Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

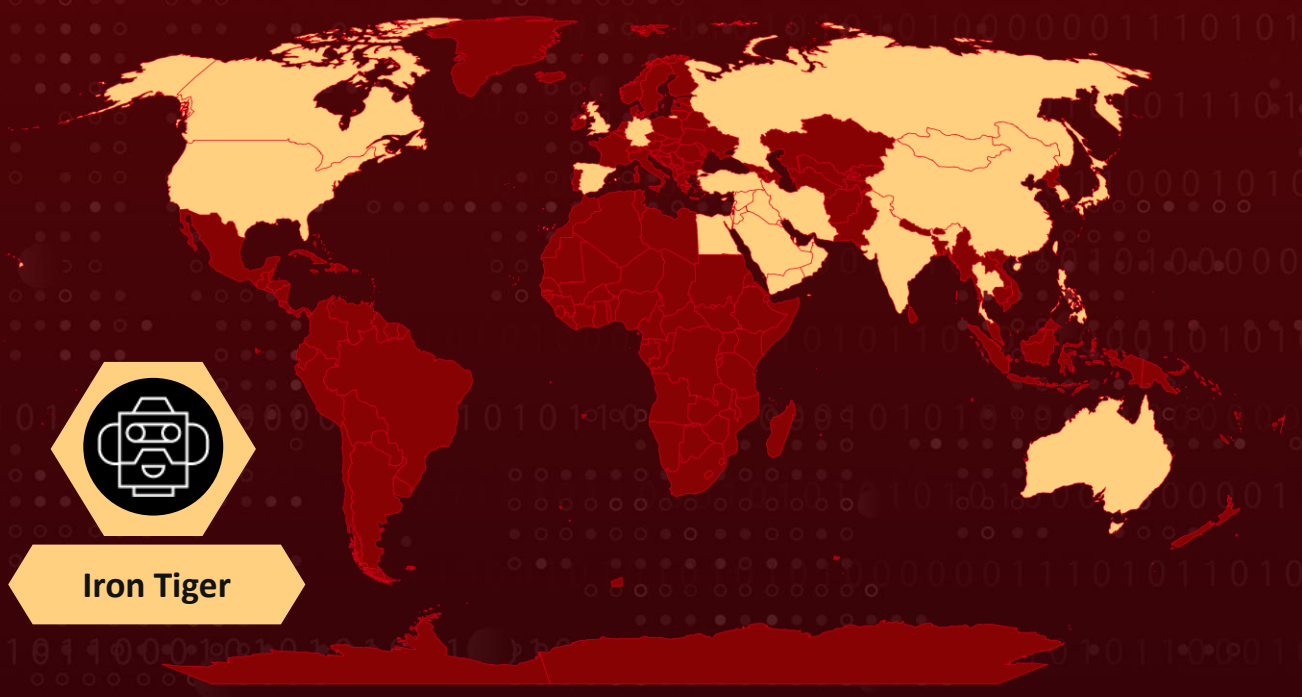
# Iron Tiger APT Group Updates SysUpdate Malware to Target Linux Platforms


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| March 02, 2023 | A1 | TA2023112 |

# Summary

**First Appearance:** 2010
**Actor Name:** Iron Tiger (APT 27,Emissary Panda,LuckyMouse,Bronze Union,TG-3390,TEMP.Hippo,Budworm,Group 35,ATK 15,Earth Smilodon,Red Phoenix,ZipToken)
**Target Region:** Australia, Canada, China, Germany, Hong Kong, India, Iran, Israel, Japan, Mongolia, Philippines, Russia, Spain, South Korea, Taiwan, Thailand, Tibet, Turkey, UK, USA and Middle East.
**Affected Platform:** Linux, Windows
**Target Sectors:** Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Telecommunications, and Think Tanks.
**Attack:** The Iron Tiger APT group updated their custom malware, SysUpdate, to target Linux platforms and evade security solutions. They specifically targeted a vulnerability in a Wazuh signed executable, using a complex loading process and new C&C communication through DNS TXT requests.

## Attack Regions



# Attack Details

**#1** Iron Tiger is a well-known advanced persistent threat (APT) group that primarily engages in cyber espionage. In 2022, they updated their custom malware, SysUpdate, to include new features and add support for Linux platforms. The loading logic of the malware is complex, likely in an attempt to evade security solutions.

