INC Ransom Affiliate Model Enabling Targeting of Critical Networks

ACSC Australian **Cyber Security** Centre

CERT TONGA
Tonga Computer Emergency Response Team

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
NEW ZEALAND

Table of contents

Context

This advisory, developed by the Australian Cyber Security Centre (ACSC), Kingdom of Tonga's National Computer Emergency Response Team (CERT Tonga) and New Zealand's National Cyber Security Centre (NCSC) outlines the activity of ransomware group INC Ransom and their affiliate network, and the threat their operations currently pose to networks hosted in Australia, New Zealand, and Pacific island states. The advisory is intended to be understood by both general and technical users. ACSC, CERT Tonga and NCSC encourage network defenders to read and apply the mitigations described in this advisory.

Key points

- INC Ransom operates a Ransomware-as-a-Service (RaaS) operation. INC Ransom affiliates have compromised organisations worldwide, including Australia, New Zealand and the Pacific Island states since 2023.
- INC Ransom affiliates employ double extortion tactics. Affiliates steal sensitive data, encrypt files, and threaten to publish stolen data via their dedicated leak site (DLS), to pressure organisations into paying the ransom.
- INC Ransom affiliates rely on compromised credentials or public facing vulnerabilities for initial access into victim's networks.

Background

INC Ransom is a financially motivated cybercriminal group that emerged in mid-2023. INC Ransom provides a Ransomware-as-a-Service (RaaS)[1] operation to its affiliate network. Affiliate members use INC ransomware to target organisations, encrypting vital information before directing the affected organisations to a dark web site or demanding payment in exchange for a decryption key. While affiliate members distribute the ransomware, INC Ransom extorts affected organisations and handles payments.

Their strategy primarily targets high-value entities handling sensitive data, with activity suggesting a trend towards disproportionately targeting health care providers worldwide.

INC Ransom and their affiliate network previously targeted the United States and United Kingdom, but since early 2025, they have been increasingly observed targeting Australia, New Zealand and Pacific island states.

INC Ransom is also known as Tarnished Scorpion and GOLD IONIC.

1 Ransomware-as-a-Service (RaaS) is an arrangement between an operator and an affiliate. The RaaS operator develops and maintains the ransomware – including developing payment portals and dedicated leak sites – and sells access to an affiliate. The affiliate performs the intrusion and is responsible for the deployment of the ransomware payload onto the target network. The operator and the affiliate then split any profits.

INC Ransom impact to the Health Care sector in Australia, the Kingdom of Tonga and New Zealand

Australia

Between 1 July 2024 and 31 December 2025, the ACSC responded to a total of 11 reported INC Ransom related incidents in Australia, affecting predominately Professional Services and Health Care.

Since January 2025, the ACSC has observed INC Ransom affiliates target Australian Health Care sector entities using compromised accounts. Upon initial access, affiliates have conducted privilege escalation by creating admin level accounts and moving laterally within victim networks. INC Ransom deployed malicious files with the file name win.exe. In some incidents, the ACSC has observed data exfiltration of personally identifiable and medical information. Ransom notes were found containing a link to the INC Ransom Tor-based DLS and INC Ransom contact details.

Kingdom of Tonga

On 15 June 2025, the Tongan Ministry of Health (MoH) ICT environment was impacted by a ransomware attack that rendered core services inaccessible and disrupted the national health care network. An INC Ransom ransom note was found embedded within MoH's file system. INC Ransom claimed responsibility for the attack on 26 June 2025 via their dark web DLS.

As part of this incident, the Russia-based cybercriminal Roman Khubov (also known as "blackod") controlled the malicious infrastructure used for data exfiltration in the MoH incident.

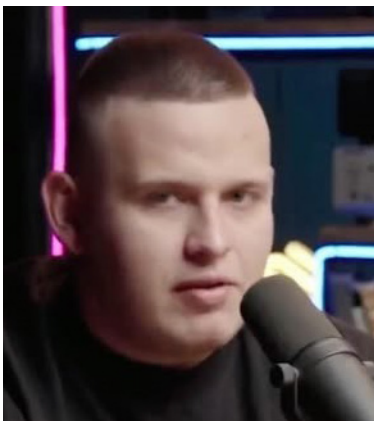

Figure 1. Roman Khubov (aka "blackod")

New Zealand

Ransomware and data extortion continues to have devastating impacts in New Zealand, with opportunistic actors and groups impacting organisations in all sectors of the economy. In May 2025, the NCSC received an incident notification from an organisation in the health sector stating that it had been impacted by ransomware. Many of the organisation's servers and endpoint devices had been encrypted, and a large amount of data was stolen. INC Ransom claimed responsibility for this incident, and published the dataset on its DLS.

