ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

INC Ransomware Expands Cross-Platform Capabilities Targeting Enterprise and Mainframe Infrastructure Across the Asia-Pacific Region

TLP: CLEAR
Distribution: Public
Advisory on: INC Ransomware Expands Cross-Platform Capabilities Targeting Enterprise and Mainframe Infrastructure Across the Asia-Pacific Region
Severity: High
Threat Type: Ransomware / Data Extortion / Cross-Platform Malware
Date: 05 July 2026

Executive Summary

BGD e-GOV CIRT has analyzed publicly available threat intelligence regarding an active INC ransomware campaign targeting organizations across the **Asia-Pacific region**. The analysis reveals a significant evolution in ransomware capabilities, with threat actors expanding beyond traditional Windows environments to support multiple enterprise computing architectures, including IBM Z (s390x), PowerPC, SPARC64, RISC-V, Linux, and VMware ESXi platforms.

The exposed attacker infrastructure contained ransomware payloads, Active Directory reconnaissance data, Group Policy deployment scripts, credential theft artifacts, custom data exfiltration tools, and victim information. The findings demonstrate a mature ransomware operation capable of compromising heterogeneous enterprise environments and critical infrastructure.

Although no confirmed victims have been identified in Bangladesh at the time of publication, organizations operating enterprise servers, virtualization platforms, Active Directory environments, or legacy computing systems should review their exposure and strengthen defensive controls.

Risk Level	High
TLP	CLEAR
Threat Actor	INC Ransomware
Known Aliases	Lynx, Sinobi
Malware Family	INC Ransomware
Primary Targets	Manufacturing, Healthcare, Food & Beverage, Education, Pharmaceuticals
Observed Region	Asia-Pacific
Bangladesh Impact	No confirmed victims identified; organizations are advised to remain vigilant

Threat Overview

INC Ransomware is an active ransomware operation that continues to evolve its capabilities to target enterprise infrastructure. Recent analysis identified exposed operational servers containing deployment scripts, ransomware binaries, reconnaissance data, and custom tooling used during attacks.

Unlike conventional ransomware campaigns focused primarily on Windows systems, this campaign demonstrates deliberate expansion toward enterprise and mainframe environments through cross-platform payload development.

The campaign indicates increased targeting of critical infrastructure, virtualization platforms, and heterogeneous enterprise environments.

Technical Analysis

Exposed Operational Infrastructure

Threat intelligence analysis identified two exposed operational servers used by an INC ransomware affiliate.

- The first server functioned as a deployment staging environment hosting Windows ransomware payloads and Group Policy deployment scripts.
- The second server served as the operational working environment containing approximately 675 MB of attacker tooling, reconnaissance data, configuration files, credential artifacts, and exfiltrated victim information.

The recovered files provided valuable insight into attacker methodology throughout the intrusion lifecycle.

