FUJITSU

January 2026

Hack to the future: Lessons from New Zealand's 2025 threat landscape

WhatsApp metadata flaw exposed

Ledger data breach

ManageMyHealth breach

Crypto C2

Threat Intelligence Report

A monthly digest of cyber threat activities, insights, and strategies for enhanced cyber resilience

Fujitsu Cyber

Contents

This threat intelligence report has been developed using the insights from the various teams within Fujitsu Cyber. We report on the overarching trends we have recognised in the past few months, with a focus on current events and actionable steps.

At Fujitsu Cyber, we actively take these insights from what we observed and apply them to all the work we do, whether it be with our consulting engagements, our ongoing threat hunting programme, or our managed service client environments. Our constant learning across the business helps us to stay adaptable and on top of our security game, so that we can keep our client systems as safe as possible.

Hack to the future:

Lessons from New Zealand's 2025 threat landscape

This article was written by:
Tanya Wessels
Principal Security Consultant

If Doc and Marty had set the DeLorean for 2025, they wouldn't find hoverboards and self-drying jackets; they would find state-sponsored hackers pre-positioned in critical networks and AI-powered phishing campaigns. Instead of flux capacitors, today's attackers utilise stolen credentials and unpatched vulnerabilities to travel through your systems a lot faster than 88 mph.

NCSC's 2025 Cyber Threat report reveals a digital battlefield where tomorrow's cyber war has arrived; and the enemy is already inside.

In this article, we'll unpack the key lessons learned for the NCSC's latest findings, explore what these trends mean for organisations across Aotearoa, and outline practical steps to future proof your defences.

State-sponsored campaigns and strategic pre-positioning*

NCSC's report identifies that state-sponsored actors actively target New Zealand for espionage and potential disruption, often pre-positioning in network across Government and nationally significant organisations.

Impacts:

These campaigns blend stealthy initial access (valid accounts, living-off-the-land techniques) with long dwell times to exfiltrate data or position for disruption of services. The strategic goal can be intellectual property theft, policy influence, or critical infrastructure resilience testing.

Recommended actions:

Identity hardening: enforce phishing-resistance MFA (e.g., passkeys), conditional access, and Privileged Access Management (PAM).

Threat-led testing: red-team against valid-account abuse and data exfiltration paths, including stealth scenarios and long-dwell adversary simulations.

Sector collaboration: participate in NCSC/ industry intelligence sharing and rehearse joint exercises across essential services.

Mass credential theft – Lumma Stealer at scale

NCSC emailed roughly 26,000 New Zealanders about Lumma Stealer infections. Lumma Stealer is credential-harvesting malware that silently collects usernames, passwords, and session tokens, often via phishing or compromised sites.

Impacts:

Credential theft fuels account takeovers into banks, Government portals, and enterprise applications. Browser vaults and password reuse amplify impact.

Recommended actions:

Credential hygiene: mandate password managers, unique credentials, and rotation for sensitive roles. Disable browser-stored passwords.

Compromised credential response: monitor breach corpuses, enforce step-up authentication when suspicious reuse is detected.

Endpoint hardening: block known IOCs, disable risky extensions, and auto-isolate devices with theft indicators.

* Pre-positioning in the context of cybersecurity refers to the practice where threat actors (often state-sponsored), gain and maintain covert access to network or systems well before launching an actual attack or disruption.

Supply chain blind spots and cascading impact

NCSC notes that supply chain exploitation and hidden dependencies (such as Managed Service Providers (MSP) s, Software as a Service (SaaS), firmware, and open-source libraries) are increasingly utilised to gain access and amplify impact where a single compromised vendor or component ripples through interconnected systems.

Impacts:

An initial breach in a MSP, SaaS provider, or firmware supplier can grant attackers privilege access to multiple organisations, enabling lateral movement across trusted environments. This often results in widespread data exfiltration, operational outages, and increased regulatory obligations for every affected entity.

Recommended actions:

Organisations must reassess their identity and access management strategies.

Legacy systems relying solely on passwords may need upgrades to support biometrics, hardware tokens, or passkeys. This aligns NZISM with NIST SP 800-63 standards, encouraging stronger user verification methods.

Insider risk and hacktivism

The NCSC highlights insider threats (malicious or negligent) and hacktivist activity amid geopolitical tensions. Analysts advocate an "assume breach" posture and resilience-first mindset that plans for operations even under compromise.

Impacts:

Insider risk and hacktivism can create significant disruption by exploiting trust and amplifying social or political motives. Bypassing perimeter defences and exfiltrating malicious or negligent insiders often have privilege access, making it easier for attackers to bypass perimeter defences and exfiltrate sensitive data or sabotage systems.

Recommended actions:

Insider programs: UEBA, Data Loss Prevention (DLP), privileged monitoring, segmented access for contractors, and formal pathways for reporting concerns.

Table-top exercise for data leak/extortion: implement pre-planned communications (e.g., rehearse public statements), evidence preservation, and legal engagement.

Culture and accountability: provide role-specific training, periodic employee and contractor security screening, and consequence-aware governance.

Known weaknesses and unpatched vulnerabilities

According to the NCSC Cyber Threat Report 2025, many successful cyber intrusions still exploit basic security lapses such as unpatched systems, default credentials, and misconfigurations. These weaknesses provide advisories with easy and scalable entry points, enabling them to compromise networks quickly and to maintain persistence.

Impacts:

Despite the focus on advanced threat actors, most breaches occur because of poor cyber hygiene. Known vulnerabilities and outdated systems remain a primary attack vector, allowing attackers to bypass sophisticated defences.

Recommended actions:

Patch management: implement automated patching and prioritise critical vulnerabilities.

Vulnerability scanning: conduct regular scans and remediate findings promptly.

Credential hygiene: remove default credentials, enforce strong passwords, and enable MFA.

Configuration management: harden system configurations and disable unused services.

Layered defense: combine basic hygiene with advanced monitoring and threat detection.

Conclusion

The NCSC's 2025 Cyber Threat Report shows that the future is not about flying cars. It's about future-proofing identity, designing resilience into the operational core, patching weaknesses, and securing supply chains before cascading failures hit like a temporal paradox.

