Hive Pro

Threat Level

Amber

HiveForce Labs

# THREAT ADVISORY

ATTACK REPORT

# Reptile Rootkit Targets Linux Systems in South Korea

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| August 9, 2023 | A1 | TA2023326 |

# Summary

**First appeared:** May 2022
**Attack Region:** South Korea
**Actor Name:** Winnti Group (aka APT 41, Blackfly, Wicked Panda), UNC3886
**Affected Platform:** Linux
**Malware:** Reptile, Mélofée
**Attack:** Reptile, an open-source Linux rootkit, goes beyond concealment, offering attackers a reverse shell and utilizing Port Knocking for control; observed in attacks including Chinese groups exploiting zero-days. Similarities to Mélofée malware suggest potential connections in attack strategies.

## Attack Regions

Winnti Group
UNC3886

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

# Attack Details

#1

Reptile, an open-source kernel module rootkit targeting Linux systems, has emerged as a multifaceted malware with advanced capabilities. Its presence on GitHub makes it widely accessible, and it transcends traditional malware by offering more than just concealment tactics. In a departure from conventional rootkits, Reptile introduces a reverse shell feature, granting attackers direct control over compromised systems.

#2

A standout feature of Reptile is its utilization of Port Knocking, a clever technique wherein the malware opens a specific port, awaiting a specific signal to establish a connection with a command-and-control server. This dynamic approach gives Reptile the ability to communicate in a discreet and controlled manner, making it difficult to detect and trace back to its source.

#3

To achieve its intricate tasks, Reptile employs kernel function hooking, allowing it to cloak files, directories, processes, and network activities. Its Port Knocking mechanism adds a layer of sophistication, enabling stealthy communication with remote servers.

#4

After its GitHub release, Reptile has been consistently utilized in cyberattacks. A Chinese threat group named UNC3886, exploited it in a zero-day attack on Fortinet products. Interestingly, Reptile shares similarities with the Mélofée malware, linking it to the Chinese Winnti attack group. This highlights Reptile's role as an enabler for attackers seeking to breach systems and maintain control over compromised environments.

# Recommendations

**Enhance System Security:** Strengthen your Linux systems' defenses by regularly applying security updates and patches. This practice mitigates vulnerabilities that malware like Reptile exploits. Employ intrusion detection and prevention systems (IDPS) to identify and block suspicious activities promptly.

**Implement Behavioral Analysis:** Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats like Reptile before they fully compromise your systems.

**Monitor Network Traffic:** Utilize network monitoring tools to scrutinize incoming and outgoing traffic, identifying potential Port Knocking attempts or irregular communication patterns. This can help detect and thwart attackers attempting to establish connections with their command-and-control servers.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0011**<br>Command and Control | **TA0003**<br>Persistence | **TA0040**<br>Impact | **TA0002**<br>Execution |
| **TA0005**<br>Defense Evasion | **T1105**<br>Ingress Tool Transfer | **T1070.004**<br>File Deletion | **T1070**<br>Indicator Removal |
| **T1014**<br>Rootkit | **T1205.001**<br>Port Knocking | **T1205**<br>Traffic Signaling | **T1059**<br>Command and Scripting Interpreter |
| **T1140**<br>Deobfuscate/Decode Files or Information | **T1027**<br>Obfuscated Files or Information | **T1095**<br>Non-Application Layer Protocol | **T1573**<br>Encrypted Channel |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | 1957e405e7326bd2c91d20da1599d18e,<br>246c5bec21c0a87657786d5d9b53fe38,<br>5b788feef374bbac8a572adaf1da3d38,<br>977bb7fa58e6dfe80f4bea1a04900276,<br>bb2a0bac5451f8acb229d17c97891eaf,<br>c3c332627e68ce7673ca6f0d273b282e,<br>cb61b3624885deed6b2181b15db86f4d,<br>d1abb8c012cc8864dcc109b5a15003ac,<br>f8247453077dd6c5c1471edd01733d7f |
| SHA1 | 0c6d838c408e88113a4580e733cdb1ca93807989,<br>2ca4787d2cfffac722264a8bdae77abd7f4a2551,<br>3cc2d6bf5215de3c24fb194c232a0411cede78e0,<br>467ea946ac857471e2f01bbdc4258a0ff31c01ce,<br>76d6cb6b6e9b40b07944153b1f140e786e3ae381,<br>783736e9274bd2bb90390bb9c23a62c387cde3ef,<br>7d9eaefeb0c95473ad86abbdcffdbdf6950b8dd2,<br>a5f6162c6b6b6f0c177771a56a6b1eb5d7b593a0,<br>ee295ec546158e425a3660a4a9402916087ccd97 |
| SHA256 | 133d3e070e30c94a591450b0930daf9f751debc0f4384fac6ace63f60a383818,<br>1425a4a89b938d5641ed438333708d1728cfed8c124451180d011f6bbb409976,<br>15e4e936b2f47eb3fa2455b7c22b2714bebe9f8c01b24bbf7cb5f9559999d292,<br>17bbebd7d8982d580cc3dea35d988ae2bfd62d708b69662419c41682274e0a14,<br>4305c04df40d3ac7966289cc0a81cedbdd4eee2f92324b26fe26f57f57265bca,<br>7ce7b914bd434f8a45db1cb3ec783237a5485b7abcee4df06275ea274e095295,<br>99ffc0099277bef59a37a4cfcf4cdd71df13ad33d1c7bf943dc87f803e75dd2c,<br>cbe9107185c8e42140dbd1294d8c20849134dd122cc64348f1bfcc90401379ec,<br>d182239d408da23306ea6b0f5f129ef401565a4d7ab4fe33506f8ac0a08d37ba |

