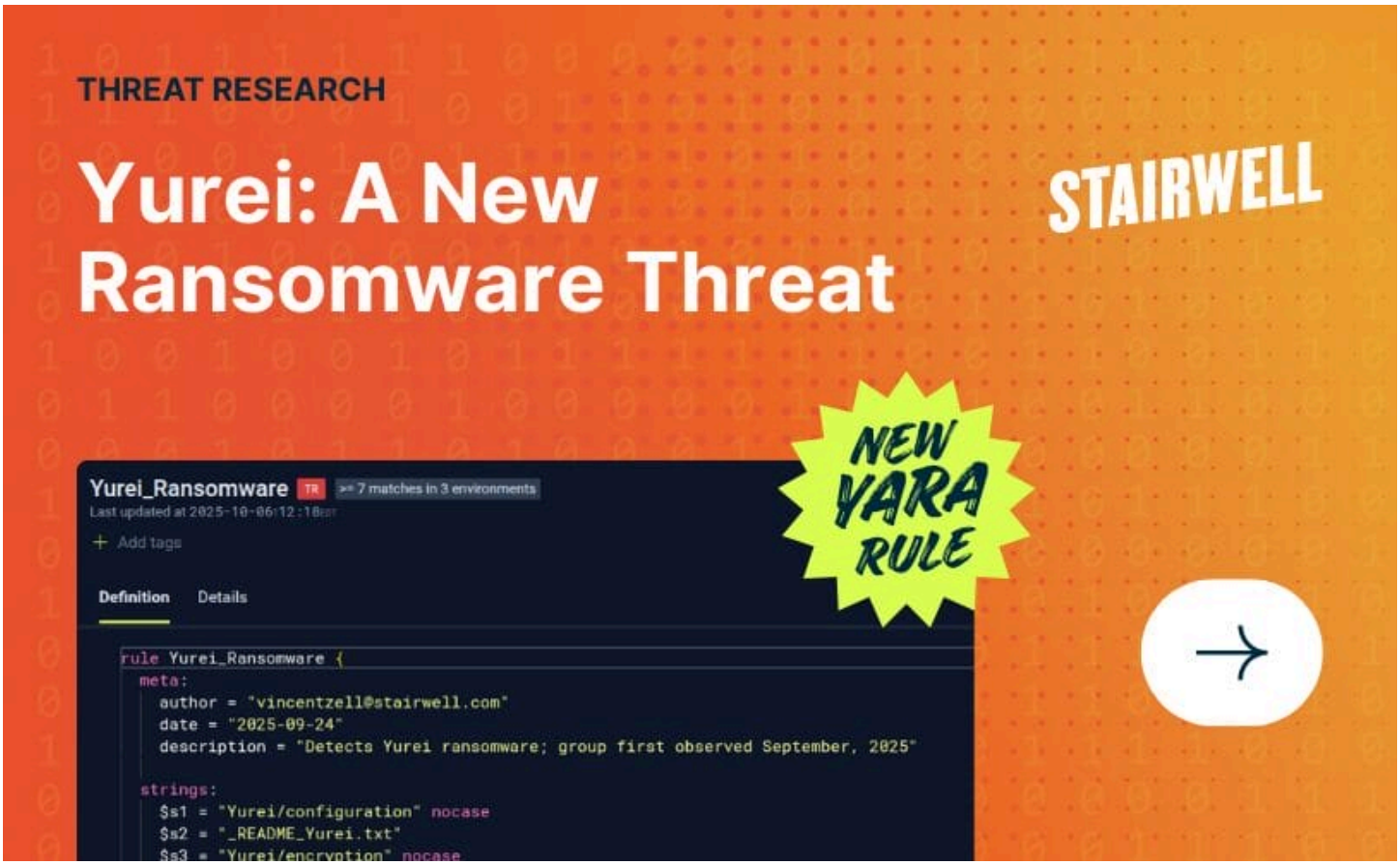
stairwell.com /resources/yurei-a-new-ransomware-threat/

Yurei: A New Ransomware Threat



Research

Written by **Vincent Zell**Threat Researcher

October 9, 2025

Yurei is a newly discovered ransomware group first observed by Check Point Research on September 5th, 2025, and has quickly made its presence known.