Fasten your seatbelt and strap up your velcro! In the world of cyber security, the journey still needs a roadmap... and patch management is your GPS.

References

NCSC Cyber Threat Report 2025, December 2025: Key judgements for 2025
NCSC Quarter 1 Cyber Security Insights 2025: Quarter One Cyber Security Insights 2025
NZSIS Security Threat Environment report 2025: New Zealand's Security Threat Environment | New Zealand Security Intelligence Service
Back to the Future Part II - Wikipedia

Article two:

WhatsApp metadata flaw exposed:

Meta responds with mitigation measures

This article was written by:
Nicky Pretorius
Senior Security Consultant

Meta started deploying fixes to address a metadata exposure vulnerability in WhatsApp that enabled adversaries to fingerprint users' devices with minimal effort.

This issue emerged when researchers highlighted how attackers could infer key device characteristics, such as operating system, device type, app usage, and device "age" based solely on encrypted metadata shared during message delivery.

Threat overview

Prior to deploying sophisticated spyware campaigns, that actors conduct reconnaissance to tailor exploits for specific operating systems. Researchers have shown that by analysing predictable patterns in WhatsApp's encryption key identifiers, attackers can accurately determine whether a target is using Android or iOS, Olang with other device details.

WhatsApp assigns sequential, identifiable key IDs to encryption keys. On iOS, these identifiers increase gradually over time, while on Android they follow a random pattern and use the full 24-bit range. Attackers exploit these patterns to identify the platform using only a target's phone number, with no interaction.

This technique leaves no trace on victims' devices. Using only a phone number, the attackers can secretly map device metadata and extract operating system and client usage details.

Device	Type	Device Type (Passive)	Device Age
Device 0	Primary	Apple iOS high confidence	N/A
Device 32	Secondary	Apple Mac high confidence	N/A
Device 33	Secondary	Web high confidence	4m
Device 34	Secondary	Web high confidence	1m
Device 35	Secondary	Android Desktop medium confidence	N/A

Figure 1: Source - https://www.securityweek.com/researcher-spotlights-WhatsApp-metadata-leak-as-meta-begins-rolling-out-fixes/

3B+ WhatsApp users at risk: covert OS-fingerprinting boosts APT and surveillance-for-hire capabilities.

Motivation and risk from threat actors

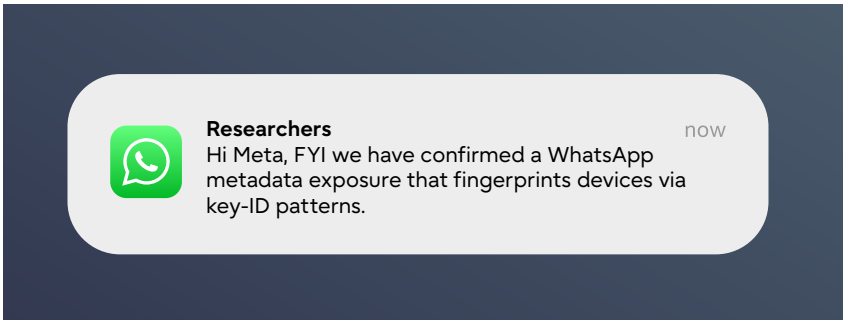
High-end spyware campaigns, such as those by Paragon and NSO Group, rely on zero-click vulnerabilities to deliver malicious payloads without user interaction. To execute these attacks successfully, adversaries must identify the target's operating system. This metadata leak streamlines the process, significantly reducing the effort required for reconnaissance.

With more than 3 billion active WhatsApp users, an undercover method for inferring operating systems from minimal data provides a significant advantage to advanced persistent threat (APT) actors to surveillance for hire groups.

Research, disclosure and attribution

Tal Be'ery, the Chief Technology Officer (CTO) of Zengo and a respected security researcher, led the investigation into WhatsApp's metadata exposure. He developed a private tool that exploited key ID patterns to fingerprint devices. Be'ery and others responsibly disclosed their findings to Meta.

Researchers documented this technique over the past two years. After they reported these issues, Meta made no immediate changes. Meta recently only implemented partial mitigation measures, such as randomising key IDs on Android.



WhatsApp says OS fingerprinting is widespread and low risk unless combined with a zero-day; Meta rates the flaw as low severity.

Meta's response and fix rollout

Meta implemented random values for One-Time Public Key (PK) key IDs on Android, eliminating the predictability that attackers previous exploited.

WhatsApp stated that OS fingerprinting is common across platforms and poses lower severity unless paired with a zero-day exploit. WhatsApp furthermore stated that operating system differences are necessary to optimise performance and enhance usability.

Meta classified the vulnerability as low severity, noting that OS inference through metadata typically does not meet the criteria for a CVE under industry standards.

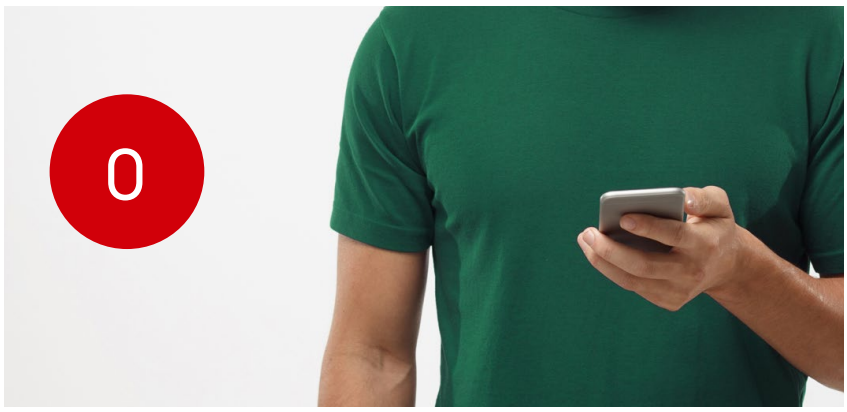
Evaluation and critical analysis

Reducing reconnaissance capabilities limits attackers' ability to match payloads to the correct operating system, disrupting high-risk campaigns targeting WhatsApp users.

Implementing platform-wide key ID randomisation would eliminate OS fingerprinting entirely, significantly strengthening user privacy.

Partial mitigation leaves iOS exposed, undermining a unified defence strategy.