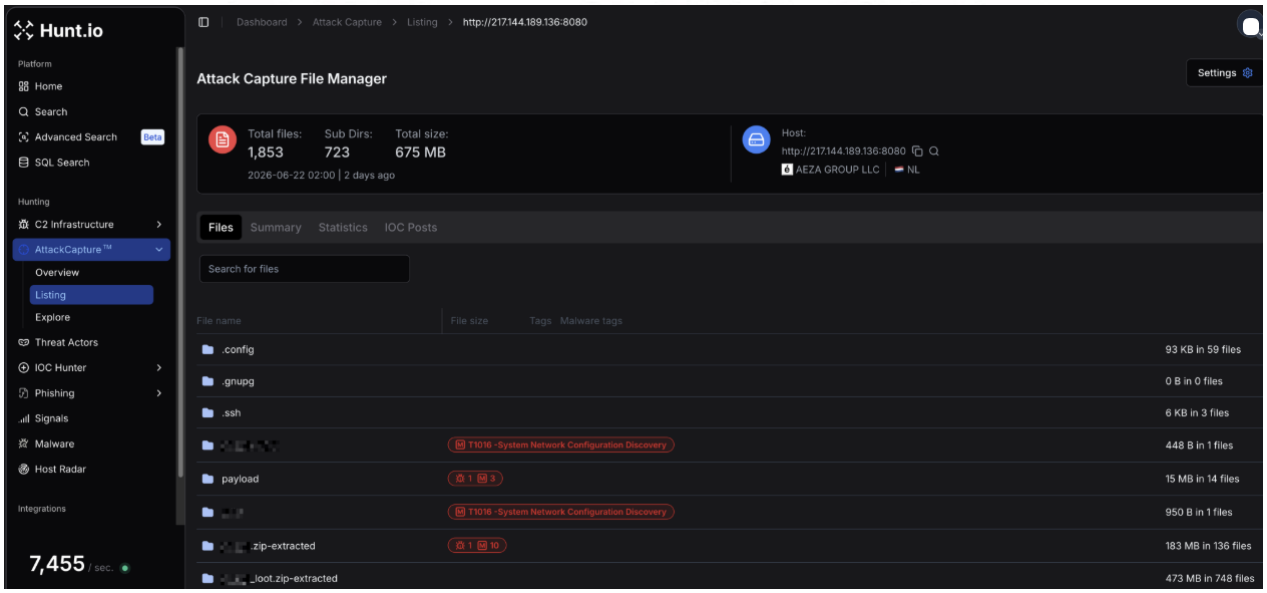
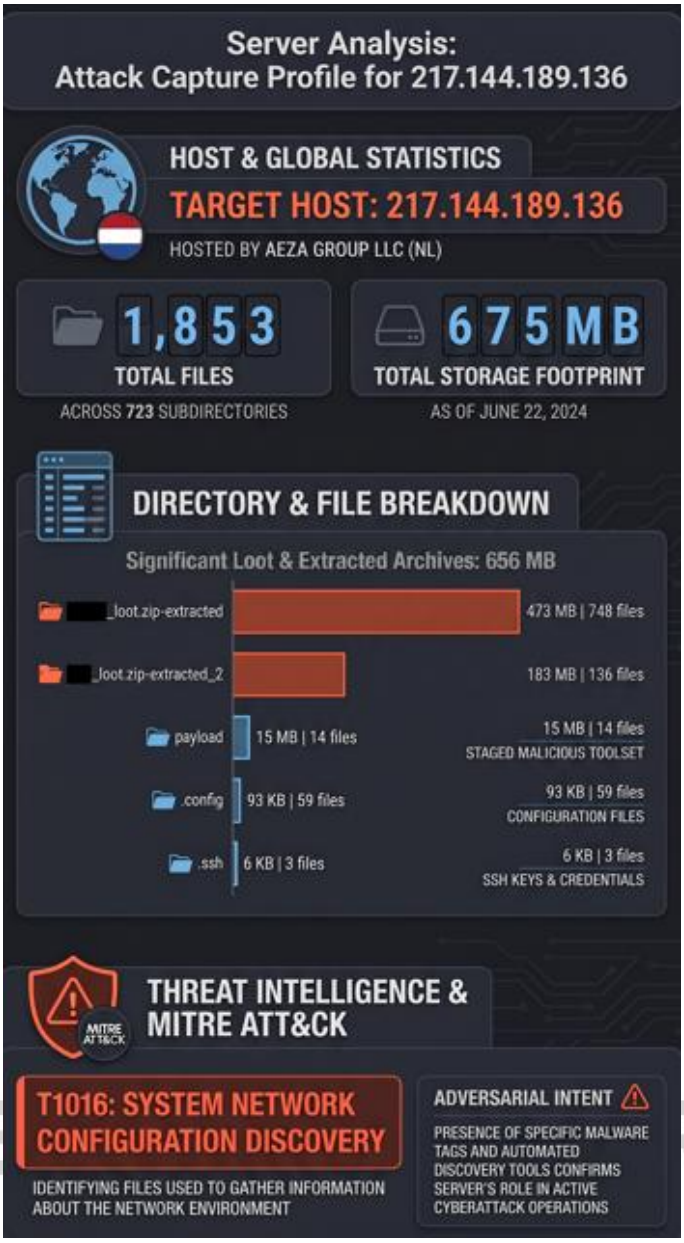


