PRIMUS PARTNERS®

Quote by Devroop Dhar, Co-founder & CEO, Primus Partners

Published in CSO
September 15, 2025

New ransomware Yurei adopts open-source tools for double-extortion campaigns News

The new group relies on data theft and encryption, but coding errors in its ransom note routine expose weaknesses that defenders can exploit.

Read on: https://www.csoonline.com/article/4057067/new-ransomware-yurei-adopts-open-source-tools-for-double-extortion-campaigns.html

Article Content- A new ransomware group called Yurei has surfaced, adopting a double-extortion model. The group encrypts the victim's files, exfiltrates sensitive data, and demands a ransomware payment for decryption and refraining from publishing stolen data.

First identified on September 5 by Check Point Research, this ransomware group has already attacked three enterprises, a Sri Lankan-based Midcity Marketing food manufacturing company, and an enterprise each in India and Nigeria.

Check Point Research has indicated that the threat actor's origins may be in Morocco.

When attacking an enterprise, the Yurei ransomware enumerates all drives, and for each drive in parallel, it encrypts files to add a .Yurei extension, the security firms said. For encryption, Yurei uses the ChaCha20 algorithm to generate a random key, a random nonce per file, and then encrypts both with ECIES using the attacker's public key.

It then attempts to set a wallpaper. But as Yurei's developer forgot to provide the URL for the wallpaper, it only displays a plain, solid color background (like black) instead of showing a

ransom note. Once the encryption is complete, the malware enters a new routine that continuously monitors for newly attached network drives to then encrypt. Yurei then provides the victim with a .onion page for further communication and price negotiations, Check Point Research said in a report.

Open-source code fuels fast entry

Yurei is built almost entirely on open-source ransomware code known as Prince-Ransomware, written in Go but with a few modifications. The same was identified as the threat actor did not strip symbols from the binary, resulting in function and module names being preserved. This same ransomware codebase was already used in campaigns by other actors as well, such as CrazyHunter, identified by Check Point Research.

This only goes to show how easily and quickly threat actors can use open-source ransomware projects to enter the ransomware business without the necessary development skills or even investing much effort.

Open-source ransomware code lowers the barrier for new groups as it removes R&D from the equation. “Turnkey codebases, build scripts, and working ransom workflows let low-skill actors ship variants in days, not months. Minimal edits (branding, concurrency tweaks, C2 endpoints) create new groups that can immediately monetize data theft, shifting the competitive edge from engineering to targeting, social pressure, and negotiation playbooks,” said Amit Jaju, senior managing director – India at Ankura Consulting.

According to Devroop Dhar, co-founder and MD at Primus Partners, instead of needing a big development team, a small group can just make a few edits and go live. It is cheap, quick, and even a rough version can still make money as long as the data theft and leak threat work.

Bigger risks beyond downtime

The double-extortion ransomware appears to be an early version, as it has loopholes. Ransomware often targets and deletes shadow copies to block victims from using Windows’ built-in recovery options. But Yurei did not delete the shadow copies, which, if enabled, can allow the victim to restore their files to a previous snapshot without having to negotiate with Yurei.

However, when data is stolen, only backups do not solve the problem. “Even when a company restores its systems, the attackers still may threaten to publish what they stole. That brings in newer risks, like regulatory fines, lawsuits, reputational damage, and exposure of intellectual property. It is a bigger issue than just downtime because it stays for long after systems come back online,” Dhar said.

Defensive gaps don’t last long

Flaws like these usually do not last long. Threat actors can easily fix the gaps in the next version, and CISOs should be mindful of the fact that the next version will fix those gaps.

“Enterprises should cut initial access by hardening internet-facing services, enforce phishing-resistant multi-factor authentication everywhere, and block legacy authentication,” Jaju said. “Enterprises must deploy data loss prevention with egress controls, fine-tune UEBA (User and Entity Behavior Analytics) for bulk file access, and monitor cloud storage and MFTs (managed file transfers). To contain attacks,

organizations should segment Active Directory and critical data zones, enforce just-in-time administration and privileged access management (PAM), and prepare incident communication and legal workflows.

Jaju added enterprises should plan for resilience with intelligence with immutable backups plus threat hunting for open-source indicators (Prince/Yurei build artifacts, PowerShell patterns, ChaCha20/ECIES markers) and subscribe to rapid intel on copycat forks. They should also cover supplier risk by mandating MFA, EDR, and logging for third parties with network or data access and pre-bake kill-switch controls in contracts.