Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

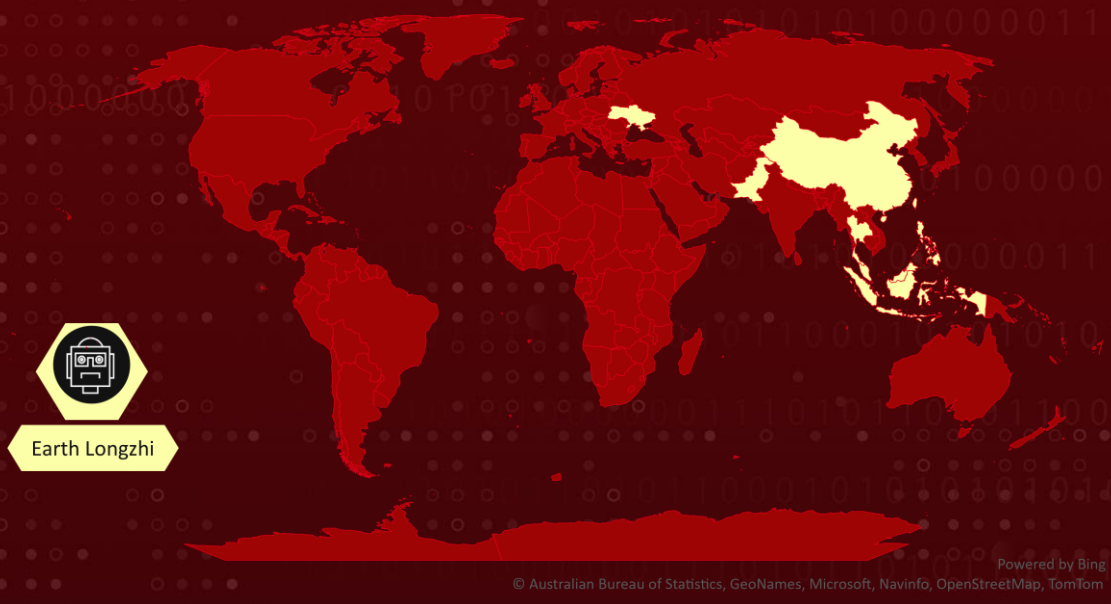
Earth Longzhi: New subgroup of APT41

Date of Publication	Admiralty code	TA Number
November 10, 2022	A1	TA2022251

Summary

First Appearance: 2020
Actor Name: Earth Longzhi(Subgroup of APT41)
Target Region: East and Southeast Asia
Target Sectors: Defense, Aviation, Insurance, Government, Healthcare, Academic, Infrastructure industries and Urban Development

Actor Map



CVE

CVE	NAME	PATCH
CVE-2019-16098	Privilege escalation in Micro-Star MSI Afterburner	✗

Actor Details

#1 Earth Longzhi is running a spearphishing campaign to infect organizations with a payload such as Cobalt Strike loader, Symatic loader, CroxLoader, BigpipeLoader, OutLoader, and other custom hacking tools.

#2 Furthermore, it was seen using the CVE-2019-16098 driver, which allows authenticated users to read/write any arbitrary address, including kernel space. Since Earth Longzhi uses similar TTPs and metadata to Cobalt Strike, it has been considered a subgroup of APT41.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Earth Longzhi (APT41)	China **MOTIVE** Financial crime, Information theft and espionage	East and Southeast Asia	Defense, Aviation, Insurance, Government, Healthcare, Academic, Infrastructure industries and Urban Development