Figure: Exposed Operational Infrastructure Used by INC Ransomware Affiliates (Source: cyberandramen.net)



Active Directory Reconnaissance

The exposed infrastructure contained extensive Active Directory reconnaissance information, including:

- Domain enumeration
- Computer inventories
- Organizational Units (OUs)
- Group Policy Objects (GPOs)
- Administrator Kerberos credential caches
- Password cracking artifacts

The presence of Kerberos credential cache files indicates preparations for Pass-the-Ticket attacks and credential abuse within compromised enterprise environments.

Credential Theft and DPAPI Abuse

Analysis identified Active Directory Data Protection API (DPAPI) backup master keys among the recovered data.

Compromise of these backup keys enables attackers to decrypt domain-protected credentials offline, significantly increasing the likelihood of full Active Directory compromise.

Recovered tooling also included:

- Administrator NTLM hashes
- Chrome credential harvesting
- Executive desktop collection
- HR database targeting
- ERP backup collection

Persistence Mechanisms

The attackers maintained long-term access through OpenVPN-based remote connectivity.

Recovered artifacts included:

- OpenVPN configuration files
- Persistent routing scripts
- Session tokens
- Session resume files

These mechanisms allow attackers to maintain authenticated access while bypassing standard authentication workflows.

vpn_route.sh

```
#!/bin/bash
# [redacted] - NEVER touch default route
case "$reason" in
  connect)
    ip link set dev "$TUNDEV" up
    ip addr add "$INTERNAL_IP4_ADDRESS/32" dev "$TUNDEV"
    ip route add [redacted]/16 dev "$TUNDEV"
    ip route add [redacted]/24 dev "$TUNDEV"
    ;;
  disconnect)
    ip route del [redacted]/16 dev "$TUNDEV" 2>/dev/null
    ip route del [redacted]/24 dev "$TUNDEV" 2>/dev/null
    ip link set dev "$TUNDEV" down
    ;;
esac
```

Figure: Persistent Remote Access Infrastructure Utilizing VPN Routing (Source: cyberandramen.net)

Cross-Platform Ransomware Payloads

One of the most significant findings was the discovery of ransomware payloads compiled for multiple processor architectures.

Recovered payloads supported:

- Windows
- Linux
- VMware ESXi
- IBM Z (s390x)
- IBM PowerPC
- SPARC64
- RISC-V

All Linux variants shared common build characteristics and implemented Curve25519 and Salsa20 encryption. The availability of these payloads indicates a strategic shift toward compromising enterprise and mission-critical infrastructure beyond traditional desktop environments.