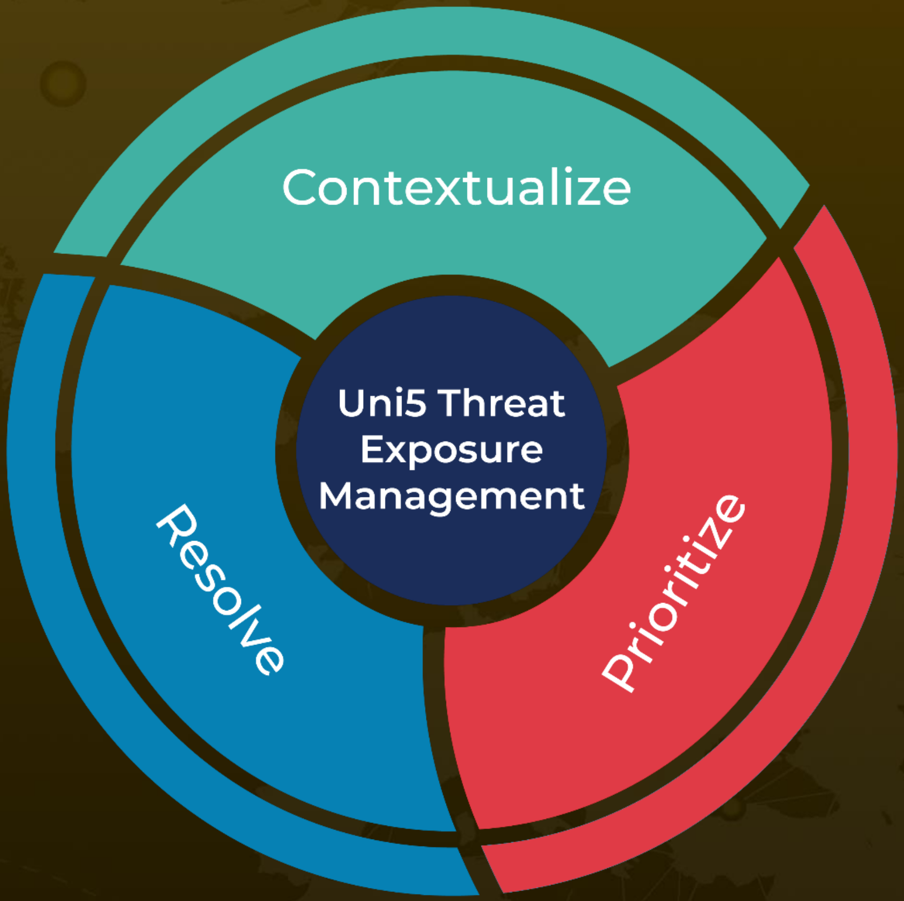
## References

https://asec.ahnlab.com/en/55785/

# 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 9, 2023 • 7:30 AM**

More at www.hivepro.com