Meta rolled out the fix silently, without public acknowledgment or communication, leaving users uninformed and creating trust gaps.



Conclusion

WhatsApp's metadata fingerprinting vulnerability exposed an undercover yet powerful reconnaissance vector that could utilise zero-click spyware campaigns. Meta has taken initial steps to mitigate the issue by randomising Android key IDs, but its approach remains incomplete and lacks transparency.

Security experts recommends a comprehensive rollout of key ID randomisation across all platforms, improved disclosure practices, and stronger collaboration with researchers. Implementing these measures would close a subtle yet impactful metadata leak and mark a critical advancement in safeguarding user privacy on a global scale.

Reference

[1] E. Kovacs, "Researcher Spotlights WhatsApp Metadata Leak as Meta Begins Rolling Out Fixes," Security Week, 05 January 2026. [Online]. Available: https://www.securityweek.com/researcher-spotlights-whatsapp-metadata-leak-as-meta-begins-rolling-out-fixes/.

Ledger data breach

What organisations and individuals need to know

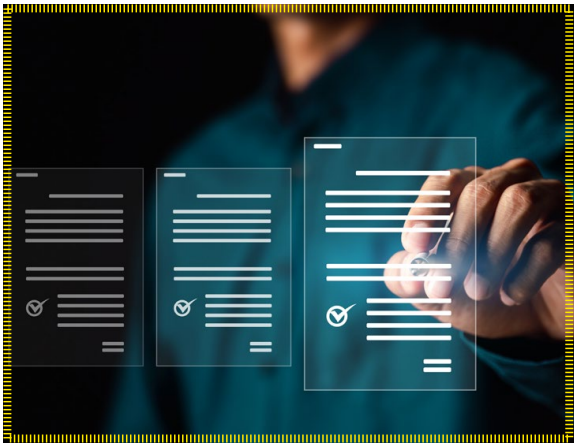
This article was written by:
Ben Sparks
Principal Security Consultant

Ledger, a cryptocurrency solutions provider that specialises in providing hardware wallets, has had customer identity data exposed in a breach of their payment partner on or around 5 January 2026.

The international payments processor Global-e alerted (1) Ledger customers that their names, addresses and order details had been accessed by an unidentified party in an incident that was now contained. Ledger followed up with communications (2) assuring customers that Ledger itself had not been breached, and core customer data such as payment details, account credentials or recovery phrases or keys had been compromised.

Within hours, customers were receiving targeted phishing emails (3). The emails claimed that Ledger and competitor product Trezor were merging, and that customers should secure their wallets via a link. In fact, the link takes them to a fake Ledger page that asks for their recovery phrase.

This incident is not the first time a crypto business, or even Ledger, has been subject to phishing campaigns, but it still has useful lessons for both organisations and individuals. As this situation develops, here are some points to note:

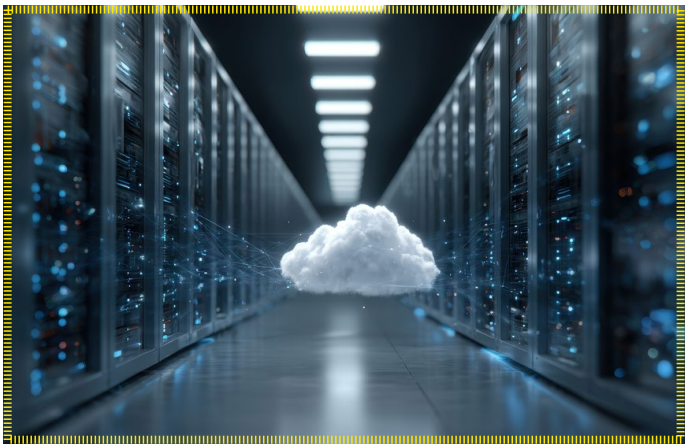


Ledger has stated that Global-e was subject to a security and privacy questionnaire before onboarding (2).

While the breach vector has yet to be revealed, proactive organisations should be looking at their vendor risk assessment processes. Effective third-party assessment questionnaires should include requests for findings from penetration tests and audits including accounts of remedial actions as part of their due diligence.

The unusual activity was spotted by Global-e in one of their cloud environments.

The origin of the breach may have been data store misconfiguration. See the article ManageMyHealth Analysis (3) in this month's newsletter for specifics of how to securely configure cloud storage environments.



The phishing emails have included order details to make them harder to spot as fakes.

While Ledger has emphasised that their customers' creds, financial details and recovery keys/phrases were not exposed, nonetheless the attackers still obtained enough personal information to create credible phishing mails. Examples of emails (5) have been posted on X.com that refer to specific products and purchase dates make the message more believable.

The first line of defence against Phishing remains the recipient of the phishing mail. As always, be alert if you received unexpected communications online and look out for:

Anomalies	Look out for URLs for webpages that don't match the supplier, attachments that have no reason to be there, and links that when hovered over, show an unexpected link destination.
Threats/ Promises	Phishing communications will try to create a sense of urgency to make you act quickly without thinking, either by promising rewards for a response, or threatening dire outcomes such as account suspension or deletion of your data.
Errors	Even in the age of AI, spelling errors and poor copies of legitimate logos are still often found in phishing emails. Whether this is a social engineering tactic to select inattentive users, or a result of the scammer rushing to exploit user data as quickly as possible, these errors are still an easy way to spot phishing attacks.

And finally, no legitimate organisation will ever ask you to disclose your passwords, keys or passphrases to them.

References

[1] "Privacy Center" Accessed Jan 6 2026 [Online.] Available: https://global-e-incident.privacy.saymine.io/global-e-incident?utm_medium=email&_hsmi=2&utm_content=2&utm_source=hs_email

[2] "Global-e Incident to Order Data - January 2026" Accessed Jan. 6 2026 [Online.] Available: https://support.ledger.com/article/Global-e-Incident-to-Order-Data---January-2026

[3] N. Pretorius "ManageMyHealth Fujitsu Cyber Security Analysis" Monthly Cyber Report January 2026

[4] "Global-e Incident to Order Data - January 2026" Accessed Jan. 6 2026 [Online.] Available: https://support.ledger.com/article/Global-e-Incident-to-Order-Data---January-2026. "(Providers must) complete a security and privacy questionnaire before onboarding" and "Prior to engaging Global-e as a provider, Ledger conducted a standard third-party due diligence review based on documentation, in line with our third-party provider risk management process at the time.

