

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## Earth Longzhi Unleashes New 'Stack Rumbling' Tactic

Date of Publication

May 4, 2023

Admiralty Code

A1

TA Number

TA2023211

# Summary

**Attack began:** 2023

**Actor:** Earth Longzhi (Subgroup of APT41)

**Malware:** Croxloader and SPHijacker

**Attack Region:** Philippines, Thailand, Taiwan, and Fiji

**Targeted Industries:** Government, healthcare, technology, and manufacturing

**Attack:** APT41's Earth Longzhi launches a new campaign targeting organizations in Asia Pacific using "stack rumbling" to disable security products and install Behinder web shell.

## 🔪 Attack Regions



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

## ⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-5713	Improper Input Validation in Malwarefox Anti-malware	Malwarefox Anti-malware 2.72.169	✗	✗	✗

# Attack Details

## #1

Earth Longzhi, a subgroup of APT41, has launched a new campaign aimed at organizations located in Taiwan, Thailand, the Philippines, and Fiji. This latest operation, which comes after a period of inactivity, utilizes a Windows Defender executable to engage in DLL sideloading and take advantage of a weak driver, zamguard64.sys, to carry out a bring-your-own-vulnerable-driver (BYOVD) attack that disables security tools on the targeted hosts.

## #2

Earth Longzhi has employed a new technique of disabling security products, which we have dubbed "stack rumbling" using Image File Execution Options (IFEO). This technique represents a new form of denial-of-service (DoS) attack. The group's latest campaign focuses on exploiting public-facing applications, Internet Information Services (IIS) servers, and Microsoft Exchange servers to deploy Behinder.

## #3

Behinder is a well-known web shell that proved to be particularly effective in this campaign due to its ability to support multiple backdoor functions. Two distinct types of malware were launched using legitimate Windows Defender binaries: a new variant of Croxloader and a tool that we refer to as "SPHijacker" that is capable of disabling security products.

# Recommendations



Organizations based in Asia Pacific should implement robust security measures to protect against APT41's Earth Longzhi's new campaign that exploits vulnerabilities in Windows Defender, IIS servers, and Microsoft Exchange servers.



Regular security assessments and updates to security protocols are crucial in mitigating the risks associated with new and emerging threats like "stack rumbling" and BYOVD attacks.



Implementing blocking Indicators of Compromise (IOCs) can also help organizations in the Asia Pacific defend against Earth Longzhi's new campaign and other similar threats.

## Potential MITRE ATT&CK TTPs

<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0005</u></b> Defense Evasion
<b><u>TA0006</u></b> Credential Access	<b><u>T1003</u></b> OS Credential Dumping	<b><u>T1003.001</u></b> LSASS Memory	<b><u>T1569</u></b> System Services
<b><u>T1569.002</u></b> Service Execution	<b><u>T1574</u></b> Hijack Execution Flow	<b><u>T1574.002</u></b> DLL Side-Loading	<b><u>T1140</u></b> Deobfuscate/Decode Files or Information
<b><u>T1070</u></b> Indicator Removal	<b><u>T1070.004</u></b> File Deletion	<b><u>T1036</u></b> Masquerading	<b><u>T1036.005</u></b> Match Legitimate Name or Location
<b><u>T1053</u></b> Scheduled Task/Job	<b><u>T1053.005</u></b> Scheduled Task	<b><u>T1548</u></b> Abuse Elevation Control Mechanism	<b><u>T1548.002</u></b> Bypass User Account Control
<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1546</u></b> Event Triggered Execution	<b><u>T1546.012</u></b> Image File Execution Options Injection	

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>SHA256</b>	7910478d53ab5721208647709ef81f503ce123375914cd504b9524577057f0ec ebf461be88903ffc19363434944ad31e36ef900b644efa31cde84ff99f3d6aed 21ffa168a60f0edcbc5190d46a096f0d9708512848b88a50449b7a8eb19a91ed 942b93529c45f27cdbd9bbcc884a362438624b8ca6b721d51036ddaebc750d8e 75a51d1f1dd26501e02907117f0f4dd91469c7dd30d73a715f52785ea3ae93c8 4399c5d9745fa2f83bd1223237bdabbfc84c9c77bacc500beb25f8ba9df30379

TYPE	VALUE
<b>SHA256</b>	8327cd200cf963ada4d2cde942a82bbed158c008e689857853262fcd a91d14a4 9eceba551baafe79b45d412c5347a3d2a07de00cc23923b7dee1616 dee087905 630bb985d2df8e539e35f2da696096e431b3274428f80bb6601bbf4 b1d45f71e ef8e658cd71c3af7c77ab21d2347c7d41764a68141551938b885da41 971dd733 e654ecc10ce3df9f33d1e7c86c704cfdc9cf6c6f49aa11af2826cbc4b6 59e97c 16887b36f87a08a12fe3b72d0bf6594c3ad5e6914d26bff5e32c9b44 acfec040 39de0389d3186234e544b449e20e48bd9043995ebf54f8c6b33ef3a 4791b6537
<b>IPV4</b>	194.31.53[.]128 198.13.47[.]158 172.67.139[.]61 207.148.115[.]125 64.227.164[.]34 194.31.53[.]128 198.13.47[.]158
<b>Domains</b>	evnpowerspeedtest[.]com www.updateforhours[.]com dns.eudnslog[.]com asis.downloadwindowsupdate[.]co

## References

[https://www.trendmicro.com/en\\_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html](https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html)

<https://www.hivepro.com/earth-longzhi-new-subgroup-of-apt41/>

# 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

**May 4, 2023 • 7:20 AM**

© 2023 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)