Named after spirits in Japanese folklore, Yurei is a group that leverages a double-extortion model, blending encryption with data theft and public exposure. Though Yurei's name initially may hint at originating from East Asia, research alludes to potential Moroccan origins based on early submissions to VirusTotal.

Early victims of this ransomware include a food manufacturing company in Sri Lanka, as well as other entities in India and Nigeria.

Technical weaknesses of Yurei

Yurei ransomware leverages the Go programming language, which offers malware authors cross-platform compilation abilities, ease of development, and the advantage of creating detection challenges for many antivirus tools. However, analysis revealed that the Yurei developers made a rookie mistake: they failed to strip debugging symbols from their binaries, exposing that their malware is essentially a slightly modified version of the open-source Prince-Ransomware framework. This has been used by threat groups in the past.

Yurei provides a ransom note named **_README_Yurei.txt**, and directs victims to a **.onion** site for negotiation using a provided access token; the attackers promise decryption tools and vulnerability reports upon payment, while victims can negotiate pricing for data recovery, file deletion, and promises of non-publication. The malware also includes enumeration, encryption in parallel, and monitoring for newly attached network shares to extend encryption.

Yurei also, however, contains a major weakness: it doesn't delete Windows Shadow copies – these are automatic backup snapshots that most ransomware seeks to target. This means, if available, victims can simply restore their files from these backups and avoid paying the ransom, further indicating a gap in the attacker's skills. Defenders can easily mitigate this by ensuring that Volume Shadow Copy Service (or other backup solution) is enabled and tested regularly.

Though not technically sophisticated, Yurei's speed of deployment and open-source code show how simple it has become for threat actors to get started; which is exactly what can make these threats dangerous and unpredictable.

YARA rule for Yurei detection

YARA rules are one of the most powerful tools for defenders when it comes to surfacing threats. At Stairwell, we make this power easily accessible; from our in-house YARA editor, to our extensive YARA library, built to accelerate response efforts.

Due to the quick spread of the malware and its threat of data leakage, the Stairwell Threat Research team has developed a YARA rule to detect Yurei samples:

```
rule Yurei_Ransomware {
  meta:
    author = "vincentzell@stairwell.com"
    date = "2025-09-24"
    description = "Detects Yurei ransomware; group first observed September,
2025"

  strings:
    $s1 = "Yurei/configuration" nocase
    $s2 = "_README_Yurei.txt"
    $s3 = "Yurei/encryption" nocase
```

```
  condition:
    filesize < 20MB and
    3 of them
}
```

This YARA rule flags binaries containing strings unique to observed Yurei samples, as well as their typical filename for a ransom note.

How AI Triage can expedite response

Beyond YARA rules, Stairwell offers other capabilities to assist defenders in analyzing threats. Stairwell AI Triage quickly analyzes your files for you. This capability is an actionable tool with real answers, powered by real data at scale. Using AI Triage, we're immediately able to reliably identify Yurei samples and gather valuable intelligence:

Sha256: **49c720758b8a87e42829ffb38a0d7fe2a8c36dc3007abfabbea76155185d2902**
AI Triage Output:

```
TL;DR: This file is a highly malicious "Yurei" ransomware variant designed to encrypt files on
local drives and network shares, exfiltrate critical corporate data prior to encryption, and
demand a ransom for decryption. It explicitly threatens public disclosure of stolen data and
deletion of decryption keys if terms are violated or third-party recovery is attempted. The
ransomware communicates via a Tor-based blog and chat for ransom payment and instructions.
MALICIOUS LIKELIHOOD: 100%
CONFIDENCE: 100%
THREAT TYPE: Ransomware
ACTOR: Cybercrime syndicate
```