**#2** The loading process entails several steps involving legitimate executables, sideloading different DLL names, and multiple binary file names being loaded by those DLLs. Iron Tiger specifically targeted a vulnerability in a Wazuh signed executable, appearing legitimate in the victim's environment.

**#3** The latest update includes similar features to the previous version, but with C++ run-time type information classes removed, and the code structure was changed to use the ASIO C++ asynchronous library, making reverse engineering samples longer.

**#4** Iron Tiger added a new feature of C&C communication through DNS TXT requests, where the malware retrieves configured DNS servers and generates a random number of 32 bits to send requests to the C&C server.

# 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 actors and attacks 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

| | | | |
|---|---|---|---|
| TA0003 Persistence | TA0002 Execution | TA0043 Reconnaissance | TA0004 Privilege Escalation |
| TA0011 Command and Control | TA0006 Credential Access | TA0005 Defense Evasion | TA0040 Impact |
| TA0001 Initial Access | T1552 Unsecured Credentials | T1552.004 Private Keys | T1027 Obfuscated Files or Information |
| T1055 Process Injection | T1456 Drive-By Compromise | T1572 Protocol Tunneling | T1404 Exploitation for Privilege Escalation |
| T1095 Non-Application Layer Protocol | T1055.012 Process Hollowing | T1140 Deobfuscate/Decode Files or Information | T1529 System Shutdown/Reboot |
| T1036 Masquerading | T1623 Command and Scripting Interpreter | T1036.006 Space after Filename | T1590 Gather Victim Network Information |
| T1590.002 DNS | T1218 System Binary Proxy Execution | T1406.002 Software Packing | T1547 Boot or Logon Autostart Execution |
| T1547.001 Registry Run Keys / Startup Folder | T1574 Hijack Execution Flow | T1574.002 DLL Side-Loading | T1566 Phishing |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 6d9031eb617096439bc8c8f7c32f4a11ffefc4326d99229fc78722873092e400<br>11f21d08f819dea21a09c602a4391142a5648f3e17a07a24d41418fcc17ea83f<br>9add546cb9527f9d7e4930aaddec6e14c70d1400d0d531a9102efd4c83b27dd7<br>3ac029e49ca71d948bfe1a7bc691967cf26cb5a731c7807d5be3cf6b579fa8ab<br>2ada1b48457c169cf3f80e248190374102615e2c89b70e574fba4ddc09b5fcd5 |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 09a3231a300d794010c3f400617cd0b1b7aab7141735a2b8635a8362584e196d<br>c65c435737ac02132d9dfeb6ec1d7d903648f61ecdda8a85b4250f064cb4673f<br>43ae4e624413a587667027c03416d78b2515ac9081b8c9c967aadb1157f49e55<br>b92a9dcdcf0bec8cd1e8b701dbf7bd6f7e68473a9e711267a4af8e4be783bb1e<br>08dd5a9fdc387855fb5a23c167abec63b22272f66de099155036c5ce7e4deeb8<br>1e2b05838edfb0460fc97e2d7bab2271891c55ca0c895d4db30cf2acfaea51d2<br>d950cc937f4df9ab0bad44513d23ea7ecdfae2b0de8ba351018de5fb5d7b1382<br>b504ab7a4a35e6deb34536d4663db696918961aadc03662b2c34e89b50ba10a1<br>a8527a88fb9a48f043a0b762c7431fb52e601b72ff2fa0d35327e5cc72404edc<br>0daa82650712f2338803521969f7dc7deebba0e34c4797a9e39d99595d7eb423<br>9499eabf880a55522c1b78d5afaa9ff34ae958950627ccd15099f2e771c9b0b1<br>ff6502b16b0c2eebef15964fd6fcc60c23b4afa88bebe99cfc54ee73f11aeb62<br>735eddc24aa98f30d8e6839dc8c669f565aa760952af8d00d4f6fbfe6776631d<br>ba1dabf7ff0a4bca8d7ff6e541b1930fc8328d240ba8a56ede96cc203daf6772<br>2027784b3f0e8e5f6add0aa42c6b9b6ea3e3e1af6373a465cb57b145d24373bf<br>76b5fa39d5b519e82e63466df1a6b2068cc9754343efbabf862924557c0fc213<br>0cd3df91582551182a0decf662a112e59591cf07f3d107f09df3194f7d498e62<br>83209d9b8ebd0add8665e533d0948ae4e878ccc21ba5e3b00bea8833b59acf9a<br>ba484eebda8dbe07b36eb07fa6c5cbb8d1dcc6638808cdcf7f33d7bab51d2805<br>123880edc91f7dc033a769d9523f783f7b426673ee95e9e33654cdfa95a6462c |

