PROJECT

CAMERASHY

CLOSING THE APERTURE ON CHINA'S UNIT 78020

THREAT CONNECT™

DGI
BH
BLUE HERON

TABLE OF CONTENTS

CAMERASHY
INTRODUCTION

ThreatConnect Inc. and Defense Group Inc. (DGI) have partnered 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 government and commercial interests in South Asia, Southeast Asia, and the South China Sea.

ThreatConnect Inc.

ThreatConnect® is an enterprise solution that bridges incident response, defense, and threat analysis. Our premier cyber Threat Intelligence Platform allows global organizations to effectively manage the massive amounts of threat information that comes in daily. Organizations are able to move proactively against threats using ThreatConnect to increase productivity and deliver dynamic knowledge management, high context indicators, and automated responses. More than 5,000 users and organizations worldwide across industries, and ranging in size from the small business through the enterprise, turn to ThreatConnect to make intelligent decisions for their cyber security.

Defense Group Inc. BLUE HERON

Led by Dr. James Mulvenon, one of the leading experts on Chinese cyber and espionage issues in the United States, DGI's Center for Intelligence Research and Analysis (CIRA) is a premier open source exploitation organization with a particular focus on foreign cyber intelligence. CIRA is staffed by a mix of more than fifty highly trained linguist analysts who have native or near-native fluency in Chinese, Russian, and Farsi, as well as a dozen additional languages; technologists who are expert in building state-of-the-art misattributable collection architectures and analytic tools needed to process the immense quantities of foreign open source data now available; and methodologists who develop innovative approaches to solving tough analytic challenges. BLUE HERON is CIRA's new commercial cyber intelligence product line, offering strategic cyber intelligence, critical indications and warning of foreign cyber intrusion planning, and detailed enumeration of your adversaries and their tactics, techniques, and procedures.

Special Thanks

The ThreatConnect / DGI team would like to send a very special thanks to the team at PassiveTotal.com for the use of their aggregated passive DNS dataset which proved to be an invaluable resource in conducting this research.

EXECUTIVE SUMMARY

ThreatConnect®, in partnership with Defense Group Inc., has attributed targeted cyber espionage infrastructure activity associated with the "Naikon" Advanced Persistent Threat (APT) group to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). This assessment is based on technical analysis of Naikon threat activity and native language research on a PLA officer within Unit 78020 named Ge Xing.

For nearly five years, Unit 78020 has used an array of global midpoint infrastructure to proxy the command and control of customized malware variants embedded within malicious attachments or document exploits. These malicious attachments are operationalized within spear phishing campaigns that establish beachheads into target organizations, facilitating follow on exploitation activities.

Unit 78020 conducts cyber espionage against Southeast Asian military, diplomatic, and economic targets. The targets include government entities in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam as well as international bodies such as United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).

We assess Unit 78020's focus is the disputed, resource-rich South China Sea, where China's increasingly aggressive assertion of its territorial claims has been accompanied by high-tempo intelligence gathering. The strategic implications for the United States include not only military alliances and security partnerships in the region, but also risks to a major artery of international commerce through which trillions of dollars in global trade traverse annually.

This report applies the Department of Defense-derived Diamond Model for Intrusion Analysis[1] to a body of technical and non-technical evidence to understand relationships across complex data points spanning nearly five years of exploitation activity. The Diamond Model is an approach to analyzing network intrusion events. The model gets its name and shape from the four core interconnected elements that comprise any event – adversary, infrastructure, capability, and victim. Thus, analyzing security incidents – from a single intrusion up to a full campaign – essentially involves piecing together the diamond using elements of information collected about these four facets to understand the threat in its full and proper context over time.

....

1   http://www.dtic.mil/docs/citations/ADA586960

Previous Works

In April of 2012, ShadowServer initially introduced what would later be known as Naikon as an "Unknown/Unnamed" threat when they shared analysis[2] of commingled spear phishing lures obtained from the HardCore Charlie[3] data dump. The Naikon APT would not achieve mainstream awareness until June 2013[4] when TrendMicro published a detailed analysis of Naikon's Rarstone malware.

The May 2014 ThreatConnect blog post "Piercing the Cow's Tongue" – a reference to the shape of the nine-dashed line China uses to demarcate its territorial claims in the South China Sea – tied Naikon to the most prolific and brazen targeting campaign against Southeast Asian nations.[5] A year later, Kaspersky Labs published a comprehensive white paper detailing historic Naikon activity and key technical findings.[6] Kaspersky also independently concluded the Naikon APT appeared to be a dedicated and resourced effort focused on targeting Southeast Asian countries, noting Naikon was responsible for an "incredible volume of attack activity around the South China Sea that has been going on since at least 2010."

Why We Are Releasing this Analysis

Ultimately, we believe it is our responsibility to inform our global user base and bring these findings to light for public consideration. ThreatConnect has demonstrated commitment to this ideal by freely sharing threat intelligence and providing an industry-recognized platform in which others can aggregate, analyze, and act against common threats. As the most widely adopted and comprehensive Threat Intelligence Platform on the market, we understand good intelligence goes beyond just tactical indicators; it must provide sufficient context to enable more informed decisions. To that end, we hope this report serves as an example of the level of full-bodied threat intelligence analysis we seek to enable for our users and encourage within the community.

The ThreatConnect/DGI team acknowledges the controversial nature of such a public indictment and recognizes that exposing the truth is not always popular. We expect the initial reaction by some will be to condemn the messenger rather than the military unit responsible for the activity revealed in this report. Others will surely marginalize or question the private sector's mandate for conducting such research despite Executive Order 13691's *(Promoting Private Sector Cybersecurity Information Sharing)*[7] recognition of the private sector's obligation to share information to mitigate common risks.

In answering the call of EO 13691, we have carefully sought to allay innate skepticism by meeting it head-on with detailed infrastructure analysis overlaid against geopolitical and "pattern of life" activities that buttress the aggregate body of evidence, which cannot be muted by the staccato of official dismissals and denials to which the court of world opinion has become so accustomed.

In addition to this report, ThreatConnect has released technical indicators we have associated with Naikon activity within the ThreatConnect Common Community, which is accessible by registering for a free account on www.threatconnect.com. 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.

....

2   http://blog.shadowserver.org/2012/04/16/beware-of-what-you-download-recent-purported-ceiec-document-dump-booby-trapped/
3   https://twitter.com/HardcoreCharle
4   http://blog.trendmicro.com/trendlabs-security-intelligence/rarstone-found-in-targeted-attacks/
5   http://www.threatconnect.com/news/piercing-the-cows-tongue-china-targeting-south-china-seas-nations/
6   https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf
7   http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf

THE NAIKON APT DIAMOND

The Diamond Model, an analytic framework for assessing network intrusion events, is the foundation of our assessment of the Naikon APT. In order to guide the reader, we will highlight which facet of the Diamond we are pivoting to throughout this assessment.

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

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 Chengdu Military Region (MR) Second Technical Reconnaissance Bureau (TRB) Military Unit Cover Designator (MUCD) 78020.

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.

GreenSky27

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 PRC national named Ge Xing (葛星), who is physically located in Kunming.
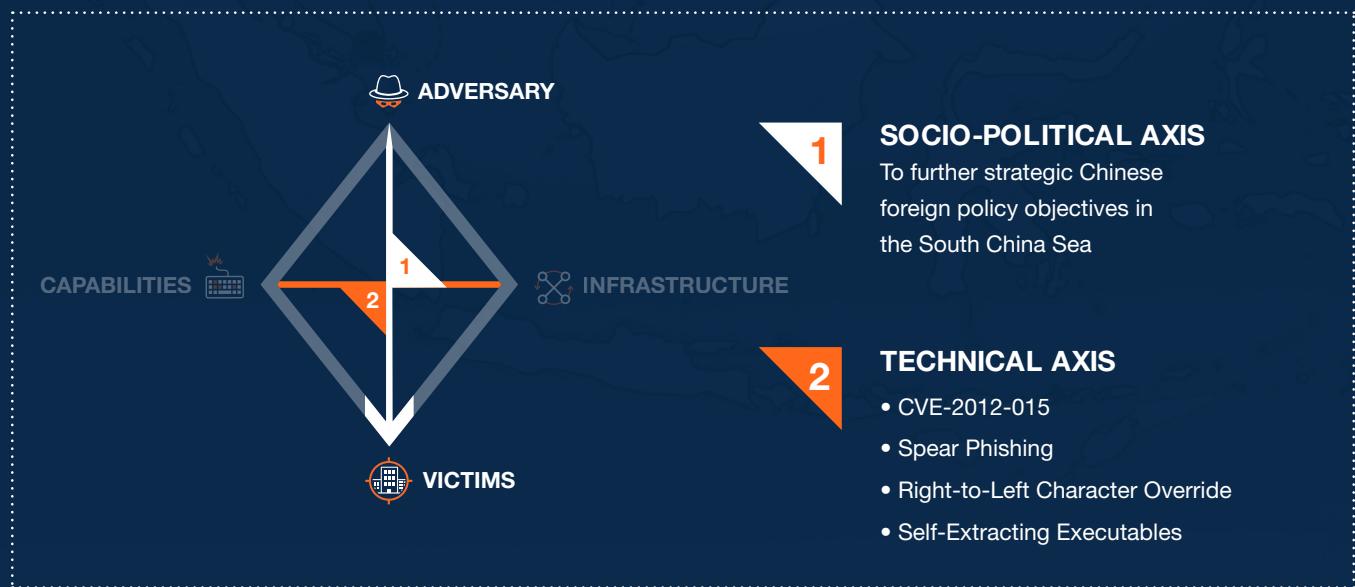
In eight individual cases, notable overlaps of Ge Xing's pattern of life activities would match patterns identified within five years of greensky27.vicp.net infrastructure activity.

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.

TENSIONS IN THE SOUTH CHINA SEA AND CHINA'S CYBER RESPONSE

ADVERSARY

CAPABILITIES

INFRASTRUCTURE

1

2

VICTIMS

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

The South China Sea lies at the crux of where the Pacific and Indian Oceans meet and is a crucial thoroughfare for the global economy. Five trillion dollars in bilateral trade and nearly a third of all global oil[8] transits the South China Sea annually, according to the White House.[9] The U.S. Energy Information Administration estimates 11 billion barrels of oil and 190 trillion cubic feet of natural gas reserves lie below the South China Sea.[10]

....

8   http://www.eia.gov/beta/international/regions-topics.cfm?RegionTopicID=SCS
9   https://www.whitehouse.gov/the-press-office/2011/11/13/press-briefing-nsa-strategic-
     communications-ben-rhodes-and-admiral-rober
10   http://www.eia.gov/beta/international/regions-topics.cfm?RegionTopicID=SCS
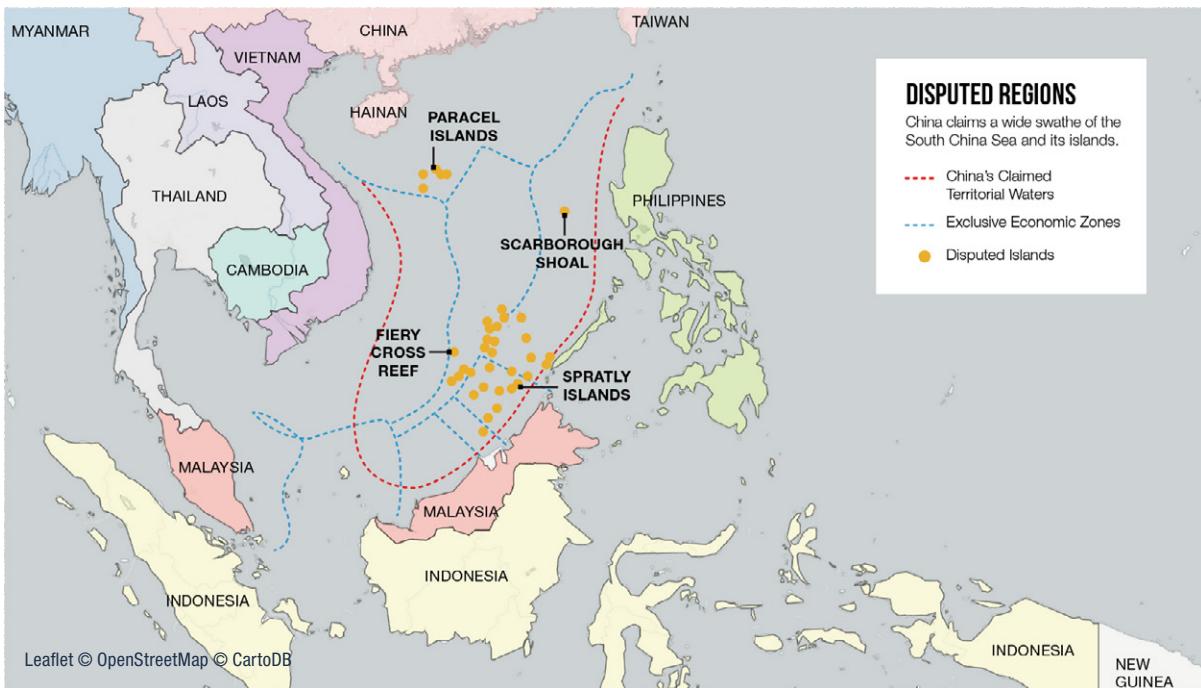
Figure 1: Disputed regions and exclusive economic zones within the South China Sea.

The littoral states have long contested the various reefs, atolls, and islands in the South China Sea. China, the Philippines, Vietnam, Malaysia, and Taiwan all claim the disputed Spratly Islands – a string of geographic features rich in energy and fisheries. China's claims are the most sweeping, with Beijing claiming most of the disputed South China Sea as sovereign territory. Confrontations between claimants have ranged from mere harassment of commercial fishing and military vessels[11] to deadly clashes.[12,13]

As the Council on Foreign Relations notes, "These tensions are shaping – and being shaped by – rising apprehensions about the growth of China's military power and its regional intentions. China has embarked on a substantial modernization of its maritime paramilitary forces as well as naval capabilities to enforce its sovereignty and jurisdiction claims by force if necessary."[14]

Dominating the South China Sea is a key step for Beijing towards regional hegemony, and the other claimants are both weaker and lack the security guarantees from the U.S. that have helped to temper similar tensions with Japan in the East China Sea.

Over the last year, China has adopted a more aggressive posture in the region. China is increasingly deploying the Chinese Coast Guard to enforce its claims over features in the South China Sea and operates PLA Navy vessels over the horizon so they are ready to respond to escalation. China's maritime law enforcement fleet, comprised primarily of Chinese Coast Guard vessels, is likely to increase in size by 25 percent and is larger than all of the other claimants combined, according to the Department of Defense.[15] China also relies heavily on its offensive cyber capabilities to gather intelligence on regional military, diplomatic, and economic intentions regarding the South China Sea. Behind the scenes, China is mounting a robust computer-network exploitation campaign against claimants, and Unit 78020 is one of the primary players involved in the Chinese cyber response.

. . . .

11   http://www.heritage.org/research/reports/2014/04/a-national-strategy-for-the-south-china-sea
12   https://www.youtube.com/watch?v=uq30CY9nWE8
13   http://news.usni.org/2012/06/20/south-china-sea-history-armed-conflict
14   http://www.cfr.org/world/armed-clash-south-china-sea/p27883
15   The Asia-Pacific Maritime Security Strategy, p. 13. http://www.defense.gov/Portals/1/Documents/pubs/NDAA%20A-P_Maritime_SecuritY_Strategy-08142015-
         1300-FINALFORMAT.PDF.

Fiery Cross Reef: A Case Study on How China Combines Cyber with Other Elements of National Power
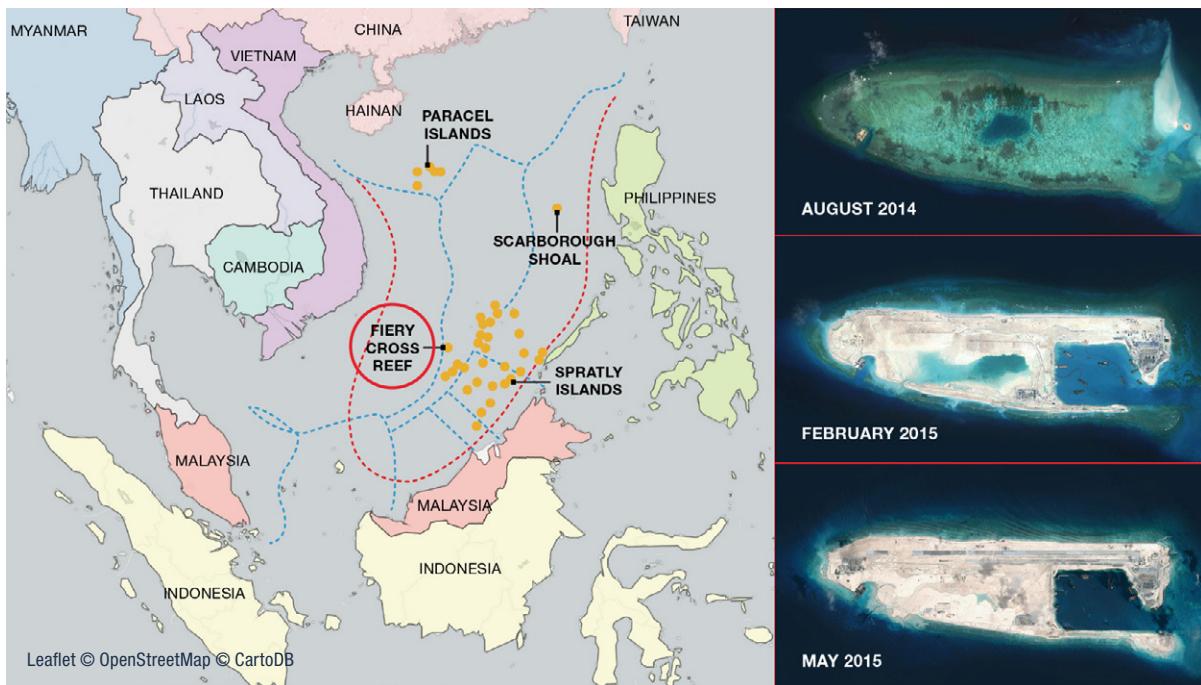

Figure 2: Fiery Cross Reef buildup; Images by DigitalGlobe, via *the New York Times*, CSIS Asia Maritime Transparency Initiative, and CNES, via Airbus DS and IHS Jane's.