Sha256: **89a54d3a38d2364784368a40ab228403f1f1c1926892fe8355aa29d00eb36819**

AI Triage Output:

```
TL;DR: This file is a highly malicious Windows ransomware variant, likely named "Yurei,"
designed to encrypt user and corporate data, exfiltrate sensitive information, and demand a
ransom payment. It communicates with its command-and-control (C2) infrastructure via the TOR
network and modifies the victim's desktop wallpaper with a ransom note. The file explicitly
warns against system shutdown, antivirus use, or third-party recovery, threatening data
deletion and public disclosure if terms are violated or negotiations are prolonged.
MALICIOUS LIKELIHOOD: 100%
CONFIDENCE: 100%
THREAT TYPE: Ransomware
ACTOR: Yurei Ransomware Group
```

No questions, no wasted time – just answers delivered instantly.

Conclusion

Yurei may not be the most advanced or sophisticated ransomware we've seen, but it's a fantastic example of how open-source malware…even with some flaws…can allow new and inexperienced actors to do some real damage. For defenders, the upside is that many of its weak points are observable and potentially mitigable, and the key is readiness. Stay ahead with YARA rules, monitoring suspicious activity and artifacts, and lean on Stairwell.

Indicators of compromise

Below are observed Yurei ransomware samples:

754865527bc33305d8dc89a88ffada71fa0180fe778e2106d5faa8e7a8801220

53397d36cab0a32695a50d179f289fa61fc946591bd97355ee98d350f7652079

c88b1ceb27808f3228b3bdaee819b1d4806ca4262ec9dde84160b08c7733c4c5

89a54d3a38d2364784368a40ab228403f1f1c1926892fe8355aa29d00eb36819

49c720758b8a87e42829ffb38a0d7fe2a8c36dc3007abfabbea76155185d2902

More resources

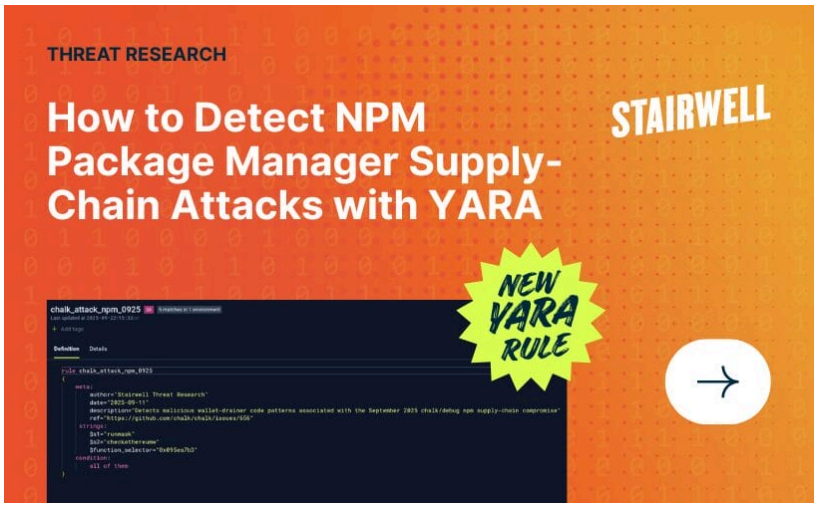
Building on CISA's Salt Typhoon YARA Rules: Stairwell finds 637 New Variants

Research

Building on CISA's Salt Typhoon YARA Rules: Stairwell finds 637 New Variants

Stairwell expands CISA's Salt Typhoon YARA rules, uncovering 637 new malware variants.

How to Detect NPM Package Manager Supply-Chain Attacks with YARA



Research

How to Detect NPM Package Manager Supply-Chain Attacks with YARA

New npm supply-chain YARA rules out—chalk/debug + Shai-Hulud worm. Retrohunt now!

The Hidden Malware Report: Uncovering Malware Variants in the Wild

The Hidden Malware Report: Uncovering Malware Variants in the Wild

The Hidden Malware Report: Uncovering Malware Variants in the Wild