Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Yurei Ransomware Haunts the Digital World Like a Restless Spirit

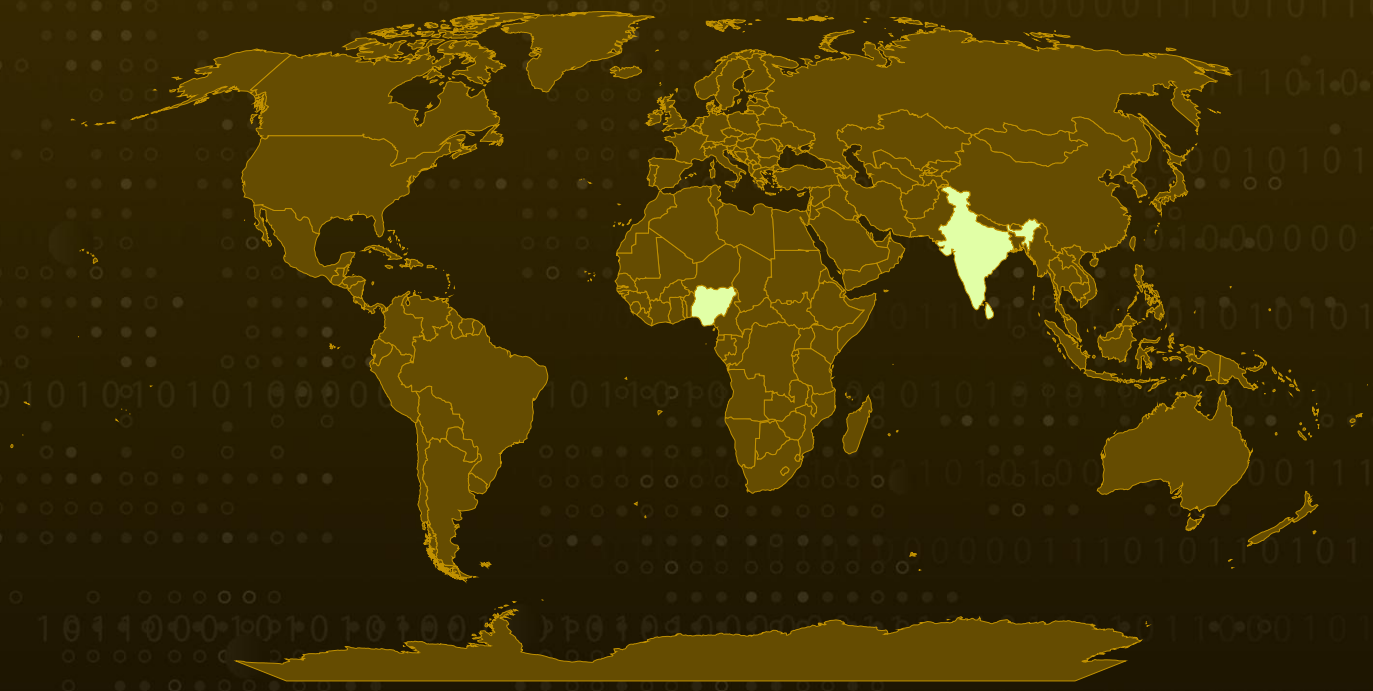
Date of Publication	Admiralty Code	TA Number
September 17, 2025	A1	TA2025285

Summary

First Observed: September 5, 2025
Malware: Yurei Ransomware
Targeted Countries: Sri Lanka, Nigeria, India
Targeted Industries: Food Service, Manufacturing

Attack: Yurei ransomware, first spotted on September 5, 2025, is a Go-based malware speculated to be linked to Moroccan threat actors, targeting companies in Sri Lanka, Nigeria, and India. Derived from the open-source Prince ransomware, it encrypts files using the ChaCha20 algorithm and spreads across network drives.

Attack Regions



Attack Details

#1 Yurei ransomware was first detected on September 5, 2025. The cybercriminal group behind the attack is suspected to be based in Morocco. The name 'Yurei' originates from Japanese folklore. The ransomware's darknet page initially disclosed a single victim a food manufacturing company in Sri Lanka. By September 9, 2025, two additional victims had been identified, one from Nigeria and another from India.

#2 The malware is written in the Go programming language and is derived from the open-source Prince ransomware, incorporating only minor alterations. This codebase has also been used in other campaigns, including those linked to CrazyHunter. Yurei encrypts files using the ChaCha20 algorithm, appending the .Yurei extension to affected files.

#3 Once encryption is complete, the ransomware initiates a secondary process that continuously searches for new network drives to include in its encryption scope, thereby expanding its attack surface. Victims find a ransom note named _README_Yurei.txt, which instructs them to visit a dedicated site and use an access token to enter a chat for negotiation.

#4 A notable weakness in Yurei's design is its failure to delete existing Shadow Copies. These are backup snapshots created by Windows Volume Shadow Copy Service (VSS), which allow users to restore files or entire volumes if enabled. Unlike many ransomware variants that remove these backups to prevent recovery, Yurei leaves them intact.

#5 As a result, victims with enabled VSS can potentially recover files without complying with the attackers demands. This oversight highlights the ransomware's limited sophistication. Given this vulnerability, it is strongly recommended to enable and regularly create system snapshots via VSS as a defense mechanism. However, while this approach can aid in restoring files, it does not protect against evolving ransomware tactics, particularly data-theft-based extortion methods that are increasingly being adopted by malicious actors.

Recommendations

Strengthen Backup Strategies with Volume Shadow Copies: Enable the Volume Shadow Copy Service (VSS) and configure automated snapshots of critical files and system states. Regularly test backup recovery to ensure that data can be restored without negotiating with threat actors. Implement offsite and immutable backups to safeguard against ransomware that targets local files.