To bolster their claims in the South China Sea, regional states have built islands by dredging seafloor material and depositing it atop coral reefs, a process that irreversibly destroys the reef.[16] Over the last 18 months, "China has reclaimed over 2,000 acres, more than all other claimants combined…and more than in the entire history of the region."[17] This activity is most notable on Fiery Cross Reef. In its natural state, Fiery Cross Reef is submerged at high tide. Between August and November 2014, Chinese dredgers created a landmass that spans the entire existing reef, increasing the land area 11 times over.[18]

"China insists that its landfill work is intended to provide public goods such as lighthouses, typhoon shelters for fishermen, weather stations, and search-and-rescue facilities," according to *The Economist*.[19] However, the Chinese have also built a 1.9-mile-long runway capable of supporting any of China's military aircraft, turning Fiery Cross into a useful power projection platform and raising concern that China's ultimate purpose is military in nature. In May 2015, a Chinese admiral said Beijing could set up an air defense identification zone above disputed areas of the South China Sea if it thought it was facing a large enough threat.[20]

Although the U.S. does not take an official position on ownership of the Spratly Islands, it has reiterated its commitment to freedom of navigation. In late May 2015, the U.S. Navy flew a surveillance mission[21] around Fiery Cross Reef and stated its intent to continue conducting routine surveillance flights, even having the U.S. Commander of the Pacific Fleet Admiral Scott Swift on one mission.[22]

.…………..

16   http://amti.csis.org/environmental-aggression-in-the-south-china-sea/
17   Secretary of Defense Ashton Carter. 30 May 2015 IISS Shangri-La Dialogue: "A Regional Security Architecture Where Everyone Rises" http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1945
18   http://amti.csis.org/fiery-cross/
19   "Asian Security: Small Reefs, Big Problems," in The Economist, July 25, 2015. http://www.economist.com/news/asia/21659771-asian-coastguards-are-front-line-struggle-check-china-small-reefs-big-problems?zid=306&ah=1b164dbd43b0cb27ba0d4c3b12a5e227
20   http://www.nytimes.com/2015/06/01/world/asia/china-says-it-could-set-up-air-defense-zone-in-south-china-sea.html
21   http://www.cnn.com/2015/05/20/politics/south-china-sea-navy-flight/
22   http://thediplomat.com/2015/07/us-commander-joins-south-china-sea-surveillance-flight/

The Philippines has taken a different approach by trying to use the weight of international law. Countries can claim a 200-nautical-mile exclusive economic zone (EEZ) off the coast of their mainlands and habitable islands under the United Nations Conference on the Law of the Sea (UNCLOS), the primary source of international law on this subject. The Philippines is seeking a ruling on whether China's building on submerged reefs confers the right to territorial waters and EEZs. China has refused to participate in arbitration thus far,[23] claiming the tribunal does not have jurisdiction.

Beijing's unwillingness to participate in international arbitration has not stopped it from surreptitiously monitoring those interested in the case. In early July 2015, Chinese APT actors (not associated with Naikon) used an Adobe Flash Player exploit within official Permanent Court of Arbitration webpages detailing the case between the Philippines and China. The exploit appeared on day three of the Netherlands-based Permanent Court of Arbitration tribunal and altered the webpage to load a malicious URL when visited, which would allow the adversary to exploit vulnerable web browsers and deploy a malicious payload to the victim host. The tactic of leveraging strategic website compromises with patched or unpatched exploits is a well-known observable used consistently by many APT groups. Additional technical details on this attack can be found in the July 2015 ThreatConnect blog post "China Hacks the Peace Palace."[24] China's efforts to target the tribunal underscore how Beijing integrates its cyber assets on a routine basis with its diplomatic, political, and military initiatives.

The Naikon APT: Conducting Geopolitically Motivated Campaigns Since 2010

Kaspersky Labs, which has authored the most comprehensive introduction to the Naikon APT, describes a group conducting high-volume, high-profile, geopolitically motivated attacks over at least five years.[25] Kaspersky assesses Naikon has a high success rate infiltrating national organizations in countries affiliated with the Association of Southeast Asian Nations (ASEAN) with early victims located mostly throughout Myanmar, Vietnam, Singapore, Laos, Malaysia, and the Philippines. Target profiles included high-profile government and military agencies around the South China Sea as well as state media and energy organizations both public and private. Appendix A: Naikon Oil & Gas-Themed Activity illustrates an example of Naikon activity likely seeking to exploit those interested in strategic regional energy resources.

The structure of Naikon operations suggests campaigns focused on individual countries, with specific toolsets deployed against a range of organizations within the designated country. To get into target networks, the Naikon APT relies on email as an attack vector and precise social engineering to identify appropriate targets. Data collection prior to an attack has included full names, email addresses, date of birth, interests in current events, nationality, gender, and previous email and social network communications to and from a target. Kaspersky notes how the Naikon APT used a United Nations discussion and vote on nuclear proliferation and disarmament, the missing Malaysian Airlines MH370 flight, and construction on the Raytheon-built National Coast Watch Center in the Philippines as decoy content for attacks. They conclude Naikon's use of decoys that maintain regional topics of interest reveals the APT's specific victims and how they change over time more strikingly than typically seen by other malicious actors. Additional examples of Naikon's use of stolen ASEAN draft talking points and classified Philippines documents can be found in the May 2014 ThreatConnect blog post "Piercing the Cow's Tongue: China Targeting South China Sea Nations."[26]

The structure of Naikon's campaigns, nature of the targets, and reliance on precision social engineering support our hypothesis that the Naikon APT is PLA Unit 78020, which will be proven conclusively with technical evidence in Chapter Two.

. . . .

23   http://economictimes.indiatimes.com/news/international/world-news/will-not-recognise-international-panel-ruling-on-disputed-south-china-sea-china/articleshow/48071215.cms
24   http://www.threatconnect.com/news/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us/
25   https://securelist.com/files/2015/05/TheNaikonAPT-MsnMM1.pdf
26   http://www.threatconnect.com/piercing-the-cows-tongue-china-targeting-south-china-seas-nations/

Unit 78020 and PLA Regional Cyber Operations

Each of the PLA's seven military regions has technical reconnaissance bureaus (TRBs), assessed to provide signals intelligence and cyber reconnaissance support.[27] TRBs appear to be tasked with communications intelligence, direction finding, traffic analysis, translation, cryptology, computer network defense, and computer network exploitation.

The Kunming TRB is one of ten military region TRBs located throughout China, and it is also known by its military unit cover designator (MUCD) as Unit 78020. Chinese military units are given MUCDs, five-digit numerical sequences, to provide basic anonymity for the unit in question and as a standardized reference. MUCDs are also used in official publications and on the Internet to refer to the unit in question.[28] Additional information on TRBs can be found in Appendix B: Technical Reconnaissance Bureaus.

In addition to conducting network reconnaissance and computer network operations, TRBs maintain a staff of linguists and regional analysts, who may be involved in traffic analysis and reporting as well as regional political, military, and economic analysis.[29] A survey of academic journal articles published by authors affiliated with Unit 78020 include not only papers related to communications technologies, network security, cryptanalysis, and social network analysis, but also publications on politics in Thailand and Vietnam and ASEAN science and technology policy (see list of publications within Appendix C: Summary of Publications Written by Unit 78020 Personnel).

....

27   Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Institute*, November 11, 2011.

28   The Chinese Army Today: Tradition and Transformation for the 21st Century — Dennis J. Blasko

29   A 2014 press release from the Kunming municipal government commends a translator within the Unit 78020 40th sub-unit (分队) as an "advanced person" (先进个人), suggesting that this sub-unit engages in translation or regional analysis. Available at http://yunnan.mca.gov.cn/article/tzgg/201405/20140500646780.shtml, accessed July 10, 2015.

Location of Unit 78020's Compound

Our research places the Kunming TRB headquarters at 158 Jiaochang East Road (教场东路158号), in the centrally located Wuhua District (五华区).[30] Additional Chinese sources show the Kunming TRB has multiple sub-units and facilities in Kunming, with several of these entities also indicating an address on Jiaochang East Road.[31,32] Satellite imagery of the facility believed to be the Kunming TRB's main compound is shown in Figure 3 below.

Figure 3: PLA Chengdu MR 2nd TRB MUCD 78020; 158 Jiaochang East Road, Wuhua District, Kunming (云南省昆明市五华区教场东路158号); Image by Digital Globe, via Google Earth. Date of image: 12/2/2012.

....

30   An article on computer network electrical surge protection measures written in 2008 by a Li Guochao at the 42nd sub-unit gives 158 Jiaochang East Road as the unit's address.
31   Papers written by personnel at the 43rd sub-unit place it at North Jiaochang Road, although the address is not entirely clear and may refer instead to northern Jiaochang Road (北教场).
32   See http://wh.km.gov.cn/uploadfiles/old/A15730.htm.

CHAPTER 2
ALL "NAIKON" ROADS LEAD TO KUNMING

CAPABILITIES

ADVERSARY

INFRASTRUCTURE

VICTIMS

TECHNICAL AXIS
Naikon malware to infrastructure relationship, with a focus on "personified" infrastructure

Having provided the backdrop of Chinese geopolitical, physical, and cyber aggression in the South China Sea region, we now turn to an in-depth, data-driven analysis of one very interesting part of Unit 78020's vast operational infrastructure. Our goal is to describe and profile the greensky27.vicp.net domain in order to develop a better understanding of the scope, structure, and activities of the adversary controlling it.

Like other APTs, Unit 78020 leverages dynamic domain infrastructure to improve the survivability and mobility of their custom malware. This allows network exploitation operators to quickly shift their C2 to new hosts without expending costly resources to refit and redeploy their malware due to a hard-coded IP address.

Unit 78020's infrastructure maintains a notably regionalized theme, with naming conventions consistent with South and Southeast Asian entities under its area of responsibility. On the next page we can map clusters of Unit 78020 infrastructure to their corresponding regionalized themes.

In addition to regionalized naming conventions, Unit 78020's personnel have in rare instances personified or personalized the infrastructure. Mandiant provided one such example in its APT 1 report revealing the "UglyGorilla" persona to be Unit 61398's Wang Dong.[33]

HOW DO ADVERSARIES BUILD MALICIOUS INFRASTRUCTURE?

We focus a lot on a particular set of adversary infrastructure in this section, but some readers may wonder how such large-scale malicious networks come to be in the first place. There are many ways an adversary can accomplish this. They can use infrastructure they own directly, but most adversaries know this is a sure-fire way to get caught. To add degrees of separation, they can buy or rent from another adversary or accomplice. Abusing infrastructure belonging to a legitimate and unwitting service provider is another avenue. Many build-it-yourself options exist, most of which involve compromising hosts on the Internet in some way and maintaining them over time through a combination of either legitimate remote management/administration and backdoor command/control (C2) malware.

Naikon Malware Associations

Specific to our current research, a member of Unit 78020 maintained the personified hostname greensky27.vicp.net since 2010 or prior, during which time it has been referenced within at least eight custom malware samples. This subsection does not analyze the technical intricacies of those samples. Our goal is merely to highlight the subset of Naikon malware families configured to communicate with the dynamic domain greensky27.vicp.net and then pivot to an in-depth analysis of that infrastructure.

MALWARE MD5 HASH	OBSERVED DATE	NAIKON SUBVARIANT
fb450ecb2639c0a550cec0497e95460e	07/04/2013	WinMM
b35f2de87343a674f5c1d809a5666349	08/10/2013	WinMM
7890eda704de4fe3f0af555c0be6ccba	08/11/2013	Wmi Inject
e645e619856fc2e8101a4e7902120ac3	10/03/2013	SslMM
def6e8ad26337890eb262b8f8dd39c17	11/10/2013	SslMM
66523a430459f284a3610c2070ca1ea7	12/27/2013	Rarstone
a2378fd84cebe4b58c372d1c9b923542	**03/26/2014**	**WinMM**
92861d0a999591aeb72988b56d458040	07/18/2014	WininetMM

Table 1: Observed Naikon implants that maintain greensky27.vicp.net command and control functionality.
Note: The highlighted hash is referenced in Figure 4.

. . . .

33   http://www.bloomberg.com/news/articles/2014-05-22/uglygorilla-hacker-left-tracks-u-s-cyber-hunters-say
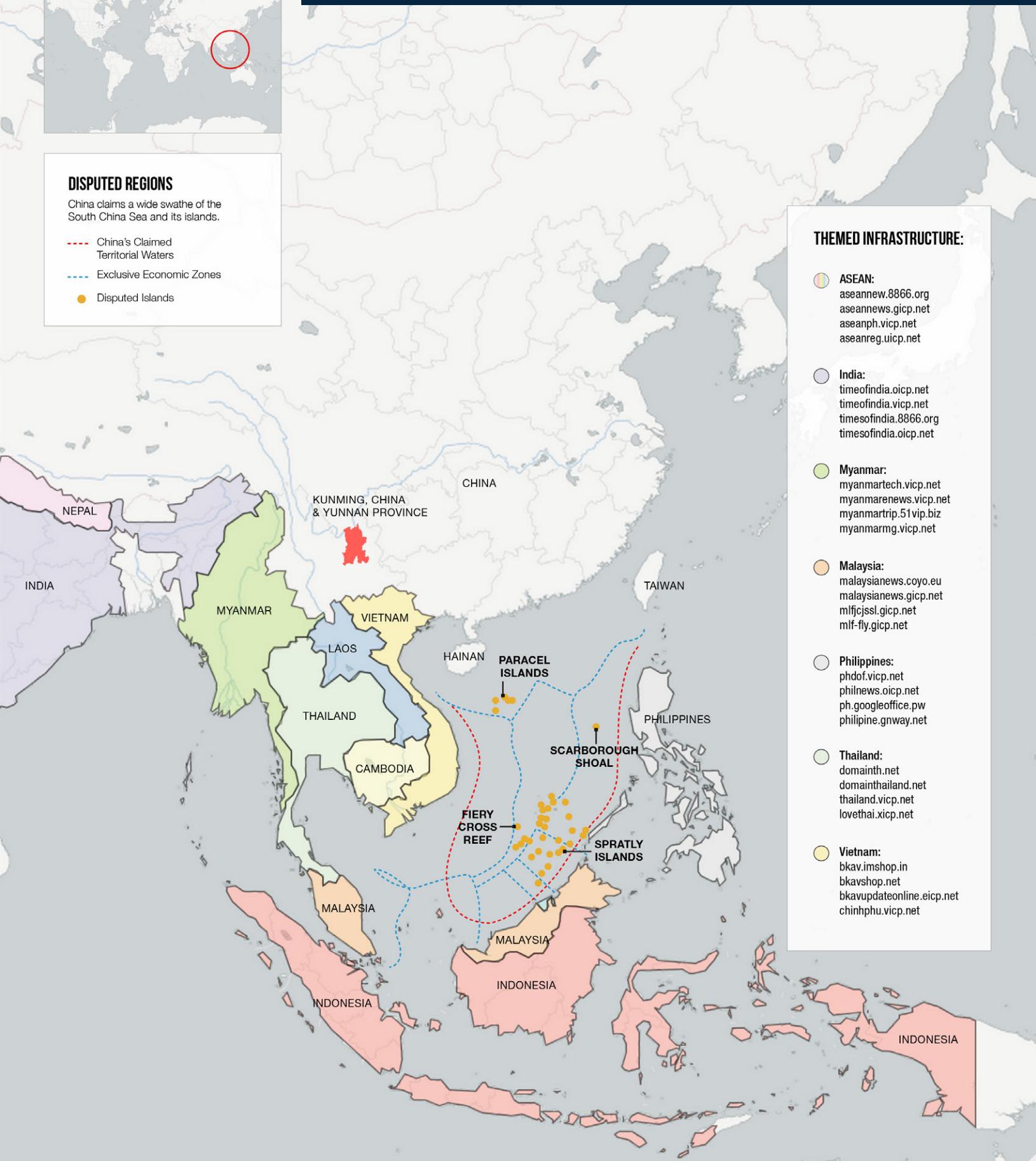
DISPUTED REGIONS

China claims a wide swathe of the South China Sea and its islands.