[5] J. Godstime. "Ledger Users Hit by Phishing Scam After Global-e Data Breach Exposes Order Information" Accessed Jan. 7 2026 [Online.] Available: https://www.cointribune.com/en/ledger-users-hit-by-phishing-scam-after-global-e-data-breach-exposes-order-information. "The phishing emails appear to rely on leaked order data, making them more difficult to identify. References to specific products or purchase dates increase the credibility of the messages."

[6] B. Toulas. "Ledger customers impacted by third-party Global-e data breach." Accessed Jan. 5 2026 [Online.] Available: https://www.bleepingcomputer.com/news/security/ledger-customers-impacted-by-third-party-global-e-data-breach/

Article four:

ManageMyHealth breach:

Key takeaways for patient portals and New Zealand's cyber resilience (Dec 2025–Jan 2026)

This article was written by:
Nicky Pretorius
Senior Security Consultant

Although the ManageMyHealth breach occurred in New Zealand, the incident reflects threat patterns and systemic weaknesses seen across the Australian healthcare sector, particularly for GP practice portals, cloud-hosted health SaaS platforms, and third-party service providers.

In late December 2025, ManageMyHealth (MMH), New Zealand's largest patient health portal, used by many GP practices and holding records of approximately 1.8 million registered users, identified an unauthorised access to its platform.

An update from RNZ indicated that on 1–2 January 2026 that the "incident was contained, with approximately 6–7% of patients potentially affected, and the unauthorised access limited to a specific group of documents rather than the core patient database or credentials". Health NZ (Te Whatu Ora) reported no impact to its systems, and the Minister of Health commissioned an independent review of the incident response.

As per the Otago Daily Times, a cybercrime group, namely Kazu demanded a **$60,000 ransom** with a mid-January deadline.

This incident occurred against the backdrop of an escalating wave of cyber activity in New Zealand, such as the Neighbourly social network outage linked to suspected unauthorised access, and persistent national trends of significant financial losses driven by scams, phishing campaigns, and business email compromise (BEC), as reported by the National Cyber Security Centre (NCSC).

This article analyses the MMH breach timeline and scope, probable intrusion patterns for health portals, stakeholder coordination, and the context of NZ's threat landscape - then offers sector specific recommendations aligned to healthcare, SaaS, and managed service environments in Aotearoa.

30 Dec 2025

MMH became aware of a cyber security incident following notification from a partner, engaged independent forensic specialists, and notified the Office of the Privacy Commissioner, Health NZ, NZ Police, and other agencies.

1 Jan 2026

Initial Public statement; MMH confirmed unauthorised access had been identified and contained. Independent investigation continued to validate scope.

2 Jan 2026

As per Radio NZ's article MMH clarified 7% of approximately 1.8 million patients may be affected, with access to a specific group of documents (no evidence of core database or credential compromise, nor data modification/ destruction). Health NZ stated its systems were unaffected and activated an incident management team with NCSC and Police support.

5 Jan 2026

The Minister of Health announced a formal review to assess root causes, protections, response capability, and improvements; terms of reference to be developed with the Government Chief Digital Officer (GCDO) and NCSC.

7 Jan 2026

Kazu begin to delete references to the attack across their site and messages.

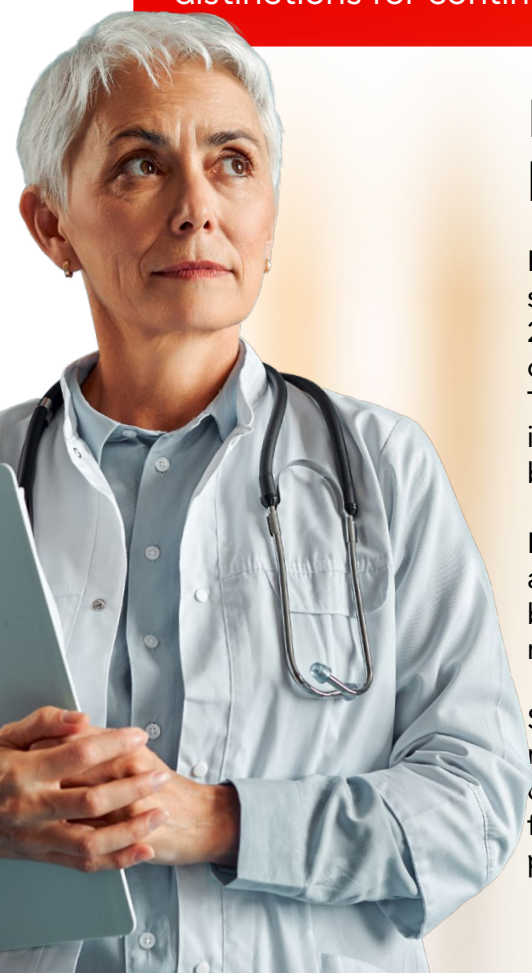
Who is Kazu

Kazu is the criminal group who have claimed responsibility for the MMH data breach. This group is relatively unknown as they are recently formed and are still establishing themselves. Although they first emerged with posts on the forum “CrackingX” in April 2025, they appear to have only recently started scaling up their operations. October marked an increase in activity and they began posting updates on telegram, claiming to have access to a Kuwait based companies network. They have since claimed to have breached other companies such as “Saudi Icon” and “CT Dent Ltd”. In terms of motives, the group does not appear to be politically motivated but rather just performing attacks for financial gain.

Scope and nature of compromise

As per Scoop’s article dated 2 January 2026, preliminary investigation reveals no evidence at this stage that the core patient database was accessed, nor any evidence of data modification or destruction within MMH’s system, nor any access to user credentials. While the police have not named anyone, the pattern of this activity is consistent with exposure of document repositories, object stores, workflow attachment stores, or misconfigured access paths (e.g., routes that bypass main database controls to access storage buckets, document services, or API).

Health NZ reinforced separation of systems between MMH and public health infrastructure and stated no clinical impact on patient care, important distinctions for continuity and public trust.