Technical Details

INC Ransom affiliates often gain initial access to target systems through spear-phishing campaigns, exploiting known vulnerabilities in unpatched internet-facing devices or using purchased valid account credentials from initial access brokers[2].

INC Ransom uses legitimate software to compress data (e.g., 7-Zip and WinRAR) before exfiltrating sensitive data from affected networks. INC Ransom uses legitimate software to facilitate exfiltration of sensitive data (e.g. rclone). Following successful data encryption, INC Ransom leaves a ransom note stating demands and contact instructions.

If targeted entities do not pay the requested ransom amount, INC Ransom engages double-extortion tactics, by publishing entity names and exfiltrated data to its DLS.

INC Ransom tactics, techniques and procedures (TTPs) shows significant overlap with other RaaS operations. Groups with similar TTPs include Lynx ransomware and historical RaaS operations Nemty, Nemty X, Karma and Nokoyawa.

See Appendix A for Mitre ATT&CK Techniques observed in INC Ransom incidents reported to the ACSC between 1 July 2024 and 31 December 2025.

Mitigations

The authoring agencies recommend organisations and government ministries implement the following controls to reduce the risk of compromise by INC Ransom and to enhance detection of this threat.

Mitigating controls

Maintain regular and tested backups

Maintain regular backups of critical systems and data. Store backups in a manner that prevents unauthorised access, modification or deletion, and regularly test backups to ensure systems can be restored when required.

Restrict network traffic

Restrict inbound and outbound network traffic to only what is required for business operations. Use network-filtering devices, such as firewalls, web content filters and email content filters, to block unnecessary services and reduce exposure to malicious activity, including phishing and malicious attachments.

Harden remote access services

Review VPN and other remote access settings to ensure only required resources, servers and applications can be accessed. Access should be restricted to authorised users and permissions reviewed regularly.

2 Initial access brokers (IAB) are cybercrime threat actors who sell access, such as legitimate credentials, for target networks to other cybercrime threat actors. These credentials are often gained through other breaches and data theft.

Restrict remote management tools

Restrict the use of remote management tools, such as TeamViewer and AnyDesk, to authorised administrators only. Disable these tools where they are not required and monitor their use for unauthorised or suspicious activity.

Implement multi-factor authentication

Implement phishing-resistant multi-factor authentication (MFA) for remote access services, online services and privileged accounts to reduce the risk of credential compromise. Prioritise MFA protections for internet-facing services and administrative access.

Control privileged access

Restrict and manage privileged access to reduce the impact of credential compromise. Use unique, identifiable accounts for all privileged users to ensure accountability and attribution of administrative actions. Grant privileged permissions in accordance with the principle of least privilege, and separate standard user accounts from privileged administrator accounts to limit exposure. Restrict or disable shared, built-in and local administrator accounts where possible.

Maintain robust vulnerability management

Regularly scan for known vulnerabilities. Apply security patches, updates or vendor workarounds to operating systems, applications and network devices in a timely manner. Verify that remediation actions are effective. Prioritise vulnerabilities affecting internet-facing services and those known to be exploited by ransomware actors. Remove or replace unsupported or end-of-life systems where possible. Where not immediately feasible, implement compensating controls such as isolation and enhanced monitoring until systems can be removed or replaced.

Enhancing detection

Monitor network activity

Monitor network traffic and firewall logs for indicators of malicious activity, including unusual internal scanning, brute force attempts and unauthorised access attempts. Focus monitoring efforts on activity originating from within the corporate network or between network zones.

Detect unauthorised remote access

Monitor for unauthorised use of remote access services and remote management tools commonly leveraged by ransomware groups.

Centralise and protect event logging

Centralise security-relevant event logs and records of configuration changes. Protect logs from unauthorised modification or deletion and retain them to support investigation and response activities. Use endpoint detection and response (EDR) or extended detection and response (XDR) capabilities, where available, to support timely detection of malicious behaviour.