- - - - China's Claimed Territorial Waters
- - - - Exclusive Economic Zones
● Disputed Islands

NEPAL

INDIA

CHINA

KUNMING, CHINA & YUNNAN PROVINCE

MYANMAR

VIETNAM

LAOS

HAINAN

TAIWAN

THAILAND

CAMBODIA

PARACEL ISLANDS

SCARBOROUGH SHOAL

PHILIPPINES

FIERY CROSS REEF

SPRATLY ISLANDS

MALAYSIA

MALAYSIA

INDONESIA

INDONESIA

INDONESIA

THEMED INFRASTRUCTURE:

ASEAN:
aseannew.8866.org
aseannews.gicp.net
aseanph.vicp.net
aseanreg.uicp.net

India:
timeofindia.oicp.net
timeofindia.vicp.net
timesofindia.8866.org
timesofindia.oicp.net

Myanmar:
myanmartech.vicp.net
myanmarenews.vicp.net
myanmartrip.51vip.biz
myanmarmg.vicp.net

Malaysia:
malaysianews.coyo.eu
malaysianews.gicp.net
mlfjcjssl.gicp.net
mlf-fly.gicp.net

Philippines:
phdof.vicp.net
philnews.oicp.net
ph.googleoffice.pw
philipine.gnway.net

Thailand:
domainth.net
domainthailand.net
thailand.vicp.net
lovethai.xicp.net

Vietnam:
bkav.imshop.in
bkavshop.net
bkavupdateonline.eicp.net
chinhphu.vicp.net

Leaflet © OpenStreetMap © CartoDB

One of the associated binaries we identified drops a decoy document (a2378fd84cebe4b58c372d1c9b923542[34], a self-extracting executable). This decoy is in the form of a Microsoft Word document containing a Thai language article and pictures from a Royal Thai Navy June 28, 2012 news release[35] depicting Vietnamese fishermen detained for fishing within the Thai exclusive economic zone (EEZ). The decoy content is consistent with Naikon's practice of using topical geopolitical events as bait to interact with malicious files. The primary takeaway, however, is the direct association between various instances of Naikon malware and the greensky27.vicp.net domain. With that connection established, we turn our investigation to the infrastructure behind greensky27.vicp.net.
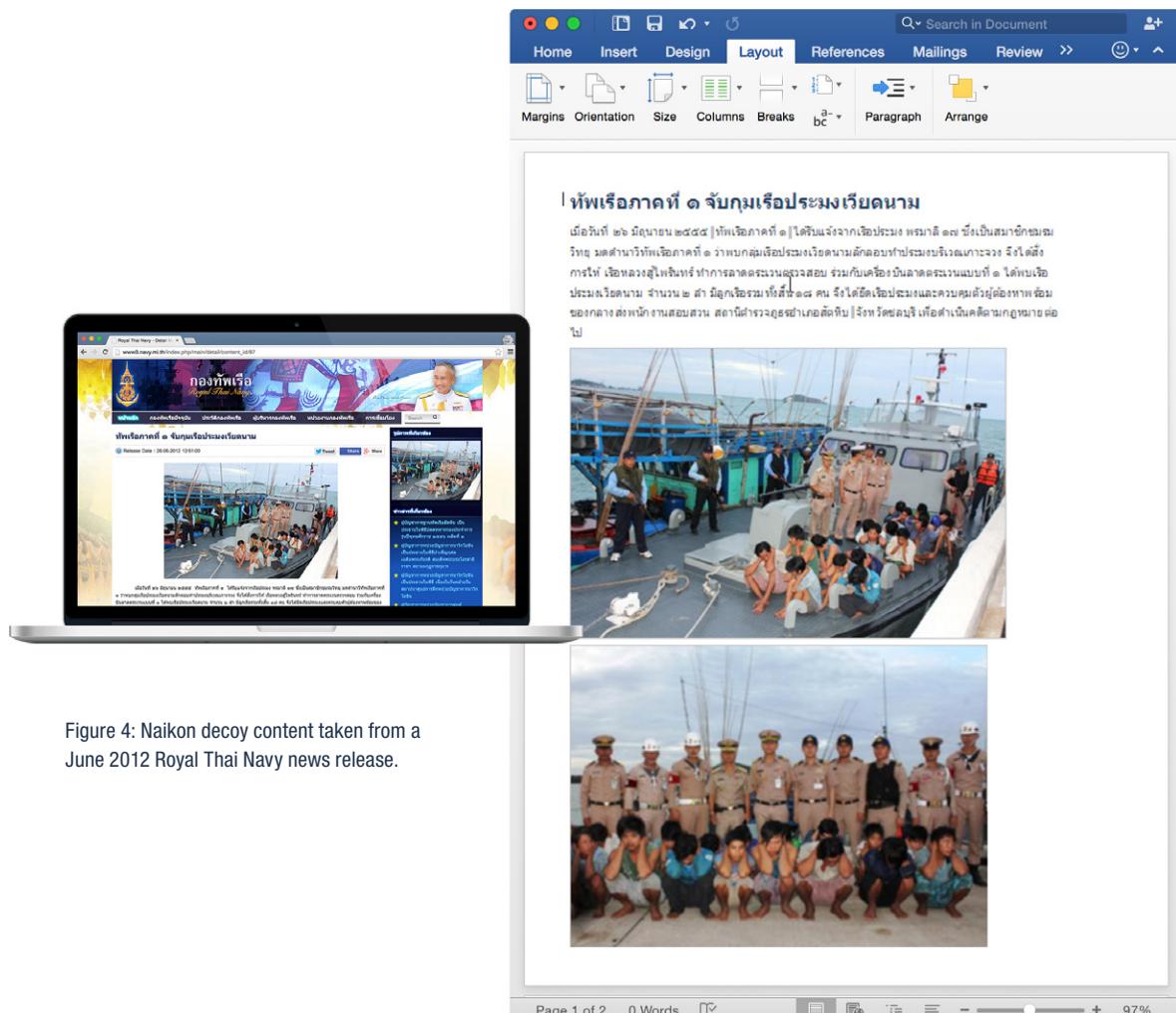
Figure 4: Naikon decoy content taken from a June 2012 Royal Thai Navy news release.

34   https://www.virustotal.com/en/file/7b73bf2d80a03eb477242967628da79924fbe06cc67c4dcdd2bdefccd6e0e1af/analysis/
35   http://www3.navy.mi.th/index.php/main/detail/content_id/87

Domain Infrastructure Analysis

By fusing ThreatConnect's active DNS together with passive DNS data sets, we constructed a timeline of resolutions to the greensky27.vicp.net domain. Activity stretches back to September 2010 and continues up to the drafting of this report in August 2015. Our records show 2,350 resolutions to almost 1,236 unique IP addresses spanning 26 cities and eight countries over that time frame. Figure 5 plots the scope of greensky27.vicp.net autonomous system numbers (ASN) on a world map.

Figure 5: ASNs of IPs associated with greensky27.vcip.net.

The physical geography is both interesting and telling. We immediately see heavy Chinese and Southeast Asian representation, supporting our earlier statements regarding Unit 78020's South China Sea regional focus. There are also a few hosts in the continental U.S. that seem far from the fray but will prove to play a big role as our investigation unfolds. Interestingly, we see no representation from regions often synonymous with financial cybercrime and "rent-a-botnet" fraud schemes such as Eastern Europe.

· · · · · · ·

> We immediately see heavy Chinese and Southeast Asian representation, supporting our earlier statements regarding Unit 78020's South China Sea regional focus.

While Figure 5 shows physical regions of interest associated with greensky27.vicp.net, Figure 6 provides insight into the roles and relationships of the underlying infrastructure.

IMPORTANT DEFINITIONS FOR THIS SECTION

▸ **DNS Resolution:** We use "resolution" or "resolved" in this report in reference to mappings between a domain and an IP address. Each time DNS records show the domain resolving to a different IP address, we count that as a resolution for the purposes of our analysis. We are NOT referring to individual DNS requests or lookups from individual clients. To add variety, we may use generic terms like "switch," "transition," "hop," or "mapping" but all should be understood to refer to the same concept as "resolution."

▸ **Resolution Duration:** We use "duration" to reference the amount of time (in hours) DNS records show the domain resolved to a given IP address before changing to another.
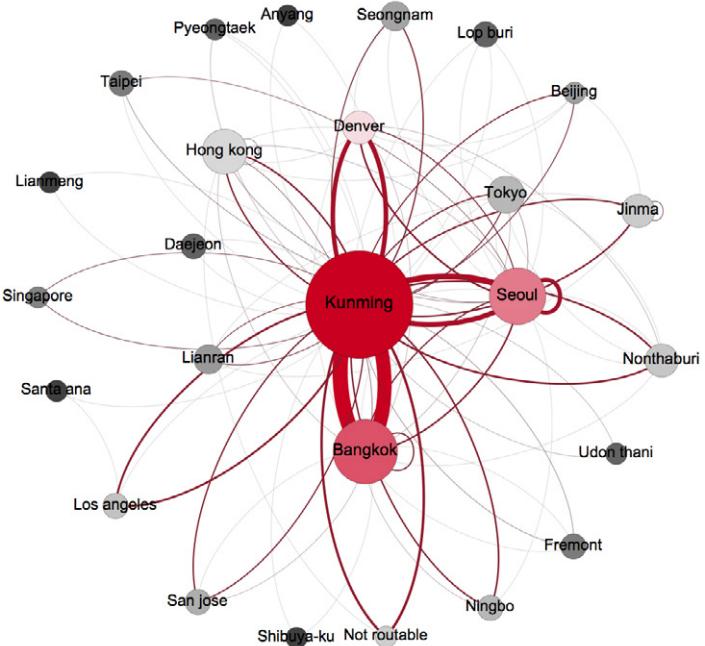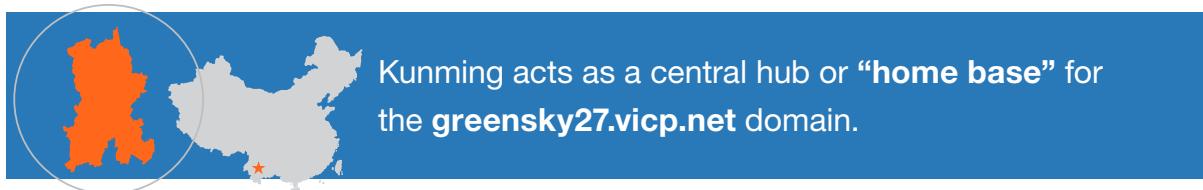
Figure 6: Network graph of IP address locations associated with the greensky27.vcip.net dynamic domain.

The network graph in Figure 6 weighs each location based upon how central it is within the greensky27.vicp.net infrastructure. The dot size coincides with the number of DNS resolutions to IPs in that city. Connecting arcs show DNS records moving between IPs in different cities clockwise from source to destination, and the thickness of the arc captures the relative frequency of these transitions. There are several conclusions we can draw.

1. **Nearly all roads lead to Kunming.** Of the 27 cities identified, 22 show DNS resolutions into Kunming and 23 resolve out. **No other city exhibits even half this number of connections** (Bangkok comes closest at 11 in and nine out). Thus, we infer that **Kunming acts as a central hub or "home base" for the greensky27.vicp.net domain.**

2. Bangkok, Seoul, Hong Kong, and Denver are also important. They exhibit recurring interactions with other nodes in the network, albeit not as heavy as Kunming. As later analysis will demonstrate, each of these nodes serves a very unique purpose within the operator's infrastructure.

3. There are many nodes with very few connections. Many transition only to one of the more central nodes mentioned above. While the network-graphing algorithm may not see them as "important," they still serve key mission-specific functions. These too will be discussed later.

Kunming acts as a central hub or **"home base"** for the **greensky27.vicp.net** domain.

ANALYSIS OF RESOLUTION METRICS

We used two observable measures – the number of DNS resolutions and the duration of each resolution – to study the greensky27.vicp.net infrastructure and how the adversary uses it to support their mission. Additional contextual information (e.g., geolocation, ASN) or derivative metrics (e.g., total time or hops within a city) also factor into our analysis but build upon those two base metrics. Distributions specific to these measures can be found within Figures 7 (resolutions) and 8 (durations) below.


50% IPs used only once
83% IPs used twice
99% IPs used < 3 times
Maximum usage of an IP: 51 times
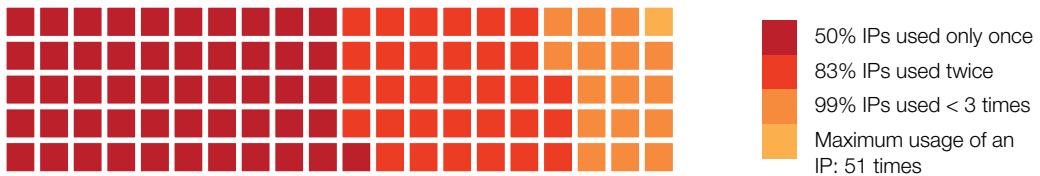
Figure 7: Distribution for number of resolutions per IP address.

25% < 1 Hour
60% < Work Day
80% < 1 Day
95% < 2 Days
99% < 1 Week
Max: 2 Months 10 Days
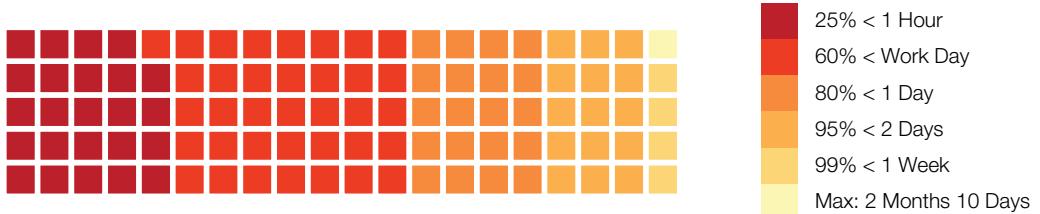
Figure 8: Distribution of resolution durations (in hours).

Both figures point to the dynamic nature of the greensky27.vicp.net domain. In Figure 7, about half of the IP addresses recorded only one resolution over the five-year time frame, and less than one percent tallied more than three. An extreme few racked up dozens of DNS records. Figure 8 reveals that while some resolutions persist for months, approximately 80 percent last less than a day. About a quarter remain bound to an IP address shorter than an hour. These findings beg for further inquiry into hosts that, statistically speaking, stand out from the rest. From a network defense perspective, this also reminds us of the **limited utility of playing "whack-a-mole" with IPs**, calling instead for more effective methods of identifying, sharing, and blacklisting malicious infrastructure on the Internet.

• • • • • • •

From a network defense perspective, this also reminds us of the **limited utility of playing "whack-a-mole" with IPs**, calling instead for more effective methods of identifying, sharing, and blacklisting malicious infrastructure on the Internet.
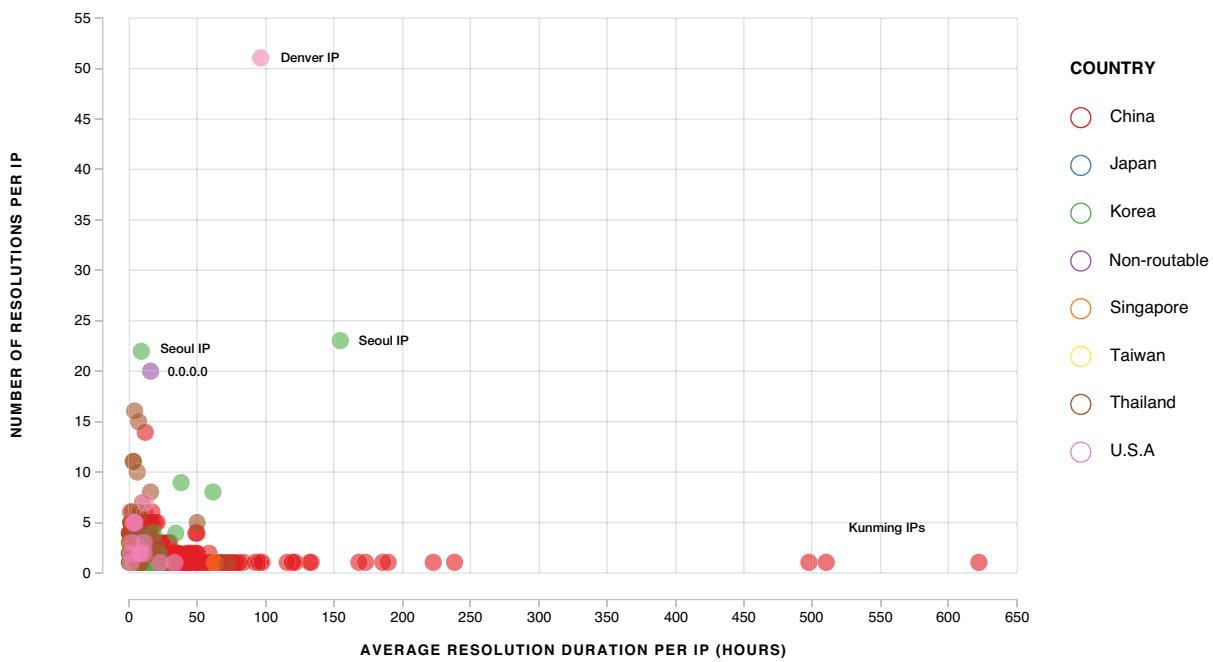
Figure 9: Average resolution duration vs. number of resolutions per IP.