Broader NZ threat landscape and health sector exposure

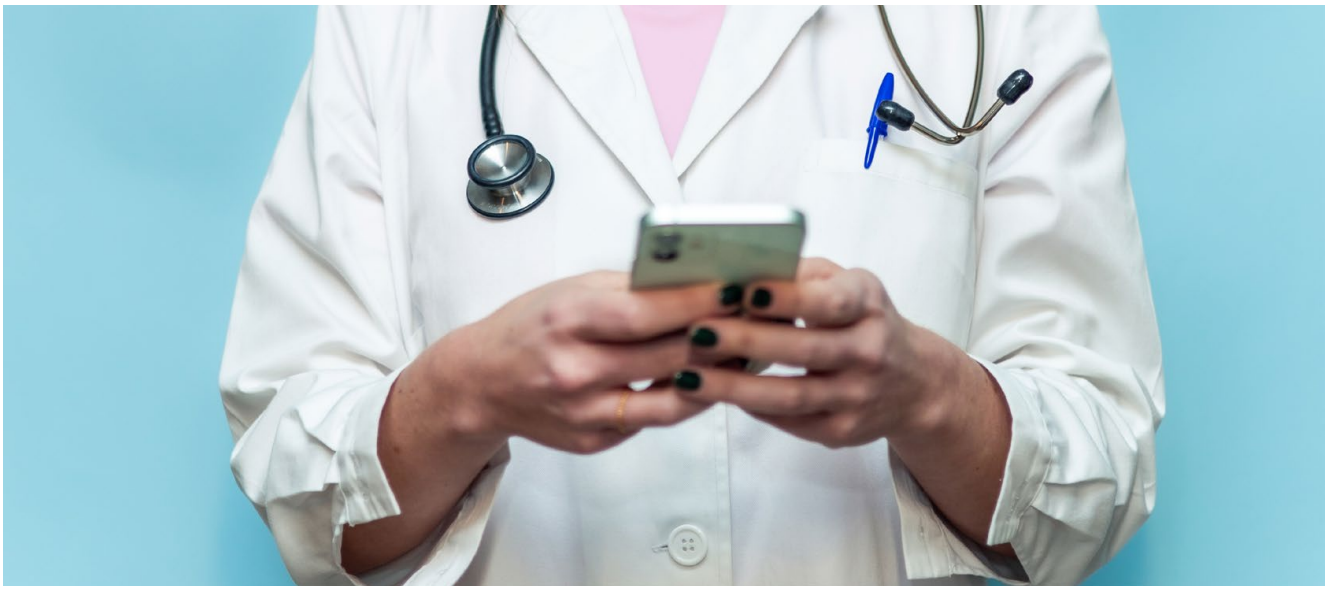
New Zealand’s national reporting shows persistent high-volume scams, phishing/credential harvesting, and BEC losses, with Q1 2025 direct losses at NZD $7.8 M (second highest on record) and continuing over 1,300 incidents per quarter throughout 2025. These patterns highlight entry point risks (identity compromise, invoice redirection) that frequently precede or amplify data breach impacts in SaaS and healthcare contexts.

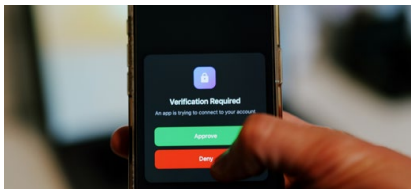
NCSC’s Cyber Threat Report 2025 underscored Ransomware-as-a-Service, exploitation of known vulnerabilities, and supply-chain blind spots—all relevant to a patient portal that integrates with multiple GP systems and third-party services.

Simultaneously, the New Zealand Banking Association introduced new scam protection commitments to reduce consumer harms, demonstrating national momentum to disrupt identity-driven fraud vectors that often intersect with healthcare portals (e.g., password reuse, phishing led account takeover).

Probable intrusion vectors for patient portals

Given MMH's early scoping (document level access without confirmed core database compromise), three plausible patterns warrant consideration for similar environments:





Document store misconfiguration / weak access controls

Many patient portals maintain a separate store for uploaded documents (referrals, lab reports, attachments). If that store (e.g., object storage, Server Message Block (SMB)/ Network File System (NFS) shares, or third-party document services) is reachable via less restricted endpoints, threat actors can request or enumerate documents without touching the relational patient database. Least privilege Identity Access Management (IAM) signed Uniform Resource Locators (URLs) with short Time-to-live (TTL)s, Web Application Firewall (WAF) rules, and strong service-to-service auth are essential mitigations.

API pathway abuse or unvalidated token scopes

Complex portals expose multiple microservices. If token scopes or role claims are too permissive, or if an internal API is inadvertently exposed, an attacker with lower privilege access may still retrieve document objects. Strong Application Programming Interface (API) gateway policies, schema validation, JSON Web Token (JWT) scope audits, and dynamic authorisation (Attribute-Based-Access-Control (ABAC)/Role-Based-Access-Control (RBAC) reduce this risk.

Credential stuffing and session hijack against non-Multi-Factor Authentication (MFA) users

With ongoing NZ trends in phishing/credential harvesting and large quantities of leaked credentials (globally and locally), accounts lacking MFA are prime targets. Even if the core Database access is protected, session tokens can enable retrieval of documents tied to the authenticated user or practice admin roles. Mandatory MFA, risk based authentication, and adaptive session protections are critical.

Recommendations

1) Technical hardening for health portals and SaaS platforms

- Enforce MFA for all users (patients, practice staff, administrators); default to Time-Based One-Time Password (TOTP)/app based authenticators and prohibit SMS only factors for sensitive data flows. Tie support workflows to strong identity verification and helpdesk challenge scripts to resist social engineering.
- Isolate document stores behind private endpoints, mutual Transport Layer Security (TLS), and service to service authentication; require short lived signed URLs with least privilege IAM. Continuously scan object storage policies for misconfigurations
- Secure APIs with strict scopes and dynamic authorisation: audit JWT/claims, token lifetimes, and limit tokens; implement gateway level schema validation and rate limits; block exploitation and known attack campaigns via WAF.
- Instrument Endpoint Detection and Response (EDR)/ Extended Detection and Response (XDR) and WAF telemetry based on relevant attacks; calibrate Distributed Denial of Service (DDoS) /WAF rules to reflect local noise vs true signals.
- Secrets and key rotation: automate rotation for API keys, storage credentials, and signing keys; monitor for key leakage in Continuous Integration (CI)/ Continuous Deployment (CD) artefacts and support systems.

