Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

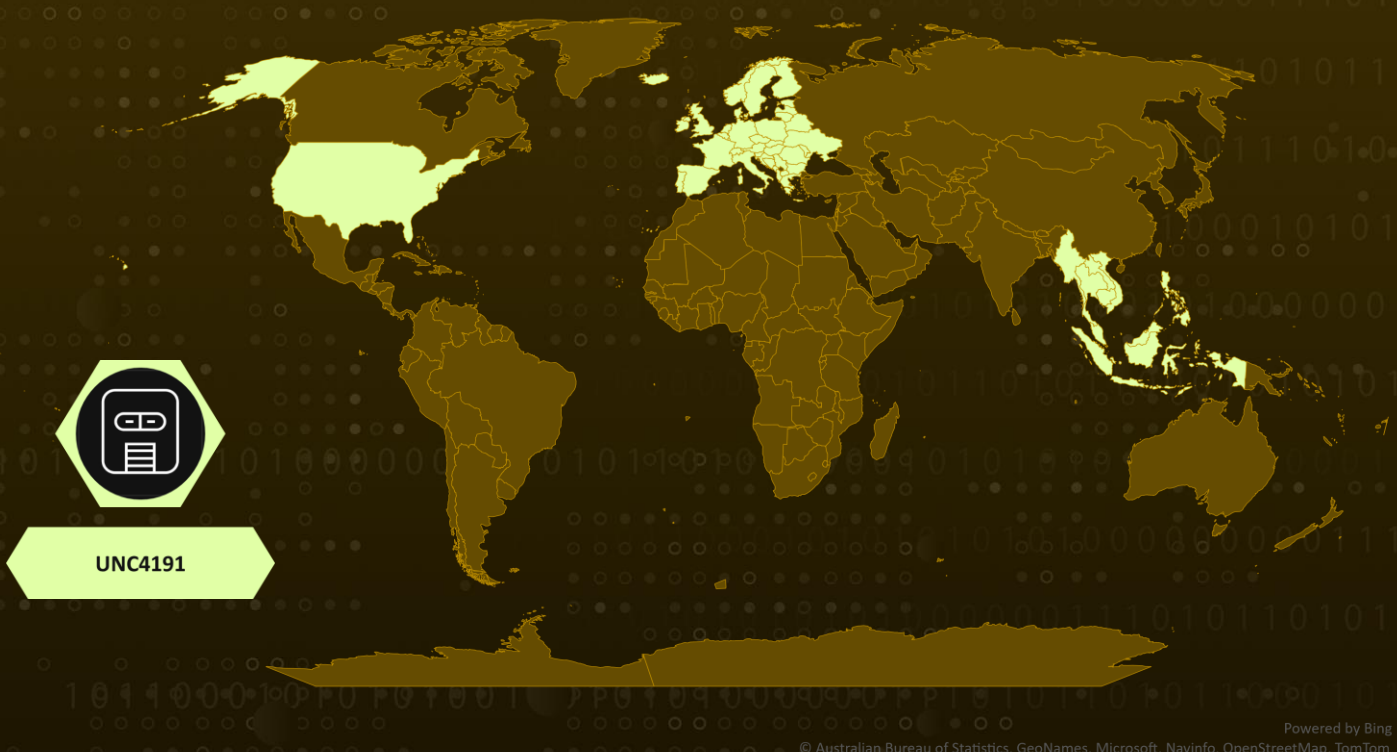
Chinese cyber espionage hackers target Southeast Asian firms

Date of Publication	Admiralty Code	TA Number
December 1, 2022	A1	TA2022277

Summary

First appearance: September 2021
Attack Region: Southeast Asia, the U.S., and Europe
Threat Actor: UNC4191
Attack: To obtain and keep access to the entity's network to gather intelligence.

Attack Regions



Attack Details

#1 UNC4191, a threat actor with a suspected China affiliation, has been linked to a series of espionage assaults primarily in Southeast Asia that use USB sticks as an initial infection vector. A variety of public and private sector entities have been impacted by the campaign.