With the goal of spotting outliers for further investigation, Figure 9 plots all IP addresses associated with greensky27.vicp.net on a coordinate plane. The x-axis represents the average duration of a resolution to an IP address and the y-axis represents the total number of DNS resolutions pointing to that IP. Most IPs share similar characteristics, clustering in the lower left. Interestingly, the most distant outliers represent three different cities in three different countries, each of which vary dramatically in their resolution-duration orientation. Rather than speculating on this, we will take it at face value for now and simply follow the data's lead into a city-centric analysis.
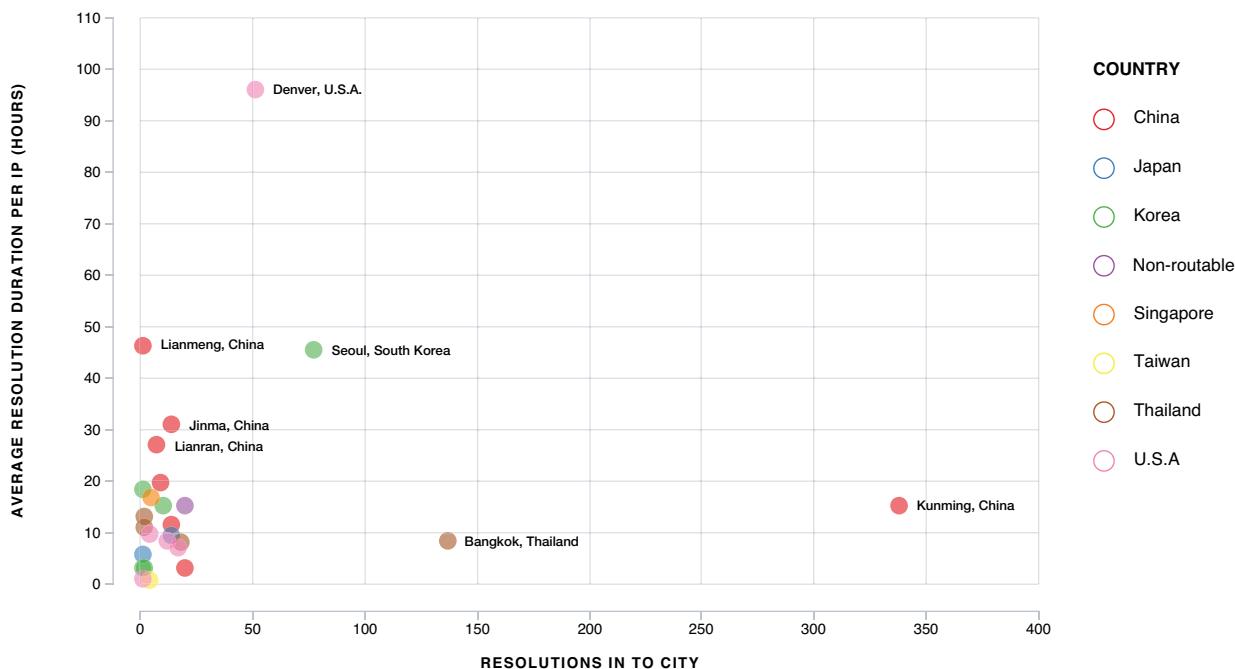

Figure 10: Resolutions into city vs. average resolution duration.

Figure 10 replots Figure 9, using instead the total number of resolutions to a city[36] versus the average resolution duration. It further strengthens the case for Kunming, Seoul, Bangkok, and Denver as major cities of interest in terms of understanding the context and role of the greensky27.vicp.net infrastructure. Building on this, Figure 11 gives a more detailed comparison of resolution metrics among these and other important cities identified in our analysis.
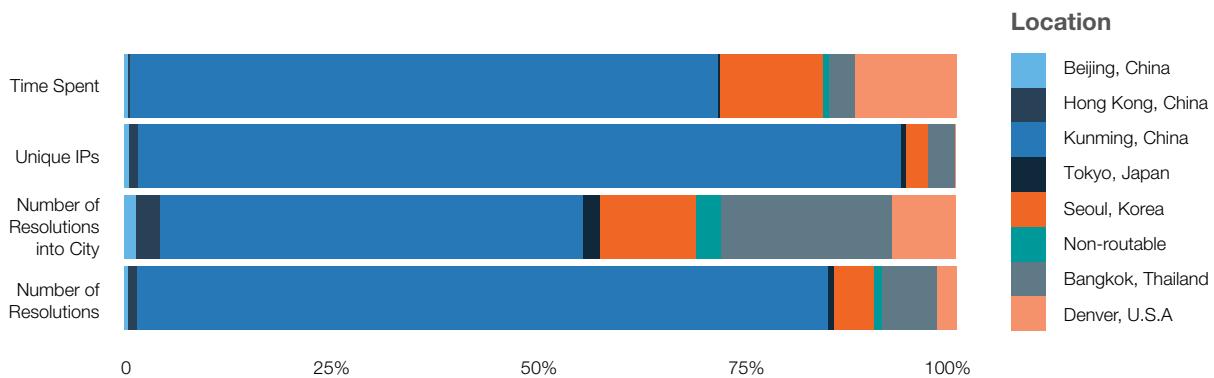

Figure 11: Resolution metrics per city.

The variation exhibited among cities in Figure 11 is readily apparent. **Kunming, home of Unit 78020, dominates everything, showing once again that it is the center of life, the universe, and everything** insofar as greensky27.vicp.net activity is concerned.[37]

The adversary resolves within Kunming more often, transitions between Kunming IP addresses, spends more overall time, and seemingly "owns" more infrastructure in Kunming than any other geography by far. Denver, on the other hand, stands a mile high above the rest in its own unique way. Denver's single IP address boasted average durations more than six times that of Kunming and more than double its next-closest competitor, Seoul.

· · · · · · ·

> Denver's single IP address boasted average durations more than six times that of Kunming and more than double its next-closest competitor, Seoul.

Seoul and Bangkok show similar profiles, except a lot more time was spent in the former. It is difficult to discern much about the other cities from this view, but the next visualization fixes that.

Figure 12 shows the proportionality for our resolution metrics relative to all cities associated with the greensky27.vicp.net domain. It provides a city-centric perspective rather than the metric-centric one seen in Figure 11. This alleviates the Kunming predominance and lets us compare cities on more even footing. All factors being equal, the ratio of resolutions to IPs to duration should be roughly the same across cities. Instead, the ratios vary dramatically, which makes these findings very intriguing. We performed statistical significance tests on the domain resolution data and confirmed the apparent differences among cities to be legitimate.[38] We therefore conclude these observations are meaningful rather than a mirage of random variations in the data. But what, exactly, do they mean?

· · · · · · · · · · · ·
36   This does not include subsequent intra-city IP hopping. We chose to omit these to better show resolution movement between cities in this figure. Otherwise, total resolutions to Kunming IP space would literally be off the chart.
37   *Hitchiker's Guide* fans will be interested to know it's also home to TRB sub-unit 42 (true statement).
38   We compared resolution metrics among cities using One-Way Analysis of Variance (ANOVA). The test yielded extremely significant results with a p-value of 1.71E-19.
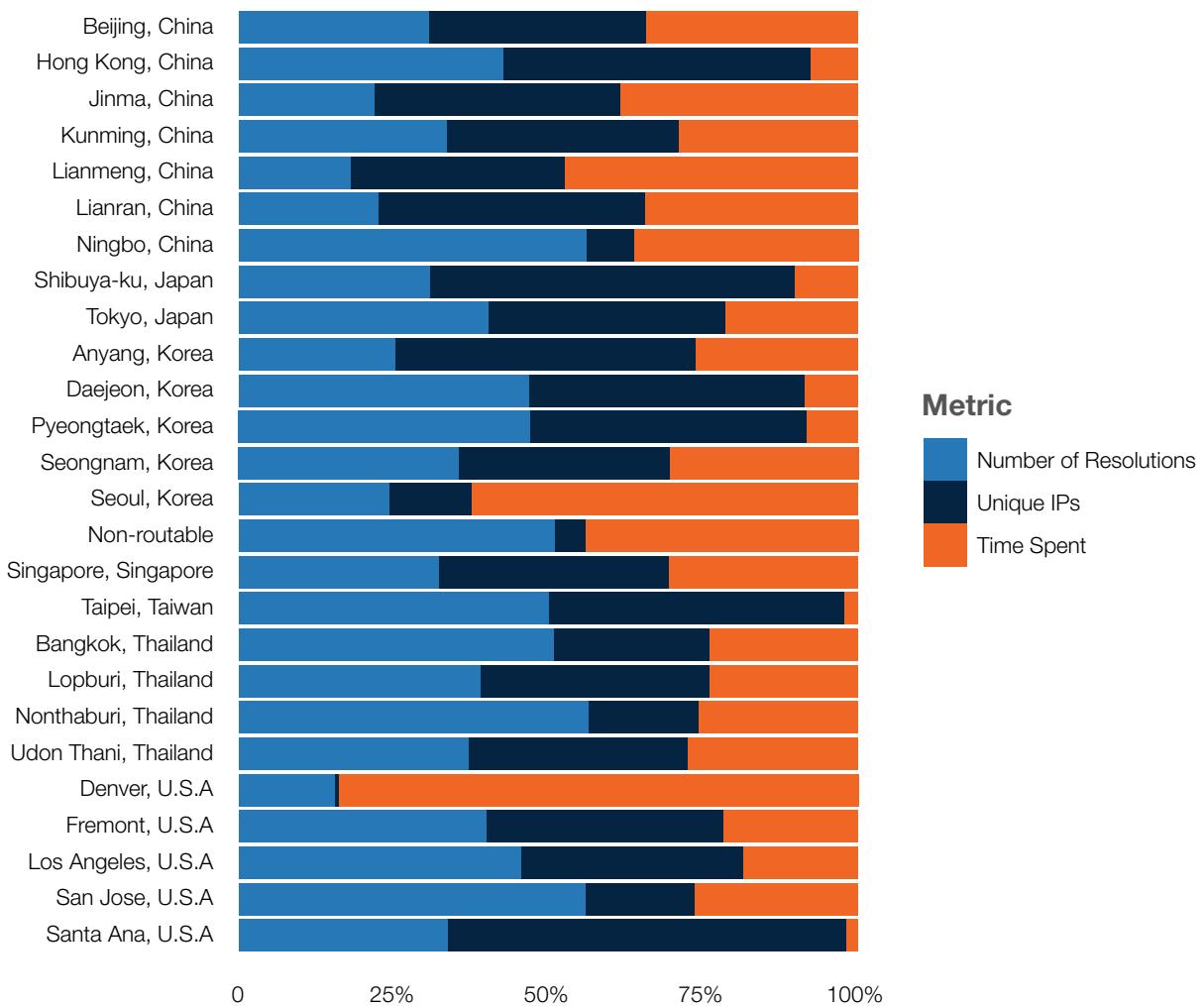
Figure 12: Ratio of resolution metrics relative to each city.

INFRASTRUCTURE AND LOCATION PROFILES

We hypothesize varying ratios among resolution metrics reflect the location's purpose and function within the larger infrastructure or campaign. A high ratio of resolutions for a given location reveals levels of access, control, and comfort. A cautious and wary adversary probably would not resolve into or within high-risk areas repeatedly over a long period of time. Instead, comparatively frequent resolutions hint at a kind of safe and familiar routine.

A heavy skewing of unique IPs corresponds to regional investment and/or control. Having a large pool of single-use hosts within a region means infrastructure is easy to come by and suggests a high degree of ownership with low attachment to individual hosts. Conversely, locations with only one or two IPs and frequent resolutions over several years indicate strategic importance and value at both the host and location levels.

When the ratio of time resolved is comparably higher than the number of resolutions or unique IPs, it shows the adversary has the motive and means to keep the domain static for long periods of time. Chapter Four provides examples of why an adversary might do this.

From our analysis of the infrastructure behind greensky27.vicp.net, we infer three general infrastructure patterns or profiles:

LOCAL IP SWITCHING

Kunming falls squarely in this camp, with a huge number of fleeting resolutions to single-use IPs throughout the five-year time frame. This suggests a deep relationship between the adversary and the city of Kunming, and it may also indicate a lack of operational security or oversight. We surmise the person controlling the greensky27.vicp.net domain likely lives in or near Kunming and has installed the Oray Peanut Shell client, which automatically obtains Kunming-based IP addresses from the local service provider's address pool when his VPN connection is not active. This is not dissimilar to someone's laptop automatically grabbing new IP addresses as they move between home, office, coffee shop, etc.

REMOTE COMMAND/CONTROL (C2)

Another pattern to note is brief, periodic resolutions to recurring IPs in a given location. This pattern accounts for a majority of non-Chinese cities. This phenomenon is likely explained as routine intelligence collections on targets in the South China Sea region. The actor connects to suborned hosts for traditional remote C2 and exits after acting on the objective. We estimate the more hasty exits may simply be a by-product of quick connectivity checks to see if victims are beaconing in. Alternatively, the actor may not be experiencing favorable operational conditions. Some examples include network saturation and subsequent latency or the C2 IP address being blocked, forcing the actor to transition to a different C2 to reacquire access to the victim implant(s).

DOMAIN PARKING

Patterns observed in Denver, Seoul, and non-routable (0.0.0.0) suggest they are likely used when the greensky27.vicp.net domain is either offline for a given time or not interacting with routable infrastructure.

Patterns observed in Denver, Seoul, and non-routable (0.0.0.0) suggest they are likely used when the greensky27.vicp.net domain is either offline for a given time or not interacting with routable infrastructure. They are the only locations where total time resolved is disproportionately higher than unique IPs and resolutions. Seoul serves as a mixed bag where some of Seoul's multiple IPs are most likely used for adversary domain parking, while others appear to be traditional remote C2 hosts. Figure 13 drives this point home visually by splitting out ASNs in Seoul. ASN 10036 exhibits more of a C2 profile, while ASN 3786 closely mimics the parking pattern.
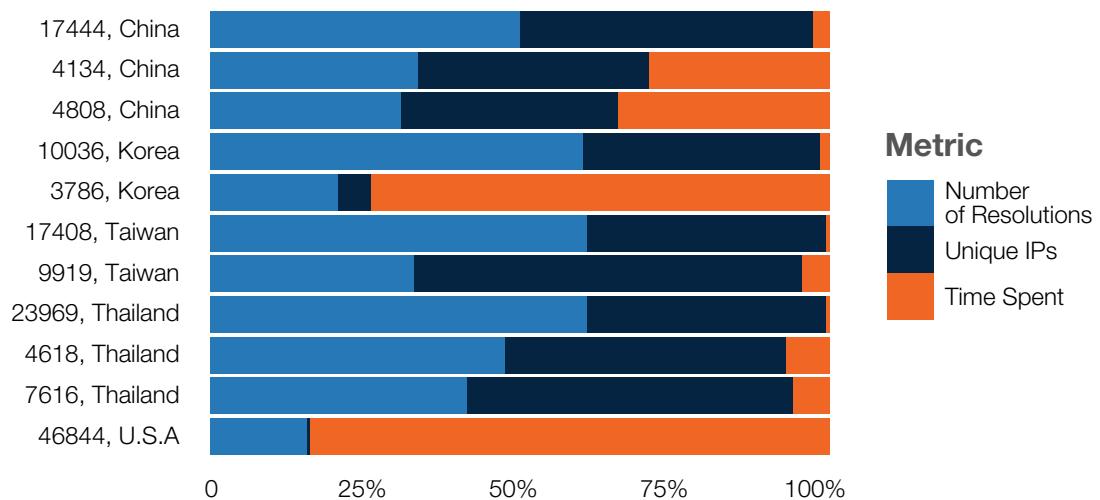
Figure 13: Ratio of resolution metrics relative to selected ASNs.