2) Identity, access, and credential hygiene

- Mandatory password resets and login risk prompts for affected cohorts; deploy risk based auth to challenge logins from new devices/locations and step-up verification for document export actions.
- Strong RBAC/ABAC: separate patient, GP, practice admin, and support roles; deny by default for document retrieval APIs; use just in time elevation with timeboxed approvals for support engineers.

3) Operational resilience and incident response

- Tabletop exercises simulating document store compromise: rehearse discovery, scoping, law enforcement engagement, Privacy Commissioner notification, and GP/patient comms (multilanguage templates; SMS/email/portal banners).
- Crisis communications playbook: publish clear FAQs, breach specific security steps (enable MFA, change passwords, beware phishing), and coordinate with sector bodies (GPNZ, College of GPs) to ensure frontline awareness.
- Supply chain due diligence: require security attestations (e.g., ISO 27001/SOC2), software bill of materials (SBOMs) for critical components, and patch Service Level Agreements (SLAs), specifically assess hidden dependencies (cloud storage addons, document viewers).

4) Antifraud and consumer protection alignment

- Align portal notifications with bank anti scam measures (confirmation of payee concepts for payments inside the portal, pre-action warnings, 24/7 reporting); share indicators with NZ anti scam Alliance and banks to counter Business Email Compromise (BEC) and invoice redirection affecting practices.

Implications for NZ healthcare and digital services

The MMH incident is a timely reminder that NZ's health data ecosystems, often hybrid, interconnected across public and private providers, must treat document repositories and supporting microservices as first class attack surfaces, not merely adjuncts to the "core" patient database. Sector leaders should combine technical hardening with rapid, empathetic communications to blunt secondary harms (phishing, fraud). With scams and credential attacks continuing at scale, and ongoing multiagency efforts to uplift consumer protections, consistent MFA, least privilege design, and API discipline are non-negotiable foundations for trust.

Conclusion

While MMH's preliminary statements suggest limited scope (document level access, no proven core database breach), the incident underscores the fragility of adjacent data stores and the operational importance of rapid, coordinated response. It is important to consider a defence in depth approach and by implementing the recommendations above we can meaningfully reduce risk and strengthen public confidence.

References

[1] Manage My Health, "MMH Cyber Breach Update," Scoop, Jan. 2, 2026. https://www.scoop.co.nz/stories/BU202601/S00009.htm
[2] Radio New Zealand, "Health NZ says systems unaffected by ManageMyHealth app breach," Jan. 2, 2026. https://www.rnz.co.nz/news/national/583067
[3] New Zealand Government—Beehive, "Review commissioned of ManageMyHealth cyber security breach," Jan. 5, 2026. https://www.beehive.govt.nz/release/review-commissioned-managemyhealth-cyber-security-breach
[4] Stuff (NZ), "Government launch review of ManageMyHealth cyber security breach," Jan. 4, 2026. https://www.stuff.co.nz/nz-news/360920836
[5] Newstalk ZB / NZCity, "More than a hundred thousand Kiwis may have been affected in a cyber security breach," Jan. 1, 2026. https://home.nzcity.co.nz/news/article.aspx?id=437040
[6] Helm News, "Neighbourly went offline in January 2026 over a suspected data breach," Jan. 2, 2026. https://helm.news/2026-01-02/neighbourly-new-zealand-social-media-app-went-offline-january-over.html
[7] National Cyber Security Centre (NZ), "Cyber Threat Report 2025 (PDF)," 2025. https://www.ncsc.govt.nz/assets/insights/cyber-threat-report/NCSC-CyberReport2025-FINAL.pdf
[8] NZ Banking Association, "Banks step up customer scam protections and compensation," Apr. 23, 2025. [Online]. Available: https://nzba.org.nz/banks-step-up-customer-scam-protections-and-compensation/
[9] BlackVeil Security (NZ), "New Zealand Is Being Targeted... APAC Attack Data," Jan. 2, 2026. [Online]. Available: https://blackveil.co.nz/blog/apac-coordinated-attack-january-2026
[10] Otago Daily Times (NZ), "Health app cyber breach 'incredibly concerning" Jan.1. 2026. [Online]. Available: https://www.odt.co.nz/news/national/health-app-cyber-breach-incredibly-concerning
[11] utf9K "A recap of the ManageMyHealth data breach so far" Jan.4.2026. [Online]. Available: https://utf9k.net/blog/managemyhealth-data-breach-recap/

Crypto C2:

How attackers use Ethereum smart contracts to evade takedowns

This article was written by:
Marco Pretorius
Threat Researcher

The concept of "EtherHiding" or serving malicious code through blockchain technology was first documented by Guardio Labs in 2023 [7]. There has been a recent trend of Node.js malware using Ethereum smart contracts to both obfuscate and ensure the reliability of its command and control (C2) channels.

A smart contract is a digital 'contract' that can execute predefined actions via code when certain conditions are met. They are stored and executed on a blockchain; a decentralised, distributed ledger that securely records transactions across a network of computers. This architecture makes smart contracts decentralised and immutable, both desirable qualities for C2 mechanisms. The Tsundere botnet started implementing this in October 2024 soon followed by EtherRat around December 2025.

Tsundere botnet

Research by Kaspersky has linked the Tsundere botnet with the threat actor, Koneko, that has been associated with previous advertising of the "123 stealer" credential stealer [6].

The Tsundere botnet has seen a variety of distribution methods including through pirated software and game installers, as well as distribution via malicious npm packages through typosquatting. This is when a npm package mimics the names of popular libraries like Puppeteer and Bignum.js to deceive developers into installation [3].

The main benefit of using a smart contract to route malware traffic is that you can easily change the C2 endpoint with the provided smart contract function.

Figure 1: A block chain transaction changing the c2 endpoint to ws://193.24.123[.]68:3011

This allows the malware to function even if a C2 server is taken down by authorities as the Threat Actor can simply swap to a new one. The decentralised nature of smart contracts makes removing the contract itself improbable without blocking Ethereum RPC nodes completely within an environment.