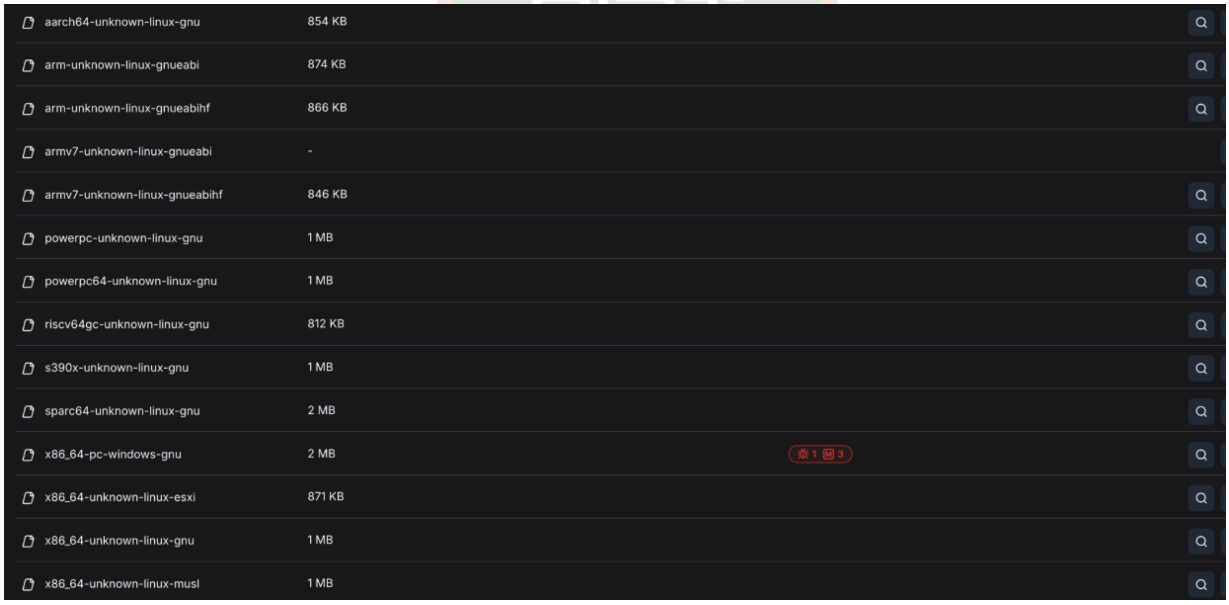


Figure: Cross-Compiled Ransomware Payloads Supporting Multiple Enterprise Architectures (Source: cyberandramen.net)

Python-Rust Hybrid Tool Development

Analysis of the recovered development environment identified the presence of the Rust PyO3 framework. PyO3 enables interoperability between Rust and Python, allowing developers to combine the performance advantages of Rust with Python-based tooling.

Although no final hybrid payload was recovered, its presence suggests ongoing development of advanced offensive tooling capable of integrating Python automation with Rust-based malware.