To test our hypothesis, we ran another statistical test[39] comparing the resolution metrics of Denver and Seoul. The results showed no significant difference between the two cities, which we would expect if both truly do share similar profiles. To take this one step further, we incorporated "non-routable" resolutions (which we know to be adversary domain parking) into another test,[40] which also found no significant differences. This provides statistical confirmation that patterns in Denver and Seoul mimic parking of one form or another. So as to not offend the "it's easy to lie with statistics" crowd, we took a calculated opsec risk and (after some due precautions) simply browsed to the Denver IP address and greensky27.vicp.net to test this. Figure 14 is what we found. This confirmed our suspicions that the greensky27.vicp.net domain will point to an IP address belonging to a Denver service provider when the user is logged out of the Oray Peanut Shell client. Those curious as to "why Denver?" are referred to Appendix D: Oray Infrastructure for further information.

. . . .

39   We used a t-test since we are comparing differences between two groups rather than three or more.
40   Back to ANOVA this time because we have three groups: Denver, Seoul, and "non-routable."

Figure 14: Browser screenshot when attempting to resolve greensky27.vicp.net and Denver IP address 174.128.255.229.
Translation: "We are very sorry, the Peanut Shell Dynamic Domain greensky27.vicp.net is not online. Please wait a while, and try again!"

THE BIG PICTURE IN MANY PIXELS

A normal picture might be worth 1,000 words, but Figure 15 is worth at least 2,000—the word count so far in this section used to analyze the greensky27.vicp.net infrastructure. It shows all of the IPs that the greensky27.vicp.net domain resolved to over a period of five years and brings everything we learned home in one (beautiful) shot.
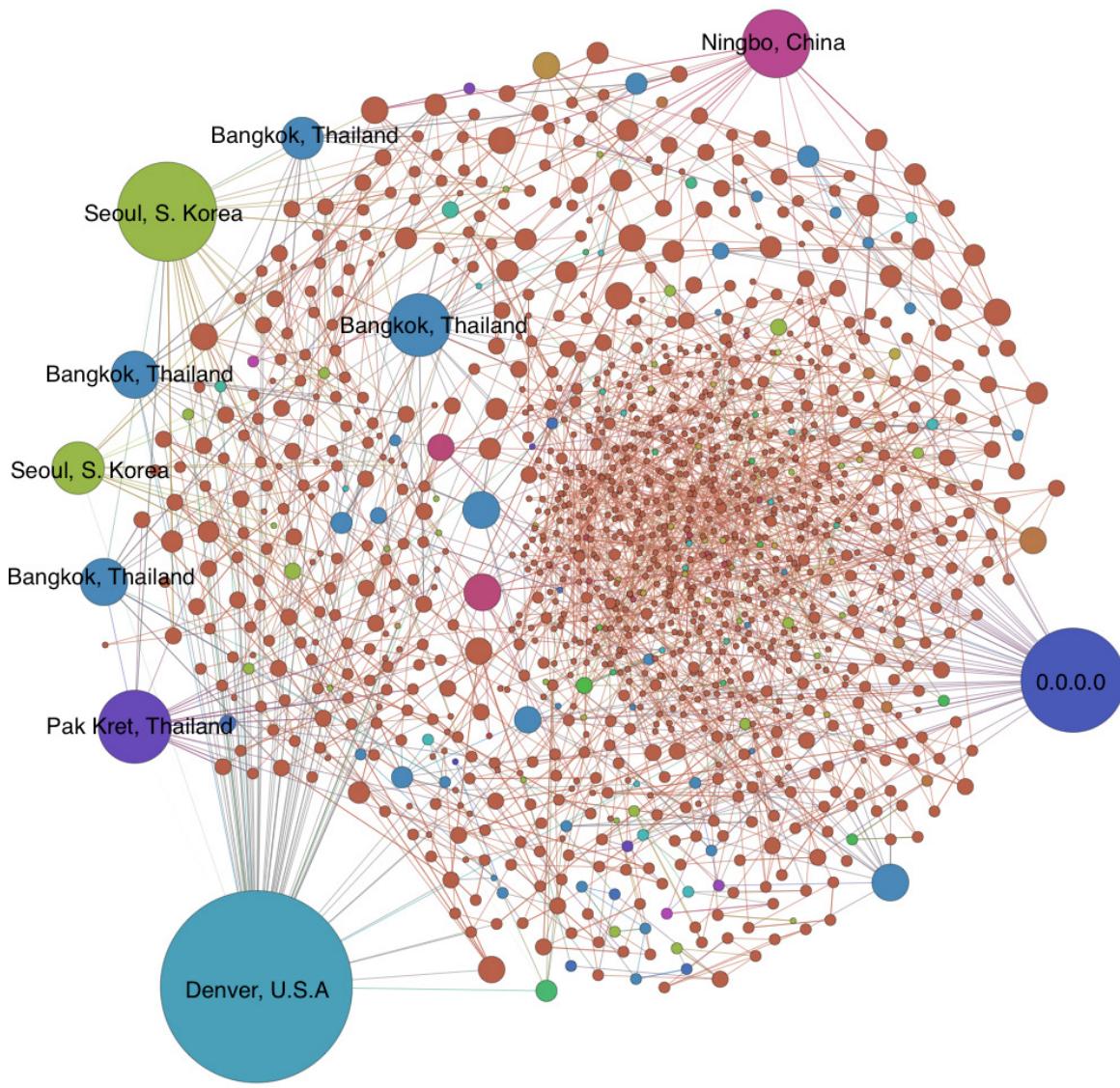

Figure 15: Network graph of all IP addresses associated with greensky27.vicp.net.

A few nexus nodes stand out in bright contrast to the field of lesser hosts. The three profiles discussed above are readily apparent. The largest dots are the parking/offline IPs of Denver, Seoul, and 0.0.0.0 i.e. not routable. The dense section of tiny specks in the middle is clearly the fast and fleeting local Kunming switching infrastructure. Other slightly larger, but still small, dots of the same color likely fall in that pattern too, but they were used a bit longer or more often than the pure burner IP addresses. The other small- to medium-sized, middle-layer nodes form the collections infrastructure, most of which are C2 hosts located in target countries in the South China Sea region. **Thailand appears particularly prominent among C2 infrastructures in Figure 15, a fact that suggests it may be the focal point of adversary collections activities.**
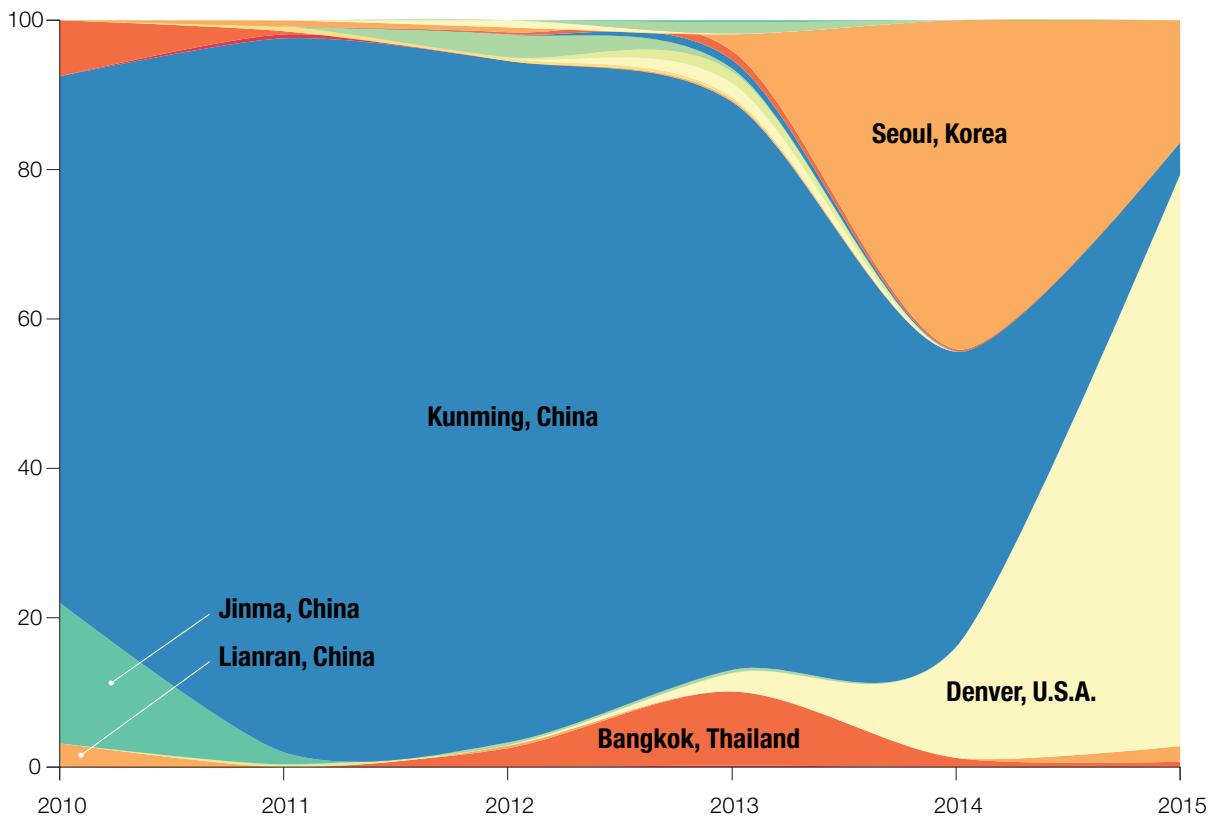
Figure 16: Stream graph of relative resolution duration per city over time.

Figure 15 is good enough to end on, but one final topic deserves mention before closing out this section. Figure 16 presents a stream graph for the relative percentage of time greensky27.vicp.net was bound to IPs in each city respectively over the time frame of study. A possible storyline emerges from the visualization that goes something like this:

Switching around Kunming and surrounding suburbs dominated the first two years, possibly the early days of the adversary's career, mission, or the campaign itself. 2012 marks a two-year rise in foreign collection activities, focused largely in Thailand and Korea. As collections dwindled (either because the mission was completed or cut short), the adversary increasingly parked the domain in Seoul before taking it offline with increasing regularity with a service provider in Denver where it remains at the time of this writing. Whatever the correct interpretation, there is clearly an important temporal – and perhaps human – aspect to the infrastructure worthy of further examination. To that end, we will now turn to the man behind the GreenSky curtain.

· · · · · · ·
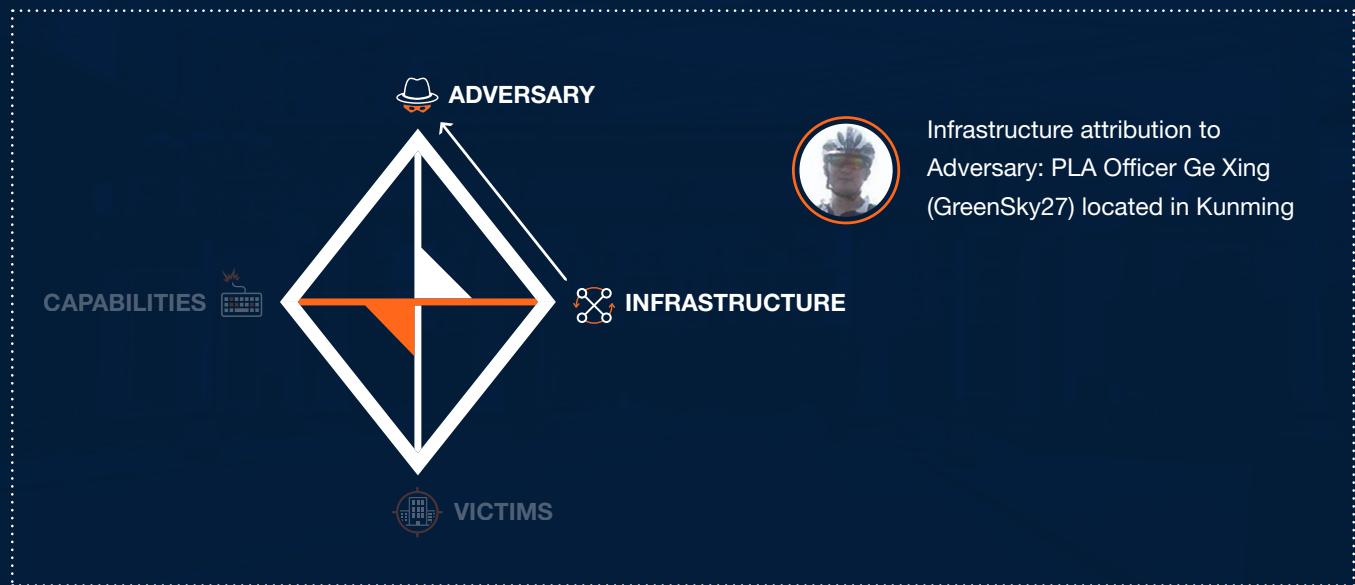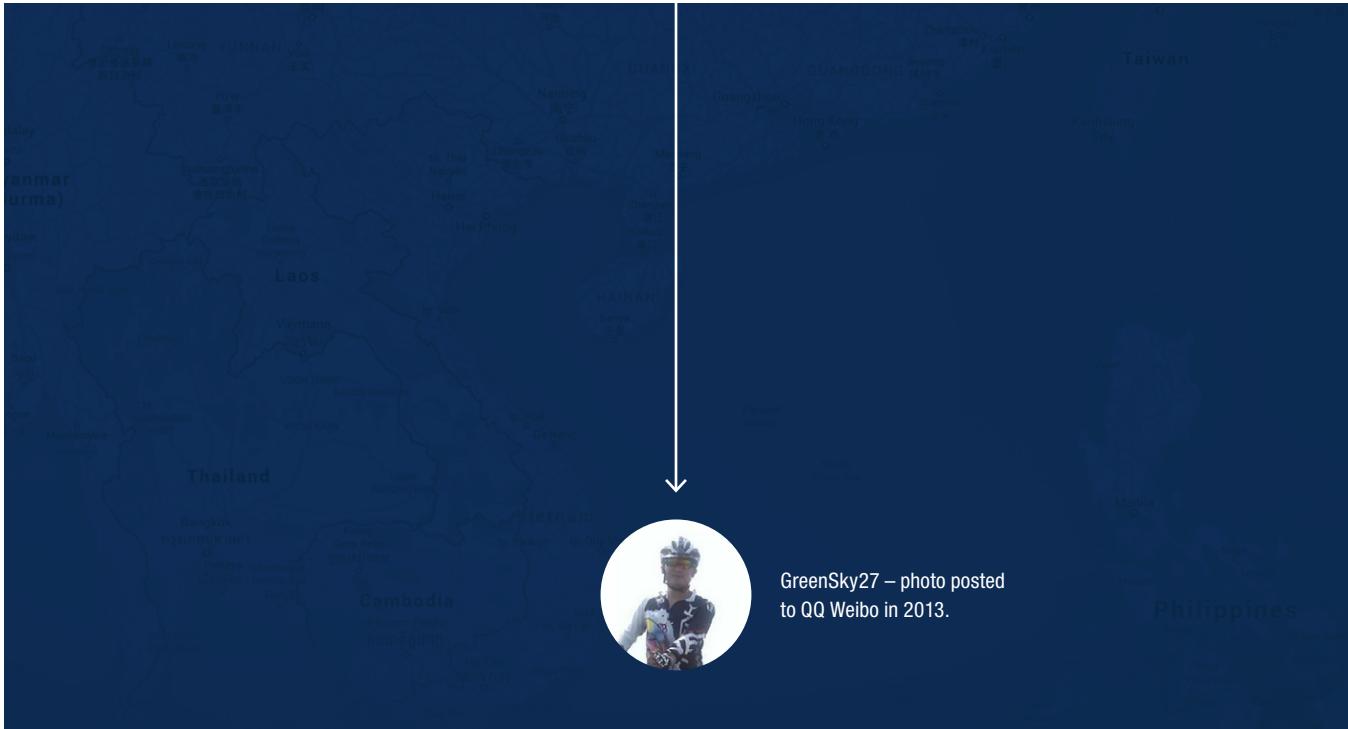
Whatever the correct interpretation, there is clearly an important temporal —
and perhaps human — aspect to the infrastructure worthy of further examination.
To that end, we will now turn to the man behind the GreenSky curtain.

CHAPTER 3
MEET 78020'S GE XING A.K.A. "GREENSKY27"

Infrastructure attribution to Adversary: PLA Officer Ge Xing (GreenSky27) located in Kunming

GreenSky27 – photo posted to QQ Weibo in 2013.

Similar to the way Chapter Two profiled the greensky27.vicp.net infrastructure, this chapter will seek to identify and profile the adversary controlling it. We have connected Naikon infrastructure to a PLA officer named Ge Xing with Unit 78020 through open source native language research. This section establishes "GreenSky27" as a username for Ge Xing across several social media accounts dating back to 2004 and places him in Kunming from content he publicly posted to the Internet. Furthermore, we document Ge Xing's ties to Unit 78020 (Naikon) through his publications and photos he took from within the unit's compound.

The personified greensky27.vicp.net dynamic infrastructure stood out amongst C2 domain names used by the Naikon APT due to its frequent resolution to hosts located in the Kunming, Yunnan Province and its strong correlation with Naikon malware likely directed against Southeast Asian entities. Further investigation by DGI's Chinese linguist analysts matched the term "greensky27" to the username GreenSky27, used by a PLA officer named Ge Xing on a personal QQ Weibo account, a Chinese microblogging platform, since July 2010 and on several other Chinese social media platforms since at least 2004.