EtherRAT

Although the initial public exploitation campaigns targeting React2Shell (**CVE-2025-55182**) saw mainly cryptocurrency miners being deployed, some of the targeted attacks saw more sophisticated malware usage. EtherRAT is an evolution of prior attack campaigns combining previously known techniques into a novel attack chain [1].

EtherRAT shares some similarities with Tsundere in that it also downloads and uses its own Node.js runtime environment as well as relying on Ethereum smart contracts for command-and-control routing.

Contract: 0x22f96d61cf118efabc7c5bf3384734fad2f6ead4

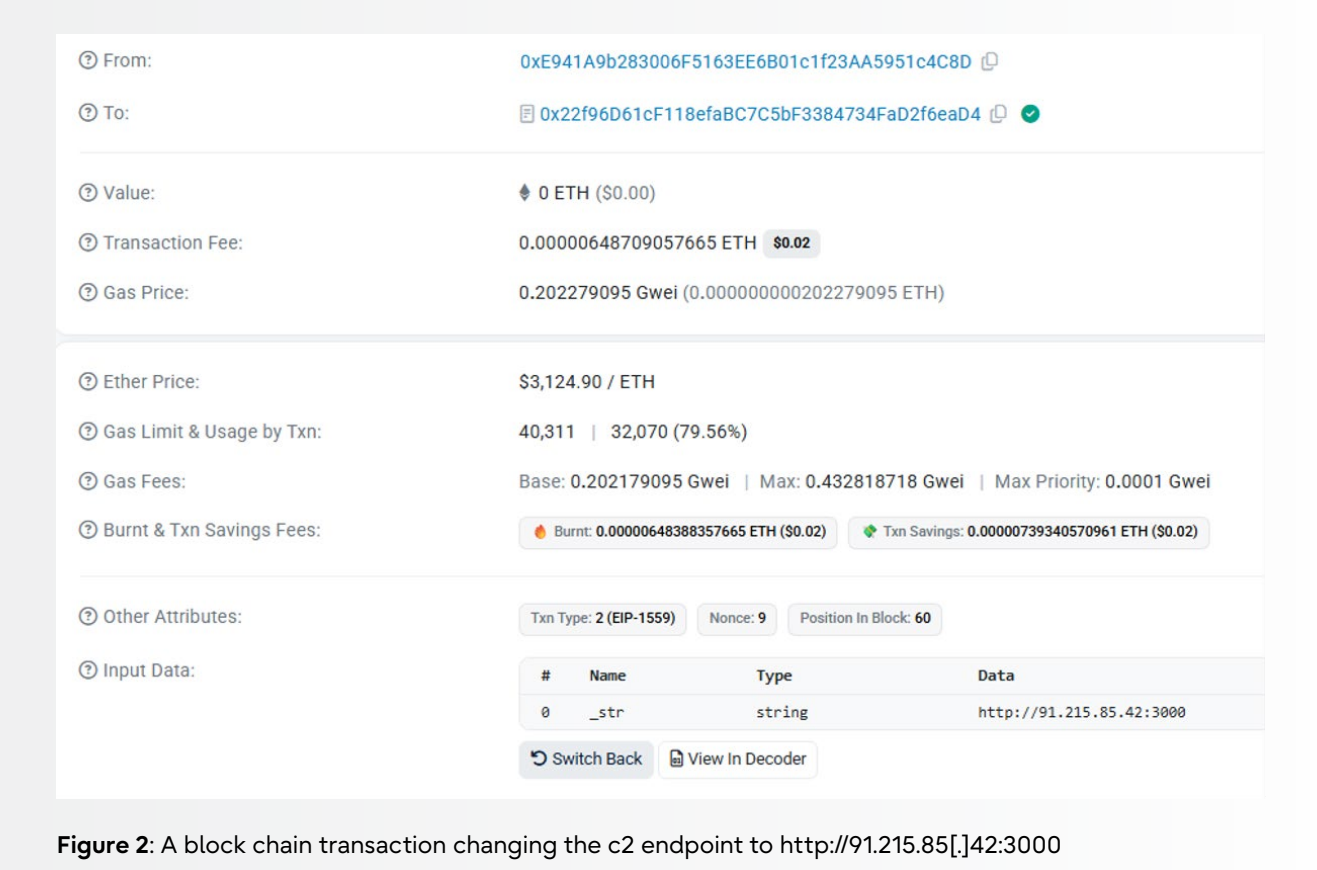


Figure 2: A block chain transaction changing the c2 endpoint to http://91.215.85[.]42:3000

This string can be retrieved by the malware and is used during its c2 beaconing stage. The beaconing itself masquerades as a Content Delivery Network (CDN) attempting to hide among legitimate web traffic. Using common web file extensions such as "css" and a variety of image extensions.

EtherRat's use of less common persistence mechanisms. By implementing the capability of using 5 independent mechanisms it allows flexibility and reliability. This provides the benefit of using lesser-known persistence mechanisms such as XDG autostart entries, while having more reliable persistence such as Cron jobs as a backup.

A final point of interest is the "/api/reobf" endpoint. When first connecting to its C2 server EtherRat sends its own source code to this endpoint before overwriting its own code with the response. Although the exact motivation behind this isn't known, it will likely work around static fingerprinting while allowing the attackers to modify the malware. This inhibits analysis and can be used to ensure that follow up stages are only delivered to real environments.

In both cases the malware leverages the decentralised nature of blockchain technology to make takeover or domain seizure difficult. The smart contracts allow them to rapidly swap the C2 address while blockchain consensus and immutability helps protect the "resolver".

Behavioural indicators:

Network

Alert on Rapid POST requests to multiple Ethereum RPCs.

