THREATCONNECT™

SEPTEMBER 23, 2015

Project CAMERASHY: Closing the Aperture on China's Unit 78020

IN BLOG, CAMERASHY, THREAT RESEARCH BY THREATCONNECT INTELLIGENCE RESEARCH TEAM (TCIRT)

[http://www.threatconnect.com/camerashy]

ThreatConnect® and Defense Group Inc. (DGI) have collaborated to share threat intelligence pertaining to the Advanced Persistent Threat (APT) group commonly known as "Naikon" within the information security industry. Our partnership facilitates unprecedented depth of coverage of the organization behind the Naikon APT by fusing technical analysis with Chinese language research and expertise. The result is a meticulously documented case against the Chinese entity targeting governments and commercial interests in South, Southeast Asia and the South China Sea. This report [http://www.threatconnect.com/camerashy] applies the Department of Defense-derived Diamond Model for Intrusion Analysis [http://www.threatconnect.com/platform/methodology/] to a body of technical and non-technical evidence to understand relationships across complex data points spanning nearly five years of exploitation activity.

Key Findings

- The Advanced Persistent Threat (APT) Group commonly known within the information security industry as "Naikon" is associated with the People's Liberation Army (PLA) Chengdu Military Region (MR) Second Technical Reconnaissance Bureau (TRB) Military Unit Cover Designator (MUCD) 78020.

- The PLA's Chengdu MR Second TRB MUCD 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.

- 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 People's Republic of China (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, aka "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.

In addition to this report, ThreatConnect has released technical indicators of the Naikon [https://app.threatconnect.com/tc/auth/threat/threat.xhtml?threat=789177] Threat within the ThreatConnect Common Community [http://www.threatconnect.com/platform/features/] , which is accessible to current users or by registering for a free account [http://www.threatconnect.com/platform/editions/#Community] . It is important to note we are not claiming this is a comprehensive listing of all

malware and infrastructure leveraged by Naikon globally for nearly half a decade. Rather, it forms one chapter of a larger story, where we look forward to enriching and expanding future collaborative research within our community of users and partners.

TAGS: Adversary Intelligence, Camerashy, Chinese APT, Cyber Espionage, Cyber Intelligence, Diamond Model of Intrusion Analysis, Economic Espionage, Ge Xing, HUMINT, incident, Naikon, South China Sea, Targeted Attacks, threat intel, Threat Intelligence

ABOUT THE AUTHOR

The ThreatConnect Intelligence Research Team (TCIRT): is an elite group of globally-acknowledged cybersecurity experts, dedicated to tracking down existing and emerging cyber threats. We scrutinize trends, technology and socio-political motivators to develop comprehensive knowledge of the cyber landscape. Then, we share what we've learned so that you can protect your organization, and your team can take precise action against threats.

RELATED POSTS

MAY 31, 2015

DECEMBER 17, 2013

Adversary Intelligence: Getting Behind the Keyboard

Adversary Intelligence: Getting Behind the Keyboard

ThreatConnect Takes Signature Management to the Next Level

ThreatConnect Takes Signature Management to the Next Level

APRIL 15, 2015

What the Verizon DBIR Says About Threat Intelligence Sharing

What the Verizon DBIR Says About Threat Intelligence Sharing

JULY 3, 2014

Getting Back to the Basics of Actionable Threat Intelligence

Getting Back to the Basics of Actionable Threat Intelligence

MARCH 18, 2013

A Tale of Two Koreas: Keeping Watch over the Digital DMZ

A Tale of Two Koreas: Keeping Watch over the Digital DMZ

MARCH 18, 2015

Premera Latest Healthcare Insurance Agency to be Breached

Premera Latest Healthcare Insurance Agency to be Breached