Hunt for indicators of compromise

Hunt for indicators of compromise associated with INC Ransom, including anomalous behaviour in system, network and endpoint logs that aligns with publicly reported tactics and techniques (see Appendix A - Mitre ATT&CK Tactics and Techniques).

Resources

ACSC

Search for the following at cyber.gov.au

Protect yourself from ransomware — practical guidance on steps organisations and individuals can take to reduce the risk and impact of a ransomware attack.

Secure administration — guidance on administering systems in a secure, accountable and auditable manner, including restricting administrative access and protecting management interfaces.

Best practices for event logging and threat detection — guidance on establishing effective event logging practices and using logs to detect cyber security events.

Implementing network segmentation and segregation — guidance on planning and applying segmentation and segregation strategies to reduce the impact of network intrusions.

Practical cyber security tips for business leaders — accessible advice on basic controls, including MFA, that organisations should apply to improve their defensive posture.

Mitigations for network defence — outlines foundational measures such as patching, MFA and segmentation to reduce network attack surfaces.

CERT Tonga

See Advisory - Inc Ransomware Attack for additional information, at cert.gov.to

NCSC

See Protect your organisation against ransomware for additional information, at ncsc.govt.nz

Appendices

Appendix A - Mitre ATT&CK Tactics and Techniques

Mitre ATT&CK Techniques observed in INC Ransom incidents responded to by the ACSC between 1 July 2024 and 31 December 2025.

INC Ransom affiliate ATT&CK Techniques for Enterprise - Reconnaissance – Table 1

Technique title	ID	Use
Exploit Public-facing application	T1190	INC Ransom affiliates exploit known vulnerabilities in unpatched, internet-facing devices to gain remote code execution with administrative privileges. In some instances, affiliates targeted exposed and vulnerable edge devices like routers for initial access.
External remote services	T1133	INC Ransom affiliates gain access to victim networks by authenticating to virtual private network (VPN) gateways without multi-factor authentication (MFA). Typically, affiliates utilised compromised account credentials, including credentials for legacy or service accounts.
Valid accounts	T1078	INC Ransom affiliates leverage compromised credentials to authenticate against externally exposed infrastructure. Affiliates either harvest these credentials directly or acquire them from cybercriminal networks, such as initial access brokers.

INC Ransom affiliate ATT&CK Techniques for Enterprise – Execution—Table 2

Technique title	ID	Use
Serverless execution	T1648	INC Ransom affiliates utilise victim database infrastructure as an execution medium to modify configuration data without deploying traditional binaries.

INC Ransom affiliate ATT&CK Techniques for Enterprise – Persistence—Table 3

Technique title	ID	Use
Create account	T1136	INC Ransom affiliates create new administrator accounts to maintain persistent privileged access.
External remote services	T1133	INC Ransom affiliates access the target environment through legitimate remote services and continue to use these remote entry points to maintain persistence.
Valid accounts	T1078	INC Ransom affiliates leverage valid account credentials obtained for initial access to maintain persistence and operational activity.

INC Ransom affiliate ATT&CK Techniques for Enterprise—Privilege Escalation— Table 4

Technique title	ID	Use
Exploration for Privilege Escalation	T1068	INC Ransom affiliates identified internal vulnerabilities and exploited them to elevate privileges. Notably, INC Ransom affiliates deployed legitimate but vulnerable drivers to perform a Bring Your Own Vulnerable Driver (BYOVD) attack and escalate system access on compromised systems.
Valid accounts	T1078	INC Ransom affiliates use credentials for service accounts and other accounts with higher privileges to perform administrative actions without the use of additional tooling or exploits.
Account Manipulation	T1098	INC Ransom affiliates created or modified accounts to expand their access and maintain persistence within the environment. INC Ransom affiliates adjusted account privileges or added new accounts to strengthen their control.

INC Ransom affiliate ATT&CK Techniques for Enterprise—Defence Evasion—Table 5

Technique title	ID	Use
Impair defences	T1562	INC Ransom affiliates ingress malicious tooling to tamper with security processes or services.
Masquerading	T1036	INC Ransom affiliates rename malicious tools to names of legitimate system or application files to avoid detection.
Valid accounts	T1078	INC Ransom affiliates continue to utilise valid accounts to mask their intrusions as legitimate user activity.

