Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ⚔ ATTACK REPORT

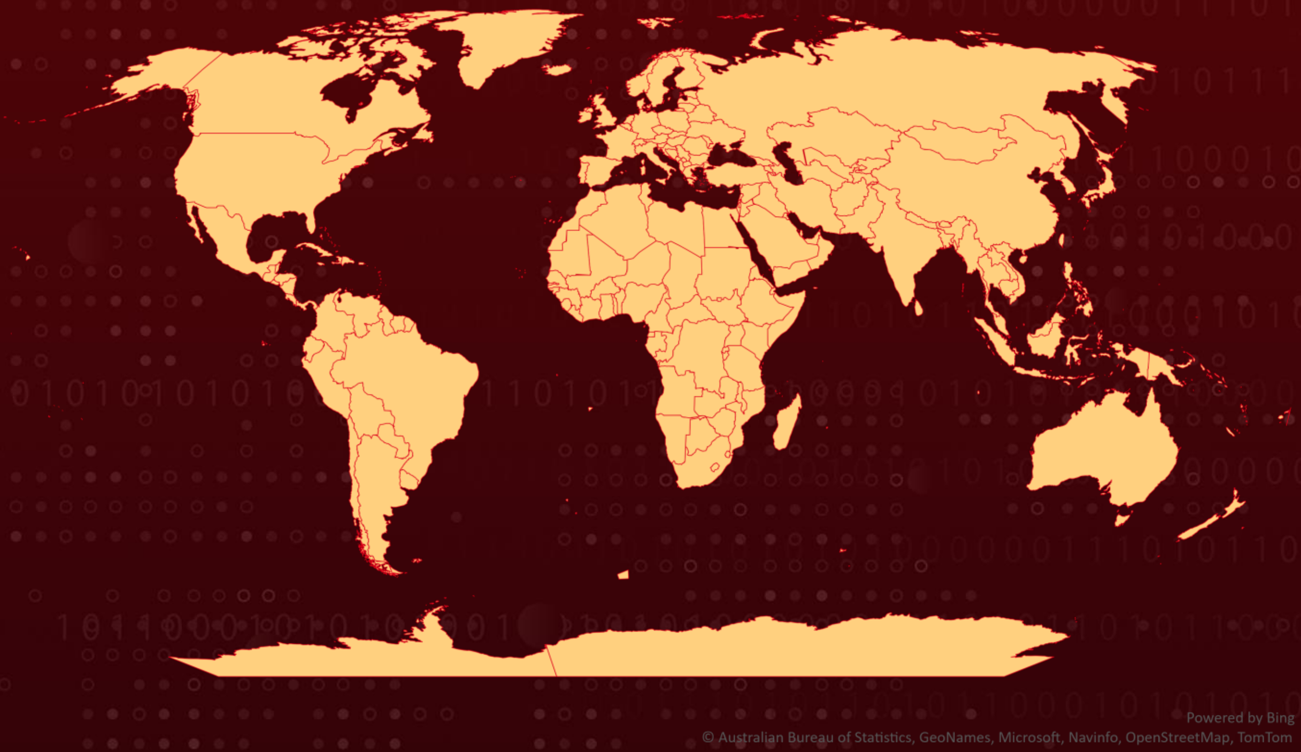
# New Yashma Ransomware Variant Mimics WannaCry in New Attack

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| August 8, 2023 | A1 | TA2023325 |

# Summary

**First Appearance:** June 4, 2023
**Attack Region:** Worldwide
**Affected Platform:** Windows
**Malware:** Yashma ransomware, WannaCry ransomware
**Attack:** A Vietnamese-origin threat actor employs a Yashma ransomware variant since June 2023, using unique GitHub-based ransom note delivery and mimicking WannaCry. This operation demonstrates the accelerated diversification of ransomware attacks due to leaked source code and builders.

## Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

# Attack Details

#1

An unidentified threat actor with likely Vietnamese origin has been using a variant of the Yashma ransomware to target entities in English-speaking countries, Bulgaria, China, and Vietnam since at least June 4, 2023. The threat actor deploys an unusual technique to deliver ransom notes: instead of embedding the ransom note strings directly into the ransomware binary, they download the ransom note from their GitHub repository by executing a batch file.

#2

Yashma ransomware, initially discovered in May 2022 and is a modified version of Chaos ransomware. The ransom note used in this campaign resembles the well-known WannaCry ransomware note, possibly as an attempt to confuse attribution. The note provides a Bitcoin wallet address for ransom payments but doesn't specify the amount.