Endpoint

Look for Node.js processes spawning from hidden directories (eg. ".local/share/") instead of /usr/bin/

Technical indicators:

Ethereum RPCs used
https://eth[.]llamarpc[.]com
https://mainnet[.]gateway[.]tenderly[.]co
https://rpc[.]flashbots[.]net/fast
https://rpc[.]mevblocker[.]io
https://eth-mainnet[.]public[.]blastapi[.]io
https://ethereum-rpc[.]publicnode[.]com
https://rpc[.]payload[.]de
https://eth[.]drpc[.]org
https://eth[.]merkle[.]io

Tsundere Botnet C2 Server: ws://193.24.123[.]68:3011
EtherRat C2 Server: http://91.215.85[.]42:3000

Recommendations

- Provided there is no business need for them, consider implementing network egress filtering to restrict access to Ethereum RPCs.
- Monitor for Node.js processes executing from unusual or hidden directories.
- Implement strong software supply chain security practices, including auditing npm package dependencies.
- Utilise behavioural analytics to detect unusual network beaconing patterns.

References

[1] G. Baran, "North Korean Hackers Exploit React2Shell Vulnerability in the Wild to Deploy EtherRAT," Cyber Security News, Dec. 10, 2025. https://cybersecuritynews.com/hackers-exploit-react2shell-vulnerability/ (accessed Jan. 15, 2026).

[2] Kaspersky, "Cute but deadly: Kaspersky reveals the Tsundere botnet that plays hot-and-cold with Windows users," /, Nov. 20, 2025. https://www.kaspersky.com/about/press-releases/cute-but-deadly-kaspersky-reveals-the-tsundere-botnet-that-plays-hot-and-cold-with-windows-users (accessed Jan. 15, 2026).

[3] T. S. Dutta, "Tsundere Botnet Abusing Popular Node.js and Cryptocurrency Packages to Attack Windows, Linux, and macOS Users," Cyber Security News, Nov. 20, 2025. https://cybersecuritynews.com/tsundere-botnet-abusing-popular-node-js-and-cryptocurrency-packages/ (accessed Jan. 15, 2026).

[4] etherscan.io, "Ethereum Transaction Hash: 0x97b45dc509... | Etherscan," Ethereum (ETH) Blockchain Explorer, 2025. https://etherscan.io/tx/0x97b45dc509931fea932d5c6d6eb1d8628f90391ba7da12a73aac71705ae1b566 (accessed Jan. 15, 2026).

[5] etherscan.io, "Ethereum Transaction Hash: 0x834769584d... | Etherscan," Ethereum (ETH) Blockchain Explorer, 2025. https://etherscan.io/tx/0x834769584d0305b7517aea4f17d3382e68e86b535c190bba51d56981c83a4705 (accessed Jan. 15, 2026).

[6] Kaaviya, "New '123 | Stealer' Advertised on Underground Hacking Forums for $120 Per Month," Cyber Security News, Jul. 04, 2025. https://cybersecuritynews.com/123-stealer-on-underground-hacking-forums/ (accessed Jan. 15, 2026).

[7] Guardio, "'EtherHiding' — Hiding Web2 Malicious Code in Web3 Smart Contracts," Medium, Oct. 29, 2023. https://labs.guard.io/etherhiding-hiding-web2-malicious-code-in-web3-smart-contracts-65ea78efad16

[8] S. Threat, "EtherRAT: DPRK uses novel Ethereum implant in React2Shell attacks," Sysdig.com, Dec. 08, 2025. https://www.sysdig.com/blog/etherrat-dprk-uses-novel-ethereum-implant-in-react2shell-attacks (accessed Jan. 15, 2026).

[9] T. H. News, "Tsundere Botnet Expands Using Game Lures and Ethereum-Based C2 on Windows," The Hacker News, Nov. 20, 2025. https://thehackernews.com/2025/11/tsundere-botnet-expands-using-game.html (accessed Jan. 15, 2026).

FUJITSU

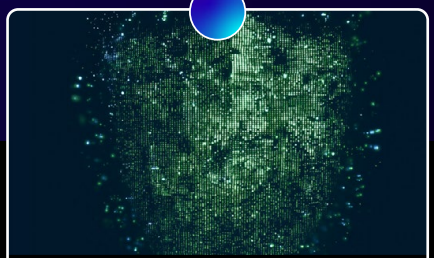
Fujitsu Cyber

Built to enhance cyber resilience

We are a Trans-Tasman team providing **end-to-end cyber security solutions designed to protect, enable, and transform organisations in Oceania.** We help you align with best practices, strengthen your defences, and ensure your systems are resilient and compliant. **Our cyber security services are structured around three core pillars:**

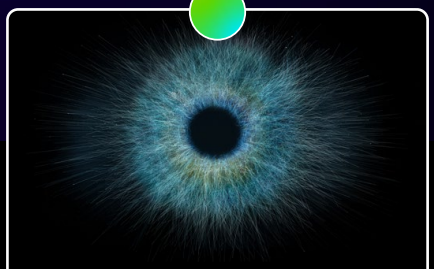
Advisory & Assurance

Delivering tailored consulting, strategic roadmaps, and hands-on support to help you identify risks, align with standards, and build resilience - empowering confident, secure business growth.



Technical Consulting

Uncover vulnerabilities and validate your defences through expert-led assessments and security testing. We provide visibility, assurance, and a clear path to uplift and secure your cyber posture.



Managed Security Operations

Providing 24/7 monitoring, proactive threat detection, and swift incident response to safeguard your organisation from evolving cyber threats. Through advanced analytics, actionable intelligence, and expert guidance, we keep you secure, resilient, and future-ready.

Fujitsu Cyber draws on all parts of the business to identify key trends and changes with relevance to companies operating in New Zealand and Australia, both now and in the future. These threats are not solely technical. They can also arise from business operations, regional conditions in New Zealand and Australia, or global events that influence the cyber security environment in both countries. You may also be interested in our 'Best of 2025 Threat Intelligence Report' here

Our research is the result of collaboration across the entire Australia and New Zealand team, including detection engineers, threat intelligence analysts, threat researchers, automation engineers, digital forensics and incident response specialists, as well as training and awareness professionals.

Authors:

Tanya Wessels
Principal Security Consultant

Nicky Pretorius
Senior Security Consultant

Ben Sparks
Principal Security Consultant

Marco Pretorius
Threat Researcher

Curated by:
Thomas Hacker
Cyber Security and Threat Intelligence Analyst

Compiled by:
Ed Goodacre
Digital Content Specialist

Feedback

We welcome feedback on the usefulness of this report or requests for specific focus.

Please send your feedback to **Thomas.Hacker@fujitsu.com**

Fujitsu Cyber