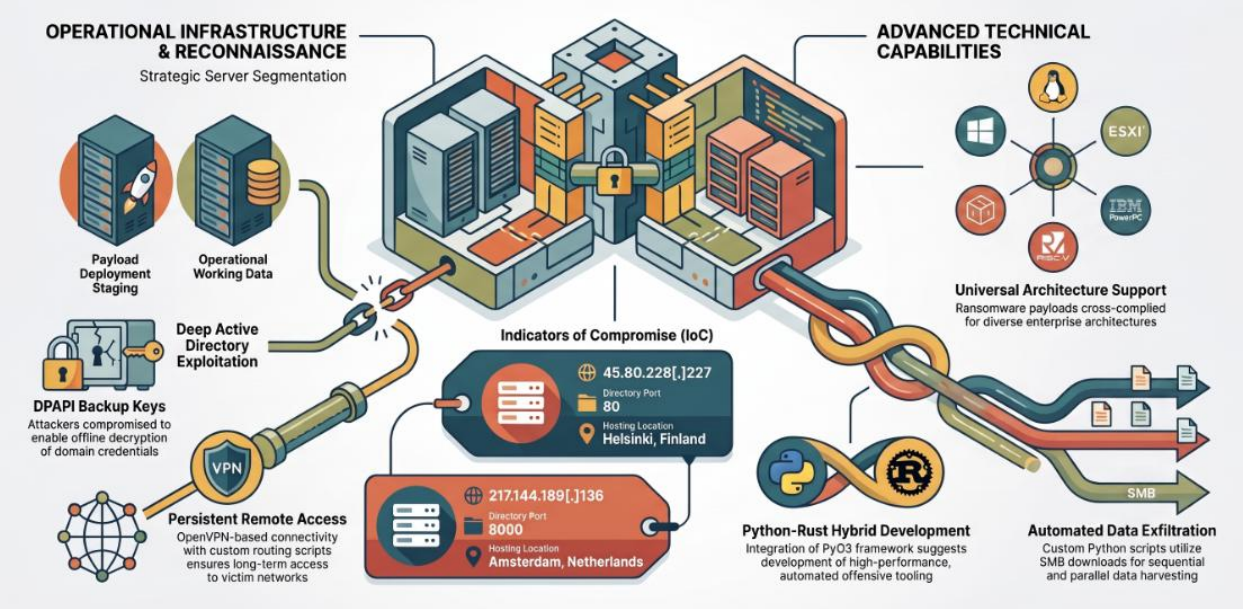


Figure: Overview of the Exposed Operational Infrastructure, Reconnaissance Artifacts, and Cross-Platform Capabilities Associated with the INC Ransomware Campaign

Potential Impact

Successful exploitation may result in:

- Full Active Directory compromise
- Credential theft
- Privilege escalation
- Enterprise-wide ransomware deployment
- Data exfiltration
- Encryption of Linux and Windows servers
- VMware ESXi encryption
- Mainframe disruption
- Operational downtime
- Financial losses.

Indicators of Compromise (IoC)

Indicator	Type	Directory Port	Hosting Location
45.80.228[.]227	IPv4	80	Aeza, Helsinki, Finland
217.144.189[.]136	IPv4	8080	Aeza Group, Amsterdam, North Holland, Netherlands

MITRE ATT&CK Mapping

Tactic	Technique	ID
Initial Access	Valid Accounts	T1078
Discovery	Account Discovery	T1087
Discovery	Network Service Scanning	T1046
Credential Access	OS Credential Dumping	T1003
Credential Access	DPAPI	T1555
Credential Access	Pass-the-Ticket	T1550.003
Lateral Movement	Remote Services	T1021
Persistence	External Remote Services (OpenVPN)	T1133
Collection	Data from Local System	T1005
Collection	Archive Collected Data	T1560
Exfiltration	Exfiltration Over C2 Channel	T1041
Impact	Data Encrypted for Impact	T1486

Recommended Immediate Actions

BGD e-GOV CIRT recommends that organizations immediately implement the following security measures:

Network Security

- Segment critical infrastructure from corporate networks.
- Restrict lateral movement using network segmentation.
- Block unauthorized remote administration protocols.

Active Directory

- Secure Domain Controllers.
- Monitor Active Directory enumeration activities.
- Protect DPAPI backup master keys.
- Review privileged account access regularly.

Endpoint Protection

- Deploy Endpoint Detection and Response (EDR) across Windows, Linux, and ESXi systems.
- Monitor PowerShell, Python, and administrative scripting activity.
- Detect ransomware execution behaviors.

Remote Access

- Enforce Multi-Factor Authentication (MFA) for VPN and remote access.
- Review OpenVPN configurations.
- Remove inactive remote access accounts.

Backup Strategy

- Maintain immutable offline backups.
- Regularly validate restoration procedures.
- Protect backup repositories from direct network access.

Monitoring

- Integrate updated threat intelligence into SIEM platforms.
- Monitor for abnormal Kerberos authentication activity.
- Review privileged account logins.
- Detect unauthorized Group Policy modifications.

The observed INC ransomware campaign demonstrates a significant evolution in ransomware operations through support for diverse enterprise computing architectures, advanced credential theft techniques, and sophisticated persistence mechanisms. Organizations operating hybrid enterprise environments, virtualization platforms, or legacy infrastructure should proactively strengthen security controls, monitor for indicators of compromise, and ensure resilient backup and incident response capabilities to mitigate the risk of ransomware attacks.

References:

- https://cyberandramen.net/2026/06/24/inc-ransomware-targets-mainframes-exposed-servers-reveal-cross-platform-payloads-and-apac-campaign/
- Cyble Threat Advisory