# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Maui Ransomware and DTrack linked to Andariel group

**Tracker ID:** TN0822 **Date:** 18/Aug/22 **Category:** Threat Actor **Industry:** All **Region**: Asia, Russia

### Background

Recent research has linked the Maui and DTrack ransomware campaigns to the North Korean state-sponsored threat group "Andariel," which is well-known for using illegal online operations to make a profit and sow chaos in South Korea. Since at least 2015, the group has targeted state, federal, and military organizations, as well as financial service providers. The details revealed validate a previous Maui attack on a Japanese housing company, along with subsequent, unattributed strikes in Vietnam, Russia, and India.

Andariel specializes in launching targeted attacks on prey that may contain information that can help strategically vital industries such as energy, aerospace, and military hardware. Andariel has been linked to cyberattacks for espionage, data theft, data wiping, and operations to generate revenue for the North Korean government (aka Stonefly). It was one of the cyber organizations supported by the DPRK, about which the US State Department announced last month information prizes of up to $10 million.

Maui is notable for being designed to be conducted manually by a remote actor via a command-line interface and for not including a ransom note with instructions for restoring access. It began performing attacks in April 2021, according to build timestamps, with a clear bias toward American healthcare organizations. The FBI and CISA had previously issued alerts on the Maui ransomware, exchanging indicators of compromise that identified North Korean threat actors. US criminal enforcement agencies continued to pursue Maui, and they have also recovered $500,000 in ransom payments made by hospitals to the ransomware gang.

The group infiltrated the target with a variant of the well-known DTrack malware, which was preceded by 3proxy months before. This was completed around ten hours before Maui was introduced to the primary target system. DTrack, also known as Valefor and Preft, is a remote access trojan used by the Stonefly organization to exfiltrate sensitive data. The Japanese victim had only been infected with the DTrack malware for a few hours before encryption, but later log analysis revealed that the "3Proxy" program had been active on the company's network for months. DTrack (formerly known as Preft) is a modular piece of malware that specializes in data theft and HTTP exfiltration using Windows commands. In earlier Andariel campaigns, a free open-source proxy server tool called 3Proxy was seen.

The malware employed against the Japanese company used the identical shellcode identified in a Symantec research from 2021 that looked into an Andariel campaign. The DTrack variant utilized in the assaults on Japanese, Russian, Indian, and Vietnamese organizations shares 84% of its code with samples directly linked to earlier Andariel activities. Furthermore, the early network compromise tactics used in these operations display familiar Andariel characteristics, such as exploiting vulnerable Weblogic servers (CVE-2017-10271). As of mid-2019, similar observations have been made in exploits and compromising techniques leveraging Andariel.

The state-sponsored ransomware campaign is consistent with the broader strategic objectives of North Korean hackers, who are known for directing attacks with monetary incentives. However, there appears to be a link between the APT and the ransomware operation, which could aid in early detection and prevention.

# KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Maui Ransomware and DTrack linked to Andariel group

**Tracker ID:** TN0822 **Date:** 18/Aug/22 **Category:** Threat Actor **Industry:** All **Region**: Asia, Russia

The state-sponsored ransomware campaign is consistent with the broader strategic objectives of North Korean hackers, who are known for directing attacks with monetary incentives. However, there appears to be a link between the APT and the ransomware operation, which could aid in early detection and prevention.

## MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Lateral Movement and Exfiltration.

## Indicators of Compromise *

Please refer to the attached sheet for IOCs.

## Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Refrain from opening untrusted links and email attachments without verifying their authenticity. Educate employees on how to protect themselves from the ongoing phishing campaigns and techniques.
- Protect employee accounts by configuring multi-factor authentication.
- Implement network segmentation to limit or block lateral movement. Follow multilayered defense solutions and active monitoring to detect and thwart threats.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.

## References


- Bill Toulas, Maui ransomware operation linked to North Korean 'Andariel' hackers, defense orgs, Bleeping Computer, 09th August 2022, External Link (bleepingcomputer.com).
- Ravie Lakshmanan, Experts Uncover Details on Maui Ransomware Attack by North Korean Hackers, Hacker News, 10th August 2022, External Link (thehackernews.com)
- KURT BAUMGARTNER, SEONGSU PARK, Andariel deploys DTrack and Maui ransomware, Security List, 09th August 2022, External Link (securelist.com).

# KPMG Cyber Threat Intelligence Platform

## Cyber Threat Notification | Maui Ransomware and DTrack linked to Andariel group

**Tracker ID:** TN0822 **Date:** 18/Aug/22 **Category:** Threat Actor **Industry:** All **Region**: Asia, Russia

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

*

| Hash SHA256 | Hash MD5 | URL |
|---|---|---|
| 6122c94cbfa11311bea7129ecd5aea6fae6c51d23228f7378b5f6b2398728f67 | 739812e2ae1327a94e441719b885bd19 | hxxp://145.232.235[.]222/usr/users/mini.ps1 |
| a557a0c67b5baa7cf64bd4d42103d3b2852f67acf96b4c5f14992c1289b55eaa | 2f553cba839ca4dab201d3f8154bae2a | |
| 92adc5ea29491d9245876ba0b2957393633c9998eb47b3ae1344c13a44cd59ae | 5bc4b606f4c0f8cd2e6787ae049bf5bb | |
| 60425a4d5ee04c8ae09bfe28ca33bf9e76a43f69548b2704956d0875a0f25145 | 95247511a611ba3d8581c7c6b8b1a38a | |