#3

The threat actor's GitHub account name and email contact suggest Vietnamese origin, and the ransom note indicates a sensitivity towards victims in Vietnam. The campaign likely started around June 4, 2023, when the actor created a GitHub repository containing ransom note text files in multiple languages.

#4

The Yashma variant ransomware sets a wallpaper on victims' machines, similar to the WannaCry ransomware. The actor's modifications to Yashma ransomware include executing an embedded batch file for ransom note delivery, establishing persistence using a ".url" bookmark file, and maintaining Yashma's anti-recovery capability, which hinders file recovery by wiping and deleting original unencrypted files.

# Recommendations

**Keep your systems and software up to date:** Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

**Conduct Regular Data Backups:** Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

**Protect your Backups:** Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0003<br>Persistence | TA0040<br>Impact | TA0002<br>Execution |
| TA0005<br>Defense Evasion | T1485<br>Data Destruction | T1490<br>Inhibit System Recovery | T1486<br>Data Encrypted for Impact |
| T1027.009<br>Embedded Payloads | T1027<br>Obfuscated Files or Information | T1036<br>Masquerading | T1547.001<br>Registry Run Keys / Startup Folder |
| T1547<br>Boot or Logon Autostart Execution | T1547.009<br>Shortcut Modification | | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA1 | 367411a1e2efde7eb9d39de66be90a96012d5d7b |
| SHA256 | 3ea6df18492d21811421659c4cf9b88e64c316f2bef8a19766b0c79012476cac,<br>de68f4bce05a856ad949e6fb1738559fc506d491d4f6227553695aa9558b64eb |
| Hostname | www.fxxz[.]com |

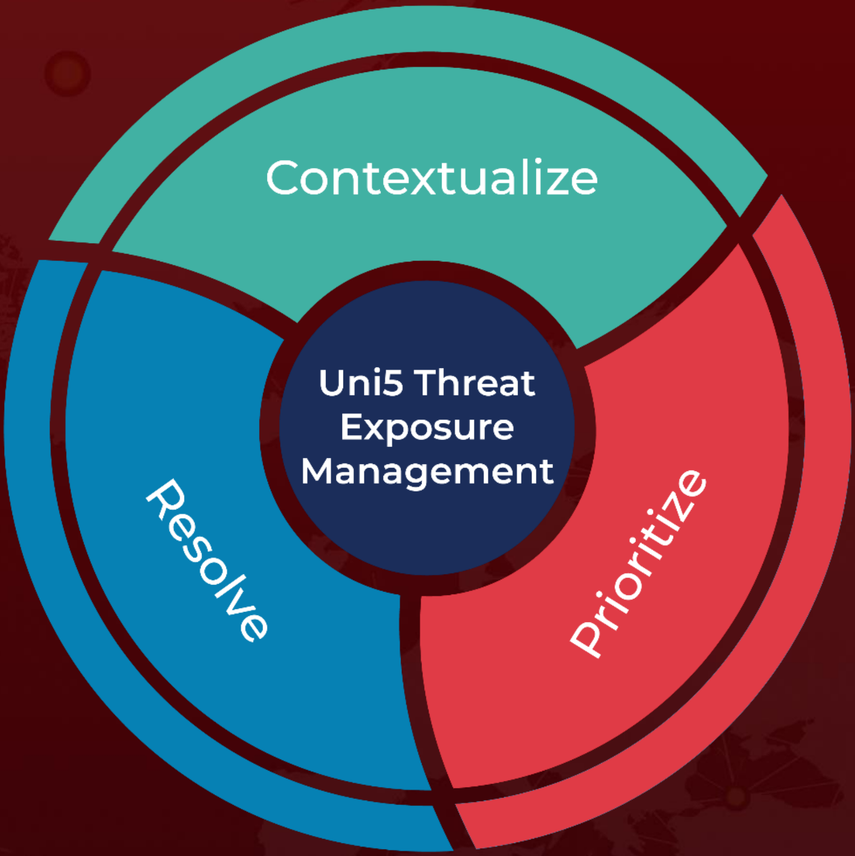
## References

https://blog.talosintelligence.com/new-threat-actor-using-yashma-ransomware/

# 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

**August 8, 2023 • 11:30 PM**

More at www.hivepro.com