Figure 17: Summary of linkages and attributes for GreenSky27.

Confirming the Name: GreenSky27 is Ge Xing

Open source research into the term "greensky27" identified numerous accounts on Chinese online forums and messaging platforms that appear to belong to a single account holder located in Kunming summarized in Appendix E: Key Chinese Sources for GreenSky27. Of particular note, a QQ Weibo account with username GreenSky27 contained more than 700 posts and photo albums with more than 500 photographs. The account appears to be actively maintained, with more than 300 followers and content updated as recently as November 2014.[41] By piecing together information from these sources, with the photo-rich QQ Weibo account at the core, we were able to develop a profile of Ge Xing, the PLA Unit 78020 officer behind the username GreenSky27.

....

41   t.qq.com/GreenSky27, accessed July 9, 2015.

Figure 18A: QQ Weibo account with username GreenSky27 contained more than 700 posts and photo albums with more than 500 photographs.
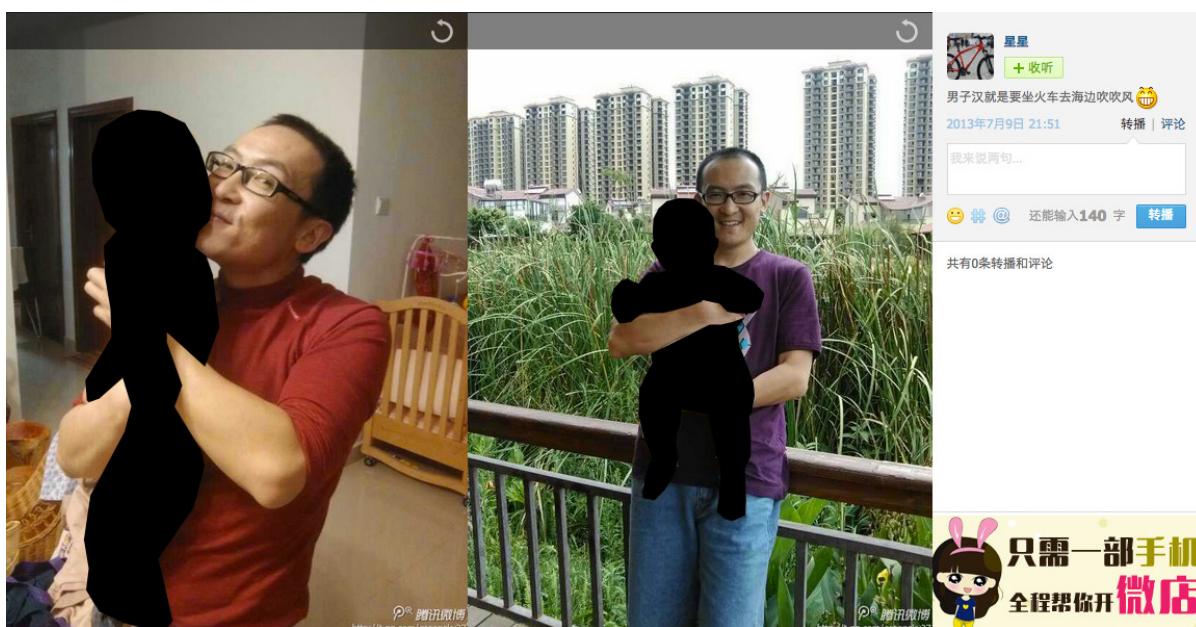

Figure 18B: GreenSky27 – both photos posted to QQ Weibo in 2013 (redacted by ThreatConnect).

Figure 19: GreenSky27, mountain biker, photo posted in 2014.

We determined GreenSky27's true name from references on his QQ Weibo account, third-party website corroboration, and advertisements he posted in Kunming for model airplane parts and mountain bike sales. First, GreenSky27 obliquely reveals his surname through a photo album of his visit to the Ge family's ancestral memorial hall on November 23, 2013. Second, the account screen name which appears at the top of GreenSky27's QQ Weibo profile is Xing Xing (星星, meaning "stars"). While users are not obligated to use a real name when registering for an account, the use of this name suggests GreenSky27's real name may be similar.
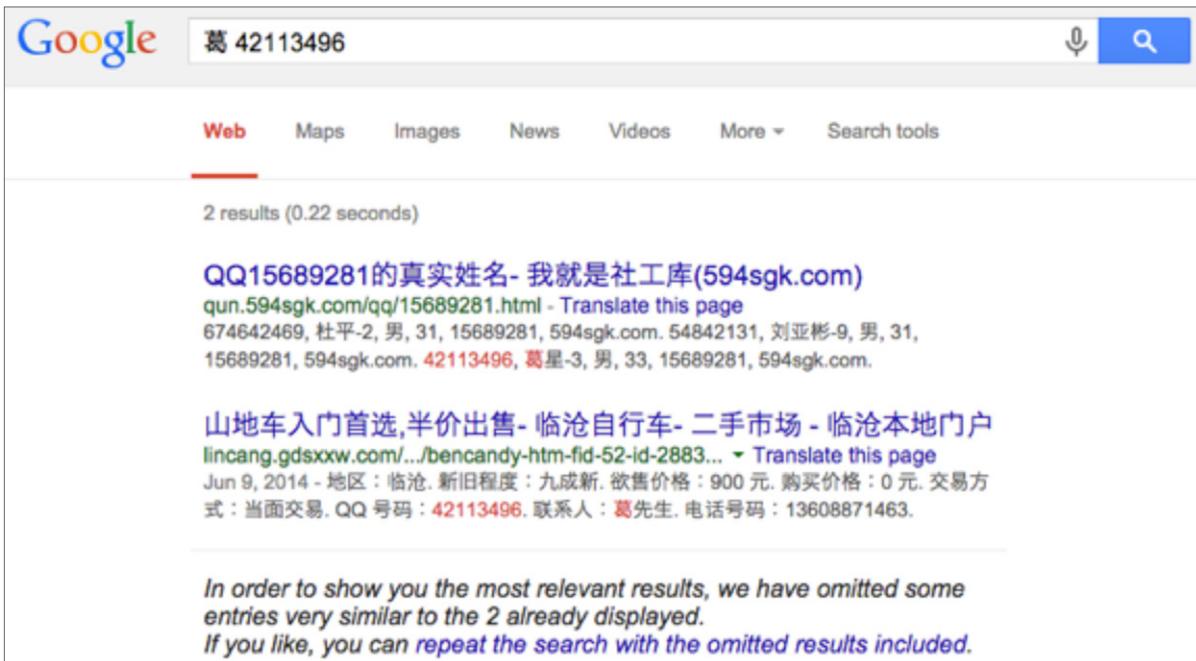
Figure 20: Google search for GreenSky27's QQ account number, 42113496, in combination with the surname "Ge."

A third-party website specializing in identifying the true names of QQ account holders indicates the full name of the GreenSky27 account holder is Ge Xing (葛星). Searches for GreenSky27's QQ account number, 42113496, in combination with the surname "Ge," return a link to the website qun.594sgk.com/qq/15689281.html, which reports Ge Xing as the owner of the account.

Ge Xing/GreenSky27's online presence corroborates this registration information. In 2004, a user named GREENSKY27, located in Yunnan Province, posted a series of advertisements for model aircraft components at the 5IRC.com remote control model forums. One posting included additional contact information, including the QQ address 42113496 and a phone number 13608871463.[42]

Searches for this QQ address and the aforementioned phone number revealed a 2014 post in a local forum for Lincang Township, a suburb of Kunming, advertising a mountain bike for sale with the point of contact "Mr. Ge" (葛先生).[43] This post was no longer accessible, but an image of a mountain bike in the advertisement could still be accessed via a cache of Google Images.[44] The bike depicted in Mr. Ge's sales advertisement is located in the same room in which other mountain bikes are shown in photos on GreenSky27's QQ Weibo page (see Figure 21), corroborating GreenSky27's surname to be Ge.

....

42 http://www.5irc.com/forum.php?mod=viewthread&tid=10476243, accessed July 3, 2015.
43 http://lincang.gdsxxw.com/2shou/bencandy-htm-fid-52-id-28836.html, accessed July 9, 2015.
44 Unfortunately, as of July 9, 2015, neither the image nor the original posting could be found online.
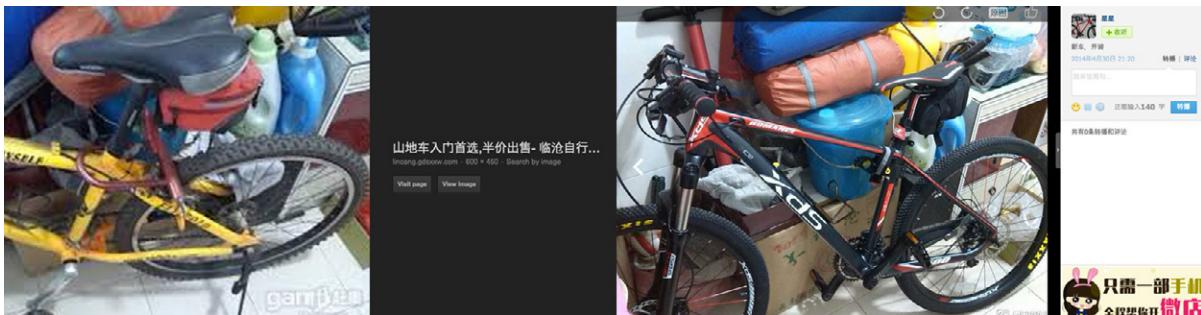
Figure 21: Image of bicycle for sale by "Mr. Ge" in online forums for Lincang Township (left). Image from GreenSky27's QQ Weibo account, showing another mountain bike located in the same room (right).

Finally, the surname Ge is again connected to the GreenSky27 QQ Weibo account by a 2012 post on Baidu Tieba, in which GreenSky27 announces the birth of his child. The November 21, 2012 post, from Baidu Tieba account "greensky27," states: "A [child], surnamed Ge, born November 20, 2012, at 11:36PM: seeking recommendations for a three-character name."[45]

Confirming the Location: Ge Xing is in Kunming

The advertisements described above place Ge Xing in Kunming. Although his QQ Weibo account lists his physical address as Ireland, numerous images uploaded to this account, including his license plate, geolocated bike routes, and photographs of landmarks in Kunming, place Ge Xing in Kunming.

YUNNAN LICENSE PLATE

The license plate attached to Ge Xing's car, a Volkswagen Golf, indicates a Yunnan Province (云南省) registration. The following photo is representative of several pictures depicting the vehicle and rear plate. The Chinese character on the left end of the plate is "Yun" (云), signifying Yunnan, and the letter A signifies Kunming.

Figure 22: Yunnan license plate on GreenSky27's VW Golf.

....

45   tieba.baidu.com/p/1928480963?pn=21, accessed July 9, 2015.

GEOLOCATION THROUGHOUT KUNMING

GPS-traced bike routes shared by Ge Xing on his QQ Weibo profile indicate paths through Kunming. These routes likely were recorded using either a smartwatch or mobile phone application. The following figure shows one of these shared bike routes through the Wuhua District in Central Kunming.
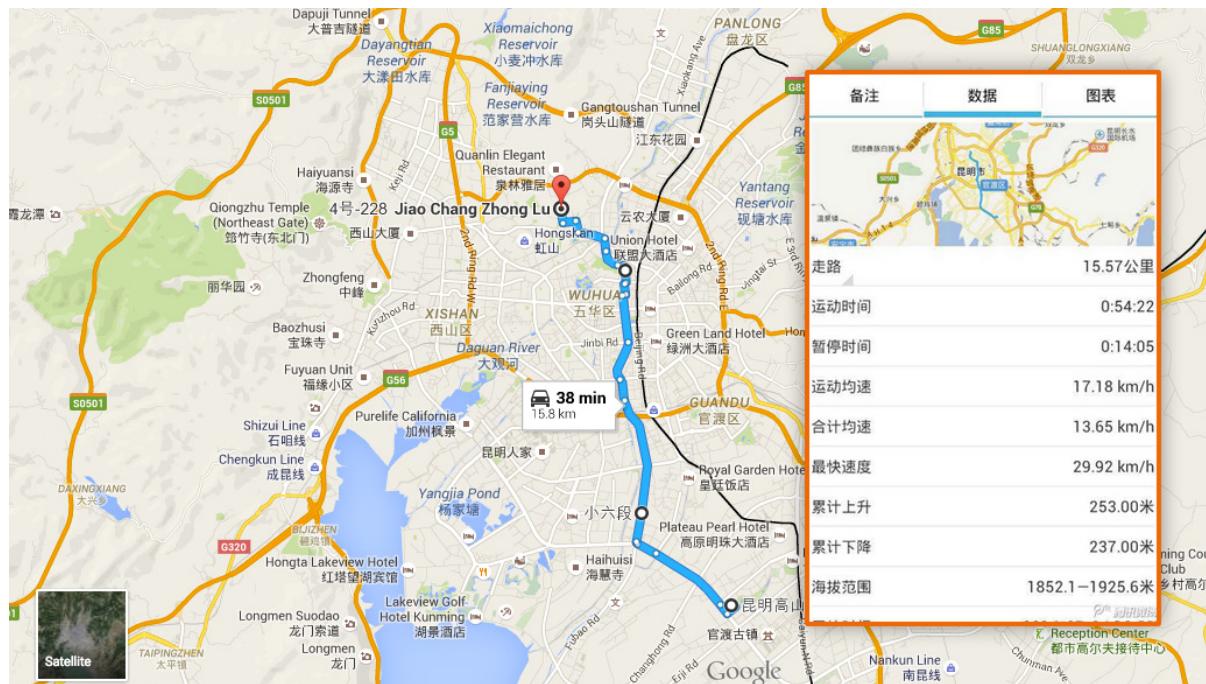

Figure 23: Ge Xing GPS-mapped bike ride through Central Kunming's Wuhua District (五华区) (right). Google Maps recreation of the route shown in background. The route terminates near Jiaochang Middle Road (Jiachang Zhong Lu) (left).