Prepare for Data-Theft Based Extortion: Even if backups allow file restoration, be aware that attackers may exfiltrate sensitive data for further extortion. Encrypt sensitive data at rest and in transit and monitor data egress points to prevent unauthorized downloads.

Implement Network Segmentation and Zero Trust Architecture: Segment networks to limit ransomware spread across interconnected systems. Apply zero trust principles verify identity and device posture before granting access, regardless of location. Use micro-segmentation tools to define fine-grained access rules.

Regularly Review and Harden File System Permissions: Audit permissions for sensitive directories and ensure that only essential processes and users have write access. Disable file sharing where not required and use access control lists (ACLs) to limit exposure.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1005 Data from Local System	T1489 Service Stop
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1543 Create or Modify System Process	T1068 Exploitation for Privilege Escalation

T1562 Impair Defenses	**T1083** File and Directory Discovery	**T1021** Remote Services	**T1135** Network Share Discovery
T1486 Data Encrypted for Impact	**T1490** Inhibit System Recovery	**T1071** Application Layer Protocol	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	49c720758b8a87e42829ffb38a0d7fe2a8c36dc3007abfabbea76155185d2902, 4f88d3977a24fb160fc3ba69821287a197ae9b04493d705dc2fe939442ba6461, 1ea37e077e6b2463b8440065d5110377e2b4b4283ce9849ac5efad6d664a8e9e, 10700ee5caad40e74809921e11b7e3f2330521266c822ca4d21e14b22ef08e1d, 89a54d3a38d2364784368a40ab228403f1f1c1926892fe8355aa29d00eb36819, f5e122b60390bdcc1a17a24cce0cbca68475ad5abee6b211b5be2dea966c2634, 0303f89829763e734b1f9d4f46671e59bfaa1be5d8ec84d35a203efbfcb9bb15, afa927ca549aaba66867f21fc4a5d653884c349f8736ecc5be3620577cf9981f, d2539173bdc81503bf1b842a21d9599948e957cadc76a283a52f5849323d8e04, 754865527bc33305d8dc89a88ffada71fa0180fe778e2106d5faa8e7a8801220, 84d68ba901462bb0918a852a01df885f986661954c14d9c4e8e40338df2a1cb8, 53397d36cab0a32695a50d179f289fa61fc946591bd97355ee98d350f7652079
TOR Address	fewcriet5rhoy66k6c4cyvb2pqrblxtx4mekj3s5l4jjt4t4kn4vheyd[.]onion
Filename	_README_Yurei.txt

Recent Breaches

https://www.midcity.lk
https://www.thepromisenig.com
https://noblecorp.net

References

https://research.checkpoint.com/2025/yurei-the-ghost-of-open-source-ransomware/

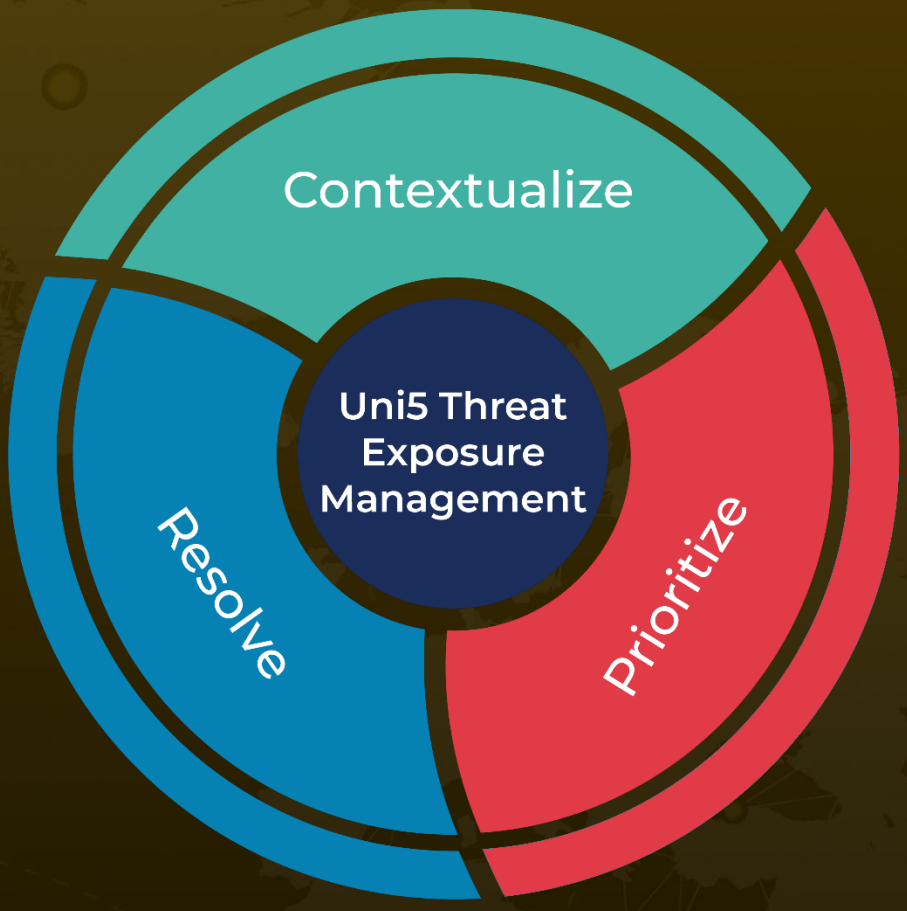
https://github.com/oakkaya/Prince-Ransomware

https://hivepro.com/threat-advisory/go-based-crazyhunter-ransomware-strikes-taiwan/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 17, 2025 . 9:30 PM

More at www.hivepro.com