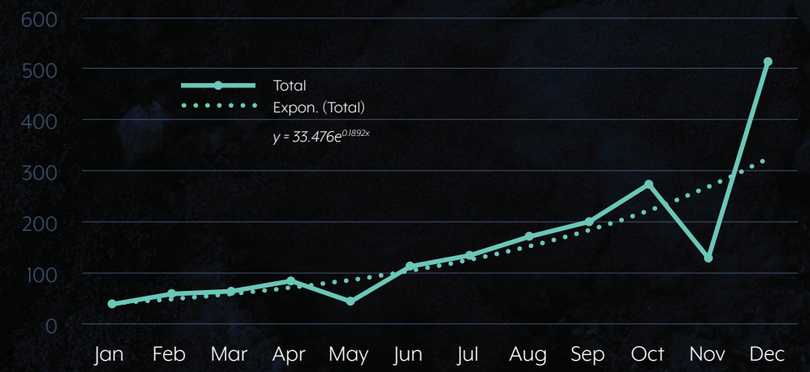
Trends & Insights

Cyber Sentience captured many data points of interest when documenting the findings contained in this research report, including the relevant intelligence source, threat actor, and datetime information. This section aims to provide deeper insights into possible trends and themes that are present in the underlying data.

In summary:

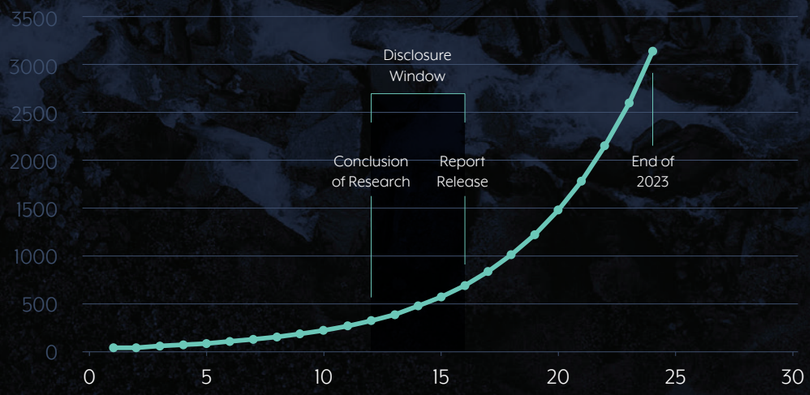
- 1215% increase in monthly malware infections when comparing the month of January 2022 to the month of December 2022.
- If current trends continue, October 2023 will have the same number of malware infections as the entirety of 2022.
- Equal likelihood of a malware infection for any given day of the week, including weekends.
- Possible to detect and respond to 95% percent of the findings in this research report within 24 hours.

6.1 Exponential Growth of Malware infections



Total observed Infected Devices per Month

The number of infected devices per month appears to be increasing at an exponential rate over the course of 2022. Compared to the first month of the year, December 2022 saw a 1215% increase in observable malware infections.



Predicted Infected Devices per Month

2023 is expected to see an unprecedented boom in the amount of unauthorised access that can be purchased to IT and web services belonging to the education sector. The number of victims of cybercrime will continue to grow at a rapid rate. To reverse this trend, more robust security technologies must be made available to the sector. The implementation of centralized security services and functions will also be the most effective way to proactively mitigate emergent cybersecurity threats.

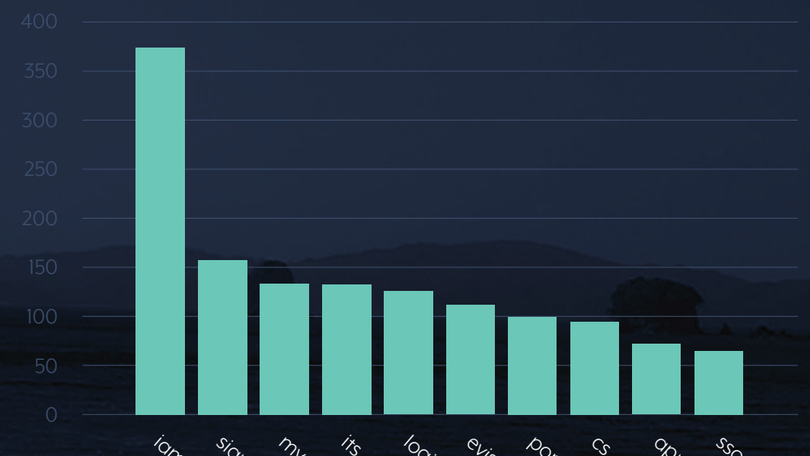
6.2 **The Most Dangerous Day of the Week**

Cyber Sentience did not note any statistically significant difference in likelihood of a malware infection event occurring on any given day of the week. This highlights that cybersecurity threats are not limited to 9-5, Monday through Friday. Cyber-attacks can occur at any time, including weekends, and controls need to be in place to deal with this reality.

6.3 **Response Times**

Cyber threat intelligence needs to be both timely and actionable for it to be valuable. To determine exactly how effective our own intelligence service is, we compared when the incident was first available to be detected online, and when we would have been alerted to it. For 95% of the threats captured in this research, Cyber Sentience would have responded to the threat within 24 hours of it being possible to detect.

6.4 **Top 10 Subdomains for Sale**



Frequency of observed subdomain sales

A subdomain is a piece of additional information added to the beginning of a website's domain name, which helps to organize and navigate to different web services provided by the same organisation. Threat actors will often purchase credential sets that contain sensitive subdomains such as 'remote' or 'vpn' that will allow them to gain access to protected networks. While these sensitive subdomains don't feature in the Top 10, the graph itself is hiding an insidious truth.

According to this research, the most widely available services for purchase underground will in fact grant unauthorised access to multiple other systems. It is common practice for organisations to allow a user to login once, and then be granted access to multiple services through what is commonly known as Single Sign-On. The subdomains 'iam' and 'sso' are common identifiers for these access management systems, with many of the other subdomains in the Top 10 also likely supporting this function. In effect, the most common keys for sale are keys that open multiple doors.

While it is impossible for Cyber Sentience to determine what access is granted to other services through these credentials without engaging with the impacted education provider, it reinforces the need to have systems in place to detect this type of exposure.

Final Thoughts

This research has helped to establish and document a range of cybersecurity threats facing the education sector. There is clear evidence to suggest that threat activity is increasing, and the sector is not equipped to deal with today's threats. Without a sharp increase in central cybersecurity leadership and service implementation, over a million New Zealander's who are actively engaged in education will continue to have an elevated risk of being impacted by criminal activity. There is an opportunity to turn our vulnerable education sector into a world leading, socially responsible centre for cybersecurity excellence which will extend protection beyond just those enrolled in academic studies.

Cyber Sentience acknowledge that this research may raise concerns for private organisations, education providers and concerned individuals. We are available and committed to helping anybody who is seeking to secure their environment against malicious cyber activity.

CYBER SENTIENCE

enquiries@cybersentience.co.nz
+64 22 101 1029
cybersentience.co.nz