In addition to these bike routes, on one occasion GreenSky27 also used the geolocating application SOSO Map Share (SOSO地图分享) to broadcast his location within Kunming. The image below places GreenSky27 at an address north of Jiaochang West Road, and west of Jiaochang Middle Road, with the caption "Kunming School of Public Health (昆明市卫生学校) (Jiaochang Campus), Yunnan Province, Kunming, Wuhua District, Jiaochang West Road, No. 6." This location is close to the northern terminus of the bike route through the Wuhua District shown above.
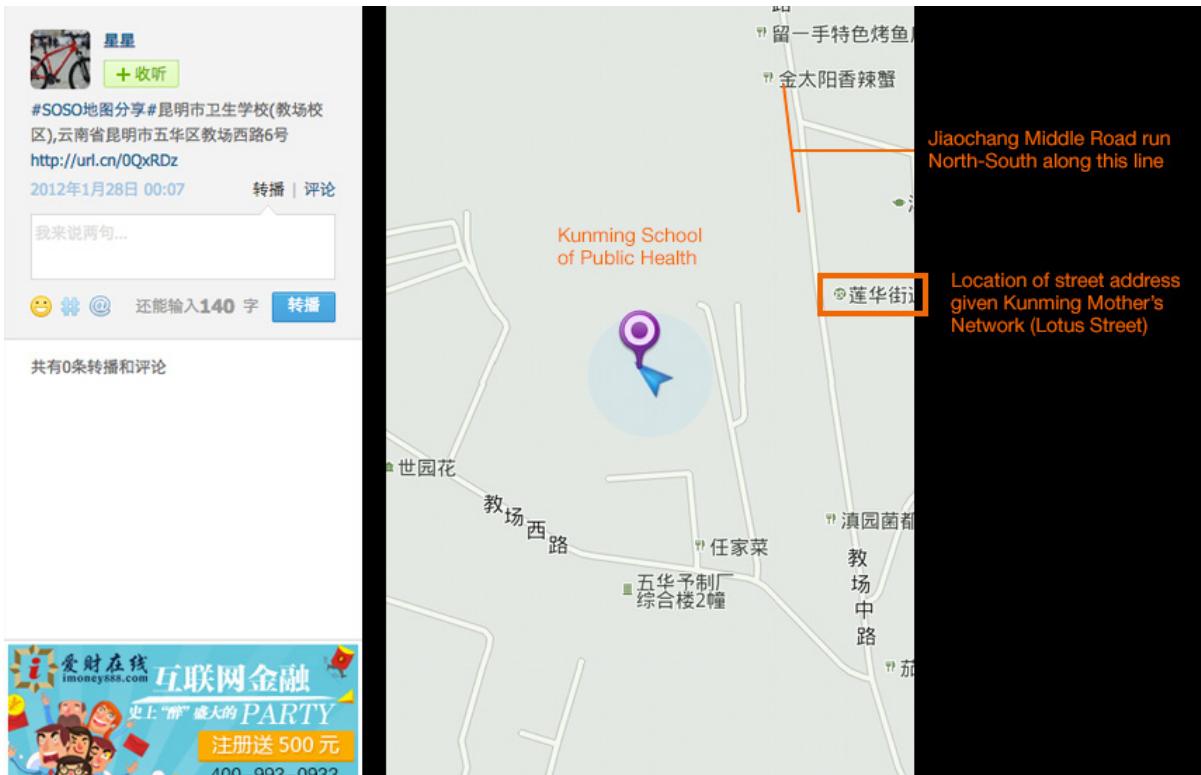
Figure 24A: Ge Xing broadcasting his location near Jiaochang Middle Road and Lotus Street.
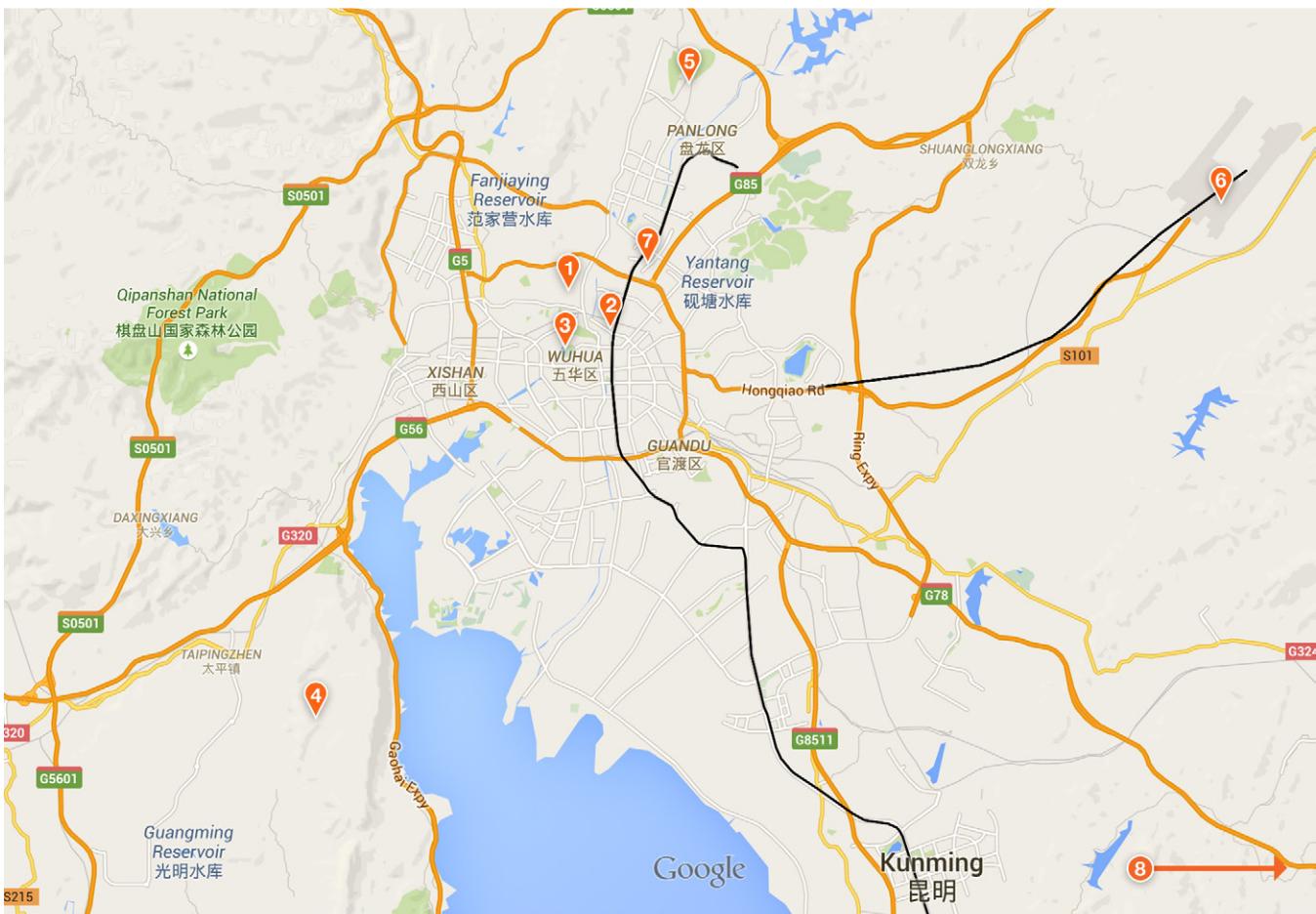
PICTURES TAKEN THROUGHOUT KUNMING

Many of GreenSky27's QQ Weibo photographs depict restaurants, gardens, transportation infrastructure, museums, and other sites in Kunming and its suburbs. The figure below locates a sample of these images on a map of Kunming. The dates of these photos range from 2012 through 2014, reflecting GreenSky27's ongoing residence in the city.

Figure 24B: Ge posted photos that he captioned "beloved party school" (亲爱的党校).

On January 2, 2013, Ge also posted photos that he captioned "beloved party school" (亲爱的党校). Kunming's communist party school (中共昆明市委党校) has multiple campuses, and it is likely Ge had to take a short course at a political academic institution like this one to fulfill a PLA political requirement.

Figure 25: Location of Ge Xing's photographs in Kunming.

1 Kunming School of Public Health 1/26/2012

2 Yunnan Railway Museum 8/2/2014

3 Yunnan Military Academy (historical site) 3/14/2013

4 Miao Miao Qing Cun 8/16/2014

5 Black Dragon Pool 7/13/2013

6 Kunming International Airport 12/28/2013

7 Xindoulongcheng Metro Station 5/12/2014

8 Yiliang Train Station 7/7/2013

GREENSKY27'S PHYSICAL ADDRESS

GreenSky27's physical address is not on his QQ Weibo profile, but an account with username greensky27 and user number 7668760 at the Kunming Mothers Network social networking website (昆明妈妈网) indicates the account holder's street address is Lotus Street Neighborhood, Wuhua District, Kunming, Yunnan Province (云南省 昆明市 五华区 莲华街道).[46]

It is likely the Kunming Mothers Network greensky27 is the same individual as QQ Weibo GreenSky27. Both profiles indicate residency in Kunming. The Kunming Mothers Network account was created in the "newborn infants" section of the website in 2012, and the photographs of GreenSky27's newborn child posted to his QQ Weibo account indicate GreenSky27's child was born the same year. The Baidu Tieba birth announcement for GreenSky27's child likewise was posted in November 2012.

Moreover, the Lotus Street Neighborhood address given by the Kunming Mothers Network account is consistent with location information in the GreenSky27 QQ Weibo account. The image above placing GreenSky27 at the Kunming School of Public Health indicates Lotus Street Neighborhood on the right-hand side of the image, to the east of Jiaochang Middle Road. The maps below show this location within Kunming's Wuhua District.

Figure 26: Location of Lotus Street Neighborhood in Wuhua District, Kunming in proximity to Unit 78020 approximately 0.42 miles.

....
46   http://www.kmmama.com/home.php?mod=space&uid=7668760&do=profile, accessed July 2, 2015.

Ge Xing's Background and Ties to Unit 78020

Ge Xing's longstanding ties to the PLA are apparent from substantial evidence on his GreenSky27 QQ Weibo page and documents available on Chinese-language websites. He launched his career as a PLA officer by attending the PLA International Studies University in 1998. Academic papers written by Ge Xing as a graduate student specifically place him at the Kunming TRB in 2008. Photos from his GreenSky27 QQ Weibo account from 2011 to 2014 place him at the Kunming TRB headquarters compound, underscoring his ongoing connection with the PLA.

ATTENDANCE AT PLA INTERNATIONAL STUDIES UNIVERSITY

GreenSky27's QQ Weibo profile information states that he matriculated at the PLA International Studies University (解放军国际关系学院) in 1998.[47,48] The PLA International Studies University was established in Nanjing in 1961, and the school has a long history of educating PLA officers in international strategy, military foreign relations, and foreign languages.[49] It operates under the General Staff Department, with graduates going on to perform intelligence translation and reporting work, military liaison, or foreign language instruction at military academies.[50] The university also operates a branch campus in Kunming, although it is unclear whether GreenSky27 maintains any association with this branch.

ATTENDANCE AT RECENT PLA EVENTS

Recent photos posted to GreenSky27's QQ Weibo account demonstrate his ongoing relationship with the PLA. A series of photos taken in 2014 shows scenes from a PLA event commemorating the 87th anniversary of the PLA in Kunming. The event appears to be an internal PLA exercise rather than a public event, with only a limited audience at an outdoor firefighting demonstration and name tags and refreshments provided at an indoor lecture.

Figure 27: Ge Xing attends an outdoor firefighting demonstration and a lecture at a commemorative PLA event in 2014. The sign in the second image reads, "Yunnan Province celebrates 87 years of PLA Army Building."

....

47   t.qq.com/Greensky27, accessed July 9, 2015.
48   This report bases the translation "PLA International Studies University" on the *Dictionary of Modern Education* (现代军校教育辞典), National Defense University Press (国防大学出版社), China: Beijing, August 2011, p. 464. Other sources use translations such as the PLA Institute of International Relations and the PLA Academy of International Relations.
49   *PLA Military History*, Encyclopedia of China Publishing House, December 2007, Beijing, p. 679.
50   http://zhidao.baidu.com/question/274704518.html, accessed July 9, 2015.

VISIT TO PLA INTERNATIONAL STUDIES UNIVERSITY IN 2014

GreenSky27's ties to the PLA are reinforced by a series of photos documenting his trip to the PLA International Studies University campus in Nanjing in 2014. The photos show exterior views of several buildings and facilities at the campus. These images do not show any other people, possibly reflecting an impromptu visit by GreenSky27 to his alma mater, rather than an official business tour. Two example images are shown below.

Figure 28: Ge Xing visits PLA International Studies University in 2014.

ACADEMIC PAPERS INDICATING AFFILIATION WITH UNIT 78020

Two research papers identified by searches on the China National Knowledge Infrastructure (CNKI) database of academic journal articles directly link GreenSky27 to the Kunming TRB. These papers, both written in 2008, indicate authorship by a Ge Xing (葛星), located in Kunming, affiliated with PLA Unit 78020. See Appendix F: Ge Xing's Unit 78020 Affiliated Publications for more info.
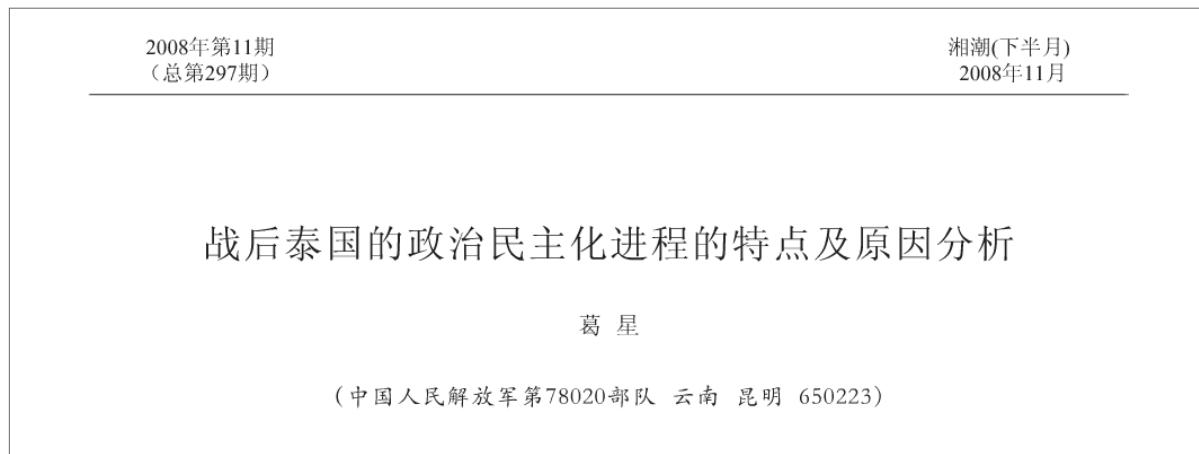

Figure 29: Title and author information for one of the publications written by Ge Xing. The author affiliation line below the name Ge Xing (葛星) reads, "Chinese People's Liberation Army Unit 78020, Yunnan, Kunming, 650223" (中国人民解放军78020部队，云南，昆明，650223). The title of the article is "Examination of Trends in Thailand's Southern Muslim Separatist Movement." The publication date is December 2008.

Both papers discuss politics in Thailand. One paper is entitled "Analysis of Post-War Thailand's Political Democratization Characteristics and Factors" and the other "Examination of Trends in Thailand's Southern Muslim Separatist Movement." The author biographies attached to these papers indicate that Ge Xing was born in 1980 and was pursuing a Master's degree in Southeast Asian international politics at Yunnan University (云南大学) in 2008.

The name Ge Xing, the author's residency in Kunming, and the author's affiliation with the PLA match the information on GreenSky27's QQ Weibo profile. From the model aircraft forum advertisements, we know that GreenSky27 has been located in the Kunming area since as early as 2004, so it is plausible he continued to reside there in 2008. The 1980 year of birth is also consistent with what is known about GreenSky27 from his QQ Weibo profile. It is realistic that a person born in 1980 would enter undergraduate studies in 1998 and become a father in 2012.

PHOTOS PLACING GE XING AT KUNMING TRB HEADQUARTERS

Several of Ge Xing's photos from his GreenSky27 QQ account indicate he has visited Kunming TRB headquarters frequently since 2011. This section leverages Ge's photos by corroborating them with information from Chinese websites, street view imagery from QQ Maps, and satellite imagery from Google Earth. Based on his QQ account, Ge Xing appears to have taken photographs from a hotel on base and three series of photos from the main building on base.
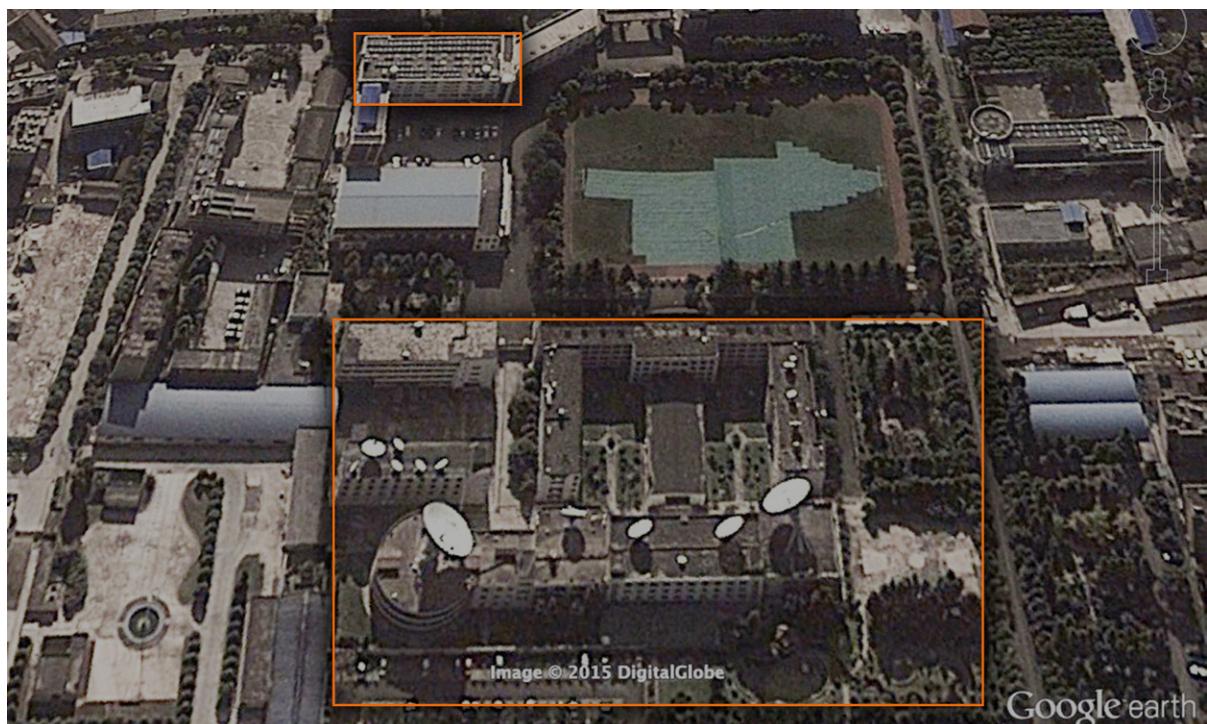

Figure 30: Unit 78020 main building and 020 Hotel outlined.

Photos from Hotel 020 Parking Lot on Base

On December 16, 2013, Ge posted photos from his visit to the 020 Hotel (0二0宾馆), a guest house (招待所) for PLA Unit 78020.[51] According to Chinese websites, this guest house is located at 158 Jiaochang East Road, Wuhua District, Kunming (云南省昆明市五华区教场东路158号), near Kunming General Hospital (25°04'23.2"N 102°42'08.9"E 25.073126, 102.702467).[52] This is the same address identified by Western analysts as the headquarters building for Unit 78020.[53]

Figure 31: Ge Xing's photos of his car parked at the 020 Hotel, posted to the GreenSky27 account.