#2 After the initial infection, the intruder used validly signed binaries to side-load malware, including three novel families MISTCLOAK, DARKDEW, and BLUEHAZE. A successful breach results in the distribution of a renamed NCAT binary and the execution of a reverse shell on the victim's system, providing the adversary with backdoor access.

#3 The DARKDEW dropper also serves to launch another executable, "Razer Chromium Render Process," which in turn executes the BLUEHAZE, a C/C++ launcher that advances the infection chain by launching a copy of Ncat to establish a reverse shell to a hardcoded command-and-control (C2) address.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	T1136 Create Account	T1136.001 Local Account
T1059 Command and Scripting Interpreter	T1091 Replication Through Removable Media	T1036 Masquerading	T1218 System Binary Proxy Execution
T1218.011 Rundll32	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	7753da1d7466f251b60673841a97ac5a c10abb9f88f485d38e25bc5a0e757d1e 6900cf5937287a7ae87d90a4b4b4dec5 f632e4b9d663d69edaa8224a43b59033 8ec339a89ec786b2aea556bedee679c7 f45726a9508376fdd335004fca65392a 707de51327f6cae5679dee8e4e2202ba ea7f5b7fdb1e637e4e73f6bf43dcf090
Domain	closed.theworkpc[.]com

References

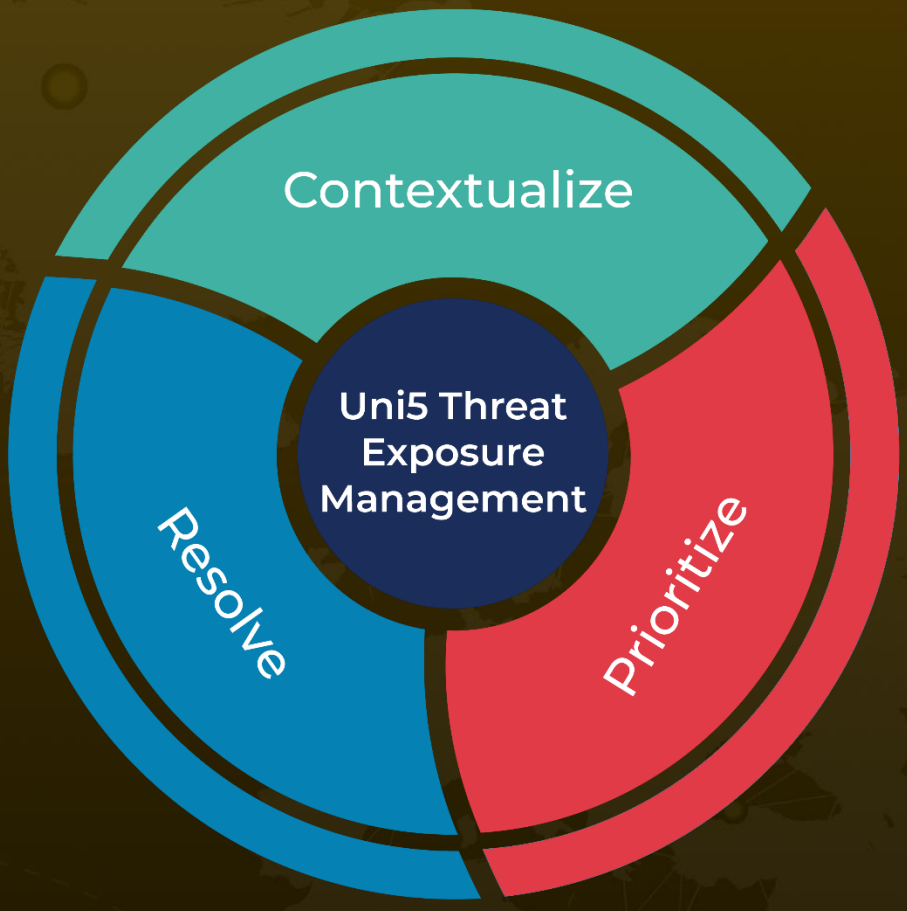
https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia

https://thehackernews.com/2022/11/chinese-cyber-espionage-hackers-using.html

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**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 1, 2022 . 4:08 AM

More at www.hivepro.com