INC Ransom affiliate ATT&CK Techniques for Enterprise—Credential Access—Table 6

Technique title	ID	Use
Brute force	T1110	INC Ransom affiliates use open-source password-cracking tools to perform brute-force and dictionary attacks against authentication services.
OS credential dumping	T1003	INC Ransom affiliates use tooling to extract cached credentials and NTLM hashes from compromised systems.

INC Ransom affiliate ATT&CK Techniques for Enterprise – Discovery—Table 7

Technique title	ID	Use
File and directory discovery	T1083	INC Ransom affiliates enumerate local files and directories to identify valuable data for exfiltration.
Network service discovery	T1046	INC Ransom affiliates execute open-source tools, like NetScan, for internal reconnaissance. INC Ransom affiliates use said tools to scan internal hosts and identify active network services.
Network share discovery	T1135	INC Ransom affiliates enumerate network shares to locate accessible data storage and back-up locations. INC Ransom affiliates use results to identify potential data repositories for collection and encryption.
Process discovery	T1057	INC Ransom affiliates deploy utilities to list running processes and identify targets of interest. Process discovery informs subsequent actions.
Remote system discovery	T1018	INC Ransom affiliates enumerate remote systems and active connections to understand internal network topology to plan lateral movement and eventual data collection, and encryption.

INC Ransom affiliate ATT&CK Techniques for Enterprise—Lateral movement—Table 8

Technique title	ID	Use
Exploitation of remote services	T1210	INC Ransom affiliates exploit internal remote services to gain additional footholds and expand ransomware propagation.
Lateral tool transfer	T1570	INC Ransom affiliates transfer tooling across internal systems to support continued lateral movement and execution.
Remote services	T1021	INC Ransom affiliates utilise legitimate remote services to laterally move across the network using existing access to compromised account credentials. By relying on legitimate internal services, INC Ransom affiliates are able to reach further into compromised networks without obvious detection.

INC Ransom affiliate ATT&CK Techniques for Enterprise – Collection— Table 9

Technique title	ID	Use
Data Staged	T1075	INC Ransom affiliates aggregated collected data into staging locations before exfiltration. Once staged, INC Ransom affiliates organised and compressed the data with archiving utilities to prepare it for transfer out of the environment.
Archive collected data	T1560	INC Ransom affiliates use compression utilities to package collected data prior to exfiltration. INC Ransom affiliates use common, free archiving tools, such as 7-Zip, to reduce file size and simplify data transfer.
Automated collection	T1119	INC Ransom affiliates deploy tooling to automatically gather data and support ransomware deployment to streamline collection and encryption efforts across multiple endpoints.
Data from information repositories	T1213	INC Ransom affiliates access and extract information from internal information repositories that often contain high-value records, like Personal Identifiable Information (PII) or sensitive commercial data.
Data from local system	T1005	INC Ransom affiliates collect data of interest directly from the local systems they compromise.

INC Ransom affiliate ATT&CK Techniques for Enterprise—Command and Control—Table 10

Technique title	ID	Use
Ingress tool transfer	T1105	INC Ransom affiliates transfer various tools into the target environments to expand operational capability. They commonly deploy free and widely available tools such as NetScan, 7-Zip and FileZilla through existing Command and Control channels to enable internal reconnaissance, data compression and data transfer.
Remote access tools	T1219	INC Ransom affiliates utilise legitimate remote access tools to maintain interactive access to the victim environment.

INC Ransom affiliate ATT&CK Techniques for Enterprise – Exfiltration—Table 11

Technique title	ID	Use
Exfiltration over web service	T1567	INC Ransom affiliates exfiltrate data through external web-accessible services.

INC Ransom affiliate ATT&CK Techniques for Enterprise – Impact—Table 12

Technique title	ID	Use
Data encrypted for impact	T1486	INC Ransom affiliates deploy ransomware to encrypt data across compromised systems, rendering victim documents and, occasionally entire systems, inaccessible. INC Ransom affiliates leverage data encryption to disrupt operations and coerce ransom payments from victims.
Defacement	T1491	INC Ransom affiliates place ransom notes throughout encrypted directories to signal compromise and intimidate victims.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ACSC