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0006** Credential Access	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0043** Reconnaissance	**TA0011** Command and Control	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1589** Gather Victim Identity Information	**T1589.002** Email Addresses	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1036** Masquerading	**T1090.002** External Proxy	**T1211** Exploitation for Defense Evasion
T1547 Boot or Logon Autostart Execution	**T1547.012** Print Processors	**T1068** Exploitation for Privilege Escalation	**T1555** Credentials from Password Stores
T1555.003 Credentials from Web Browsers	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1190** Exploit Public-Facing Application
T1003 OS Credential Dumping	**T1003.001** LSASS Memory	**T1090** Proxy	**T1090.001** Internal Proxy
T1003.006 DCSync	**T1090.004** Domain Fronting	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1036.007 Double File Extension	**T1095** Non-Application Layer Protocol	**T1070** Indicator Removal on host	**T1070.006** Timestomp
T1573 Encrypted Channel	**T1573.002** Asymmetric Cryptography		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA 256	b6d2f4d9edd7b08c9841cca69c5cb6b312fa9ad1c19a447a26e915e1fd736e09 8478718e0bad7fde34f623794e966f662aaf2d7a21d365b45db80b2a0349ed8a 4b1b1a1293ccd2c0fd51075de9376ebb55ab64972da785153fcb0a4eb523a5eb c80289a1f293dceb71230cf0dbd0a45b9444519b1367a5ba04e990ea6acf6503 30b64628aae642380147c7671ea8f864b13c2d2affaaea34c4c9512c8a779225 03795a683bf3eb9ed7673522fe7eac45949a824da8043236cd504fd8106e3593 3ba81d78f3b764dc6e369f24196c41b4cba0764414ad85d42dae5a5f79e871e1 41bcdc3fc4c878fb34ebebeff6ff7d158be166d3fc220f3b90f225ae3757f2e8 8e2aac4e7776f66da785171baeee473e41cb88c60e535b80980d55ac7f873c5c a0bde01e83ccc42c0729b813108dd3da96a9bc175b3ad53807387bbf84d58112 bd959353bc6c05b085fc37589ea2ccd2c91aaf05ec7cf1a487f5de7fa0abc962 25bfa492e295599fe30d9477ac72a4848c1ee2b71ff92ef7dcca90587c8d0945 eb8d11b63d20e3d1e164f0f25822d54a58742faa8d10ba120740e612607b5f6 947fdef565d889d3d919d8d81014d718f2d22ef3ed0049c98960f7330f51f41f 969ac3517ae9c472e436c547a6721f426a675ad8dece53c3f8e79ba44aa884eb 3de17542ca2ffefc9572cd2707a664999f157a0fed02ac4abdae5f805f6a77ac 86598469671d83cd5525a89e2d1ae83f1f9529420c3325a746d84acffeb876ec 1903cd46184aa2b70c74e2bdd47b7bedd2ae7175295d6c1dab904204dedbabca 5eb94c62e75a8a11b1220f3f716f90bee69010ce4ad61c463be6e66dcaf29379 883064cdeeddd5ccbfa74dacc1d8a8b5a0d2c9794c59acef186dd7105594fdcc 8d3216c2fdbec7fc7a9af4e2d142e021d37037a187739d5aab2fa0351e8f4ec7

TYPE	VALUE
SHA 256	31d71e04ca898cbdb45ffea1c4f45a953e0833964ad2d14c014616acb1666996 4a438626ac962db91cde46ee2c04c850b46262599bc535b4a08209661d5fb44d 4bc4d2ad9b608c8564eb5da5d764644cbb088c2f1cb61427d11f7b2ce4733add 76998c3cef50132d7eb091555b034b03a351bd8639c1c5dc05cf1ea6c19331d9 f8fa90be3e6295c275a4d23429e8738228b70693806ed9b2f482581487cb8e08 90a1e3ff729b7b91ca82e7981d2c65bf6c4b8fb2204bf9394d2072d9caa70126
IPv4	47[.]108.173.88 139[.]180.138.226
Domains	www.affice366[.]com www.vietsovspeedtest[.]com c.ymvh8w5[.]xyz

References

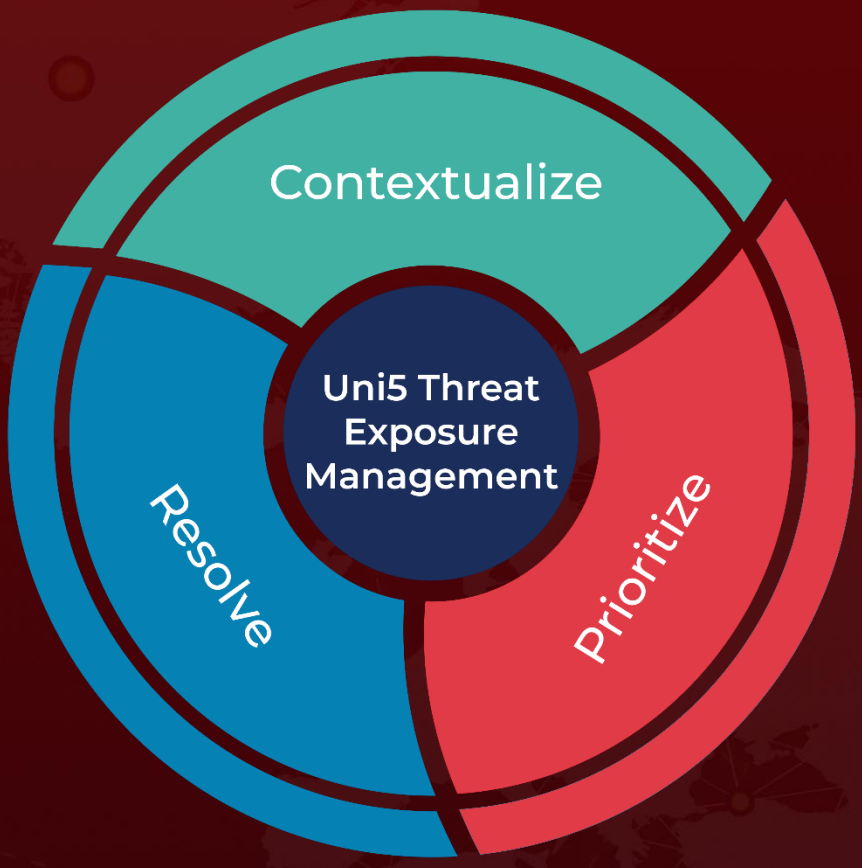
https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi/IOCs-hack-the-real-box-apt41-new-subgroup-earth-longzhi.txt

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 10, 2022 . 5:35 AM

More at www.hivepro.com