| TYPE | VALUE |
| --- | --- |
| SHA256 | fac0009d615e98238cf348819b21f0dbbb462653c2257f1c6ef552838894e166<br>39f90ef532307c23f485f6d337fd820651581aeb72f678477bcb106a3d831997<br>ed5047461b2cccac4e81bd9fa73469d69468521174b981b5f76abb450c6fdabe<br>cc196ee155bf864071cbeec3ddcd3e2451a37d4296f53a024142c70193b9691d<br>3f808df5af6889c2219fd4982dd49946535528237cc00530cce5c69c3e7f0e34<br>aad2e40411aa08e398cdf7397c7a1b3b7ab2a5ba833b6d65f68b145d51c2ed05<br>c256b85747ad81e3f3f6c49ce496e77f024b302f921cb007a5f5375ac5b672d7 |

# References

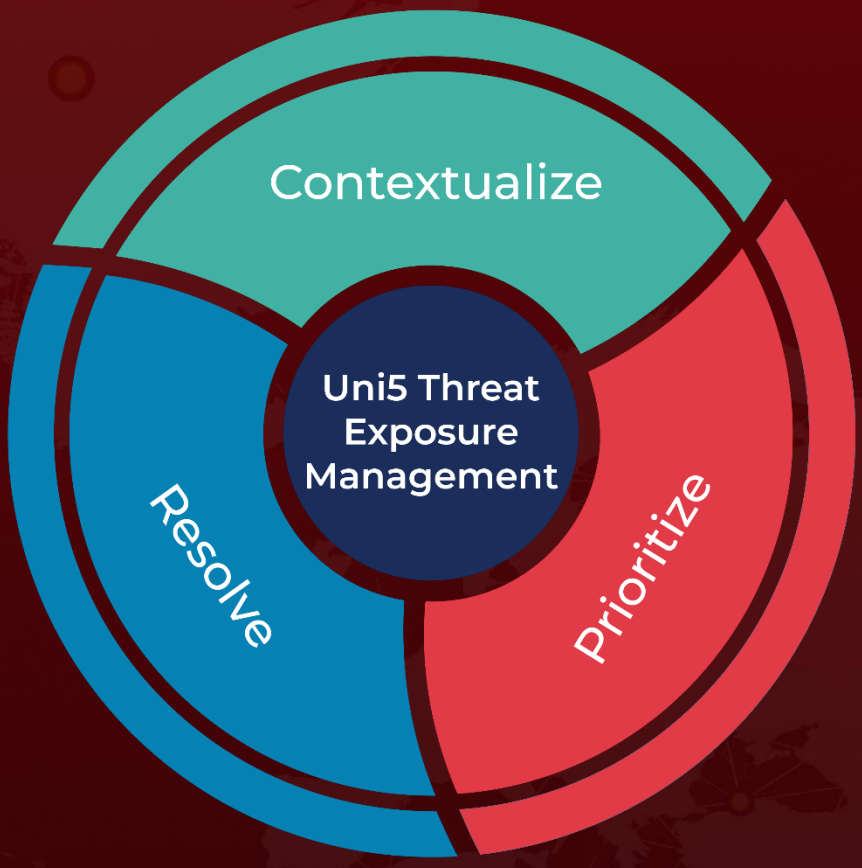

https://www.trendmicro.com/en_us/research/23/c/iron-tiger-sysupdate-adds-linux-targeting.html

https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/c/iron-tiger-sysupdate-reappears-adds-linux-targeting/IOCs-iron-tiger-sysupdate-reappears-adds-linux-targeting.txt

# 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

**March 02, 2023 • 12:30 AM**



More at www.hivepro.com