EXECUTIVE SUMMARY

PROJECT CAMERASHY

CLOSING THE APERTURE ON CHINA'S UNIT 78020

ThreatConnect®, in partnership with Defense Group Inc., has attributed cyber espionage activity associated with the Naikon Advanced Persistent Threat (APT) group to a specific unit (Unit 78020) within the Chinese People's Liberation Army (PLA).

For nearly five years, Unit 78020 has employed malicious email attachments and spear phishing campaigns to exploit its targets in the Southeast Asian military, diplomatic, and economic sectors. These targets include government entities in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam along with the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).

KEY FINDINGS:

- **Unit 78020's focus is the disputed, resource-rich South China Sea, where China has been aggressively gathering intelligence for years.**
- **The activities of one specific officer within Unit 78020 suggest that the Naikon cyber espionage activity is state sponsored.**
- **Implications of this research include not only military alliances, but also risks to a major artery of international commerce through which trillions of dollars in global trade traverse annually.**

The Project CameraShy report applies the Department of Defense-derived Diamond Model for Intrusion Analysis to a body of evidence to understand relationships across complex data points spanning five years of activity. Using this model, our team pieced together information linking PLA Officer Ge Xing to the infrastructure and unit responsible for cyber espionage attacks.

DOWNLOAD THE FULL PROJECT CAMERASHY REPORT

www.ThreatConnect.com/CameraShy

THREATCONNECT™

DIAMOND MODEL FOR INTRUSION ANALYSIS

ADVERSARY

- People's Liberation Army Chengdu Military Region
- Second Technical Reconnaissance Bureau Military Unit Cover Designator 78020
- Ge Xing aka GreenSky27

CAPABILITIES

- Families of Unique Custom Malware
- Specific Post-Infection, Second-Stage Tools & Utilities
- Use of an Exploit Kit Leveraged by Asian Hackers

INFRASTRUCTURE

- Global Command & Control Infrastructure
- Chinese Dynamic DNS Infrastructure Providers
- Attacker-Registered Domains

VICTIMS

- Governments in Southeast Asia
- International organizations such as the Association of Southeast Asian Nations
- Public and private energy organizations

1

SOCIO-POLITICAL AXIS

To further strategic Chinese foreign policy objectives in the South China Sea

2

TECHNICAL AXIS

- CVE-2012-015
- Spear Phishing
- Right-to-Left Character Override
- Self-Extracting Executables

EXPLORE THE INTELLIGENCE

Discover how the Diamond Model of Intrusion Analysis unveiled key details about Naikon activity. See the summary of conclusions below.

The PLA's Chengdu MR Second TRB Military Unit Cover Designator (MUCD) Unit 78020 (78020 部队) operates primarily out of Kunming, China with an area of responsibility that encompasses border regions, Southeast Asia, and the South China Sea.

Naikon APT supports Unit 78020's mandate to perform regional computer network operations, signals intelligence, and political analysis of the Southeast Asian border nations, particularly those claiming disputed areas of the energy-rich South China Sea.

Analysis of historic command and control (C2) infrastructure used consistently within Naikon malware for espionage operations against Southeast Asian targets has revealed a strong nexus to the city of Kunming, capital of Yunnan Province in Southwestern China.

GreenSky27

The C2 domain "greensky27.vicp.net" consistently appeared within unique Naikon malware, where the moniker "GreenSky27" is the personification of the entity who owns and operates the malicious domain. Further research shows many social media accounts with the "GreenSky27" username are maintained by a PRC national named Ge Xing (葛星), who is physically located in Kunming.

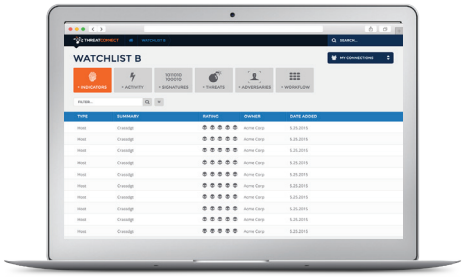
In eight individual cases, notable overlaps of Ge Xing's pattern of life activities would match patterns identified within five years of greensky27.vicp.net infrastructure activity.

Ge Xing, a.k.a. "GreenSky27," has been identified as a member of the PLA specializing in Southeast Asian politics, specifically Thailand. He is employed by Unit 78020 most notably evidenced by his public academic publications and routine physical access to the PLA compound.

STRATEGIC BUSINESS IMPLICATIONS

UNITE YOUR SECURITY OPERATIONS AROUND A COMMON DEFENSE

Project CameraShy is just one chapter in a continuously developing plotline of global cyber threat intelligence. Attacks may be politically motivated like GreenSky27, or threat actors may be after your proprietary business data and your customers' personal information. As an executive, you are responsible for maintaining the security and integrity of your brand. ThreatConnect gives CIO/CISOs and their team a single platform that integrates threat intelligence with incident response, uniting your entire security operations around a common defense. With ThreatConnect, your CIO/CISO can provide you strategic threat intelligence so you can make informed business decisions. Discover the benefits for your enterprise.



THREATCONNECT INC.
3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203

CONTACT THREATCONNECT TODAY

CALL: 1.800.965.2708