For this address, QQ Maps censors parts of the entrance and certain individuals in its Streetview. From a vantage point farther away and zoomed in, however, the entrance's features include a red star over the entrance and characters beyond the entrance that are too far to make out.

Figure 32: QQ Streetview imagery of the security entrance to the Unit 78020 compound. The image to the left had been censored within QQ, whereas the image to right was not.

Based on this information we can place Ge Xing in the compound at the hotel. Ge's vantage point is the parking lot facing towards the gate, showing a slanted wall, a reddish gate, and Chinese characters and blue rectangular panels for the Kunming General Hospital.

....

51   http://kunming.youbian.com/huangye/info74049/, accessed July 9, 2015.
52   Ibid.
53   Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute, November 11, 2011.
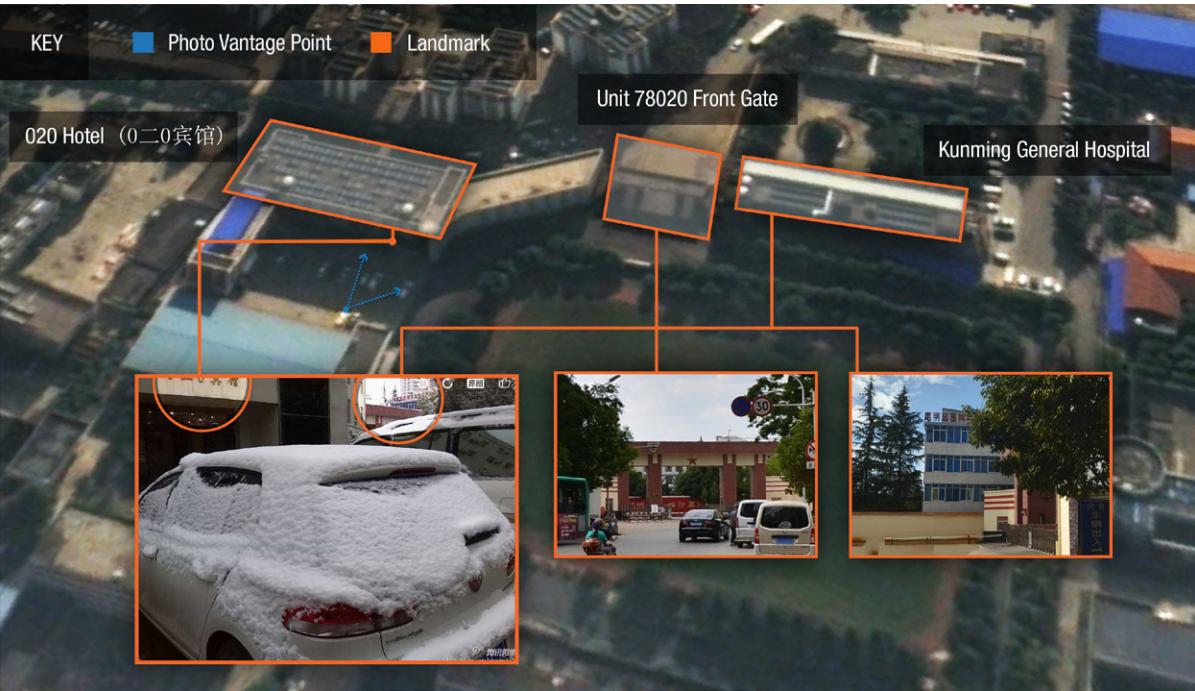
Figure 33: Likely vantage point of Ge Xing when photographing his car in front of 020 Hotel. Within the photograph of the snow-covered Volkswagen, note the characters for 020 Hotel, the red awning of the security entrance, and the red lettering and blue facade of the Kunming General Hospital in the background.

Photos Taken from the Kunming TRB Main Building

Based on Ge's QQ account, he took photos from at least three different vantage points near the Kunming TRB's main building, outlined in the figure above. First is a series of four photos of a tall building with a distinctive roof ornament, taken near a basketball court. Second are photos of a parking lot from within the compound with a distinctive tower in the background. Finally, Ge's QQ account includes a photo of a courtyard from within the compound.

The building from which these photos appear to have been taken is not labeled in open source media, but it stands out as the central structure within the compound. The numerous communications dishes arrayed on its rooftop are consistent with our assessment that it is the Kunming TRB headquarters building.

Figure 34: Overview of Unit 78020's main compound with landmarks and likely vantage points of photos posted to social media.

Photos of Building with Distinctive Roof Ornament

Four images depicting a tall apartment complex topped with a distinctive roof ornament appear to have been taken from the same location over a period spanning from November 2011 to March 2013. All four of Ge Xing's photos appear to have been taken and uploaded at about 8:30 AM on different dates. Regarding the vantage point, one of the images (the first in the sequence above) depicts a basketball hoop and backboard in the foreground, part of a basketball court that is no longer maintained and adjacent to a central building within the Kunming TRB headquarters compound.

Figure 35: Photos from within Unit 78020 of a tall building with a distinctive roof ornament (left). Within one image, a basketball hoop and backboard can be seen (top center).

Parking Lot and a Structure Resembling a Water Tower

Another series of photos sharing a similar vantage point appears to depict a parking lot and several nearby locations within the Kunming TRB compound. These photos appear to have been taken between March and December 2013 from within the central building in the Kunming TRB compound. In Google Earth and on QQ Streetview, there is a structure shaped like a water tower that matches the structure on the right side of Ge Xing's photos.
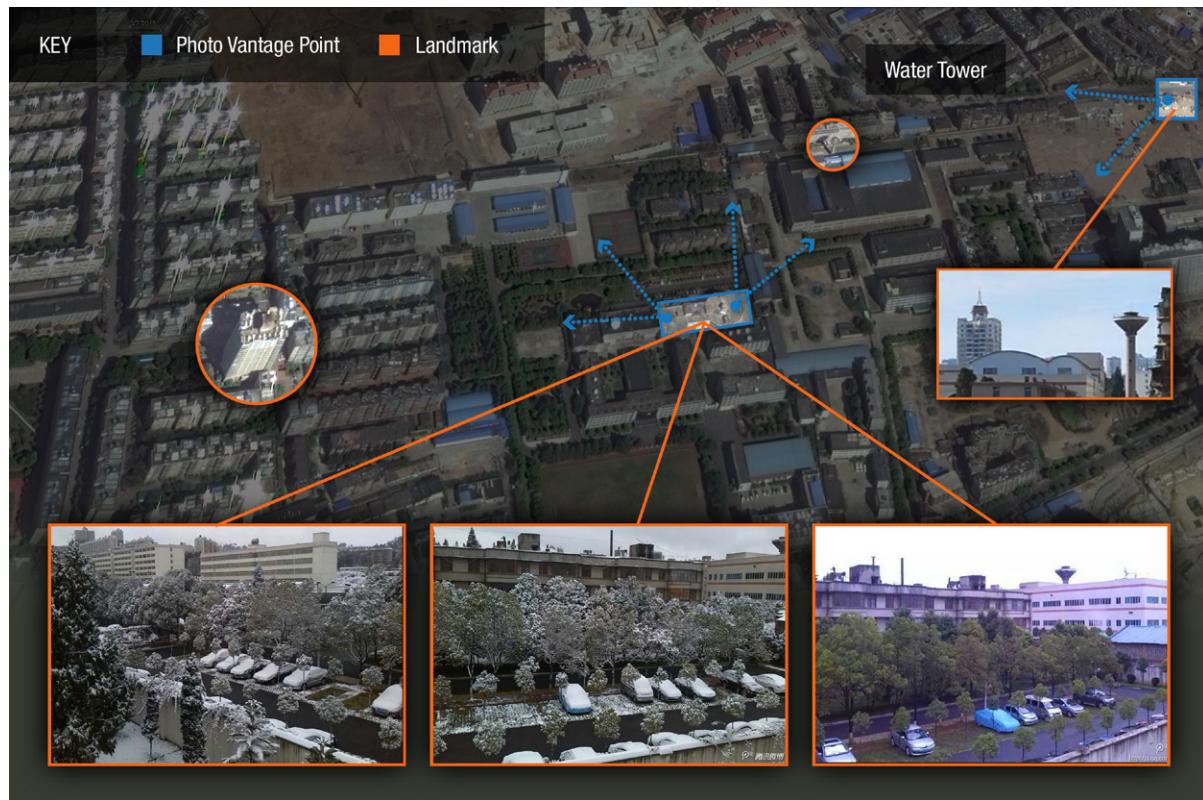

Figure 36: Photos from within Unit 78020 of the parking areas with background landmark of a water tower (bottom three images). QQ Streetview image of landmark of building with distinctive roof ornament and water tower (middle right).

Courtyard Within the Kunming TRB Compound

On September 3, 2013, Ge Xing took a photo of a courtyard, the pattern of which matches the two courtyards in the middle of the main building for the Kunming TRB.
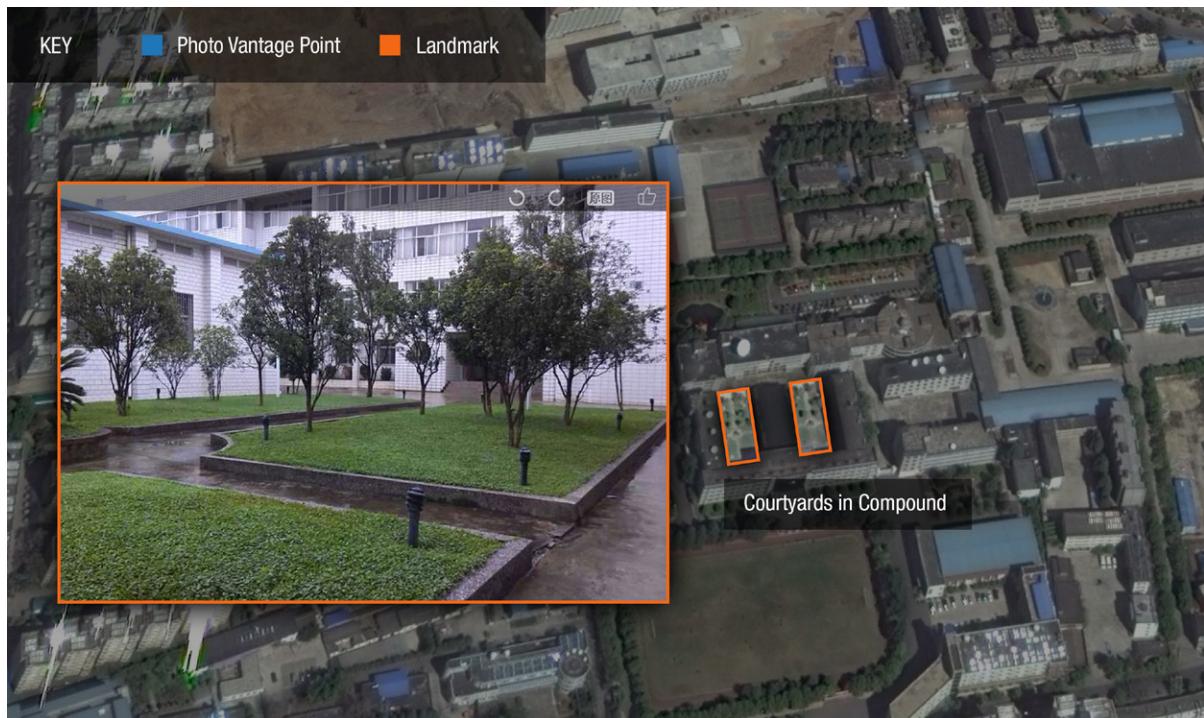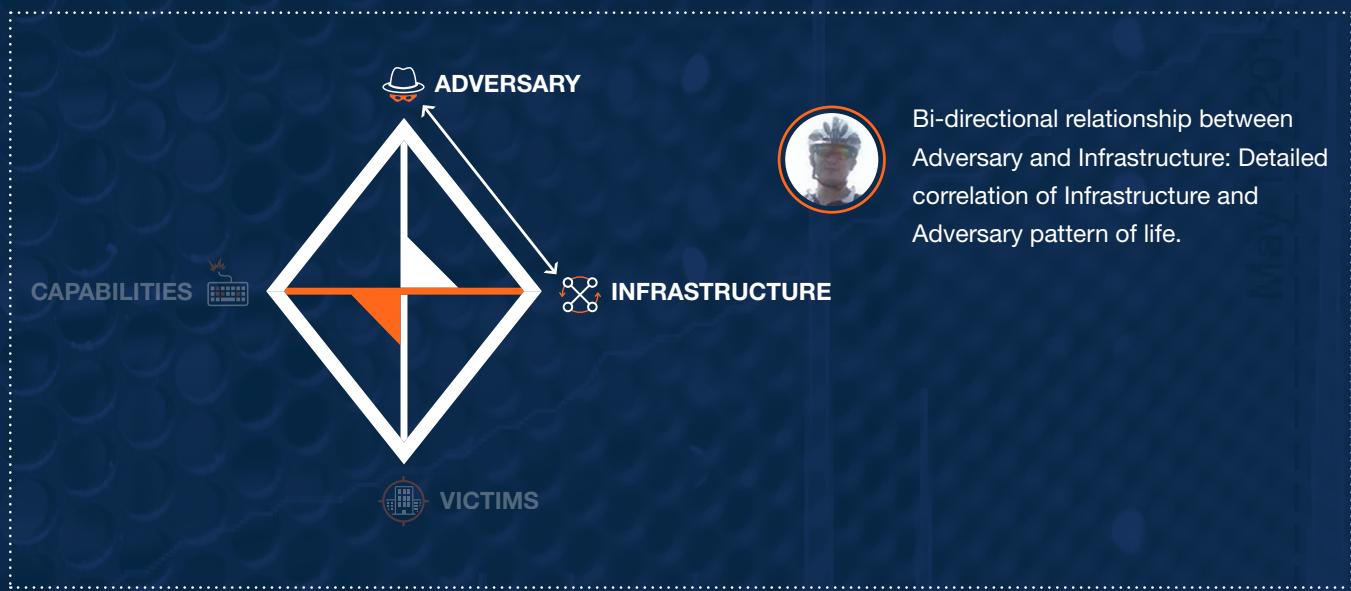

Figure 37: Photo from within Unit 78020's main compound courtyard.

In short, the totality of evidence from online Chinese media confirms both GreenSky27's identity as Ge Xing and Ge's affiliation with PLA Unit 78020. Online social media accounts, geolocated trips and photos, and references to a physical address confirm Ge Xing's identity and location in Kunming. Ge's military, academic, and publication background strongly hint at his PLA responsibilities, and his photos at the Kunming TRB's main building itself provide definitive proof of association.

We hypothesize Ge Xing is a staff officer at 78020 providing regional expertise to a team of technical personnel. He is qualified for such a role with his apparent expertise in Thai politics, evidenced by his Master's degree in Southeast Asian politics and relevant publications. Ge likely has a position within at least the middle level of the PLA professional hierarchy based on his academic credentials, 10-15 years of experience within the PLA, and his occasional travel to Beijing, Chengdu, and Nanjing. Apart from the appearance of his screen name within Naikon's C2 infrastructure, there is no indication of technical training.

NO ROOM FOR COINCIDENCE — EVIDENCE OF GE XING AND 78020'S INVOLVEMENT IN NAIKON ACTIVITIES

ADVERSARY

CAPABILITIES

INFRASTRUCTURE

Bi-directional relationship between Adversary and Infrastructure: Detailed correlation of Infrastructure and Adversary pattern of life.

VICTIMS

THREAT CONNECT™

DGI Bh BLUE HERON

Our analysis concludes the evidence tying Ge Xing to Unit 78020 and its Naikon APT activity is quite strong. This section documents how Ge Xing's background is ideal for supporting Naikon activities and how his personal schedule correlates with activity by greensky27.vicp.net. To confirm the greensky27.vcip.net domain was not the work of a freelancer, we examined the time of day during which the domain made DNS record changes. We also found striking correlations when we overlaid Ge Xing's social media postings with periods of greensky27.vcip.net domain inactivity.

The most compelling evidence of Ge Xing's involvement with Unit 78020 and the Naikon campaigns is the correlation between details of his personal-life events such as travel, vacation, family events, and Naikon activity. We base our timelines of Ge's personal life and events on his QQ photos taken across the country, as well as comments made on those photos and other social media. Trip dates are based on the posting dates for photos Ge took in a particular location. When Ge Xing is away from Kunming, analysis of the greensky27.vicp.net infrastructure indicates it is offline or parked as detailed in Chapter Two. As we dive into passive and active DNS resolutions for the greensky27.vicp.net domain over the past five years, we can identify notable resolution patterns that are consistent with events, dates, and times Ge has posted online.

To give you a bird's-eye view of the timeline of events in the greensky27.vicp.net domain history and Ge Xing's personal-life events over the last five years, we present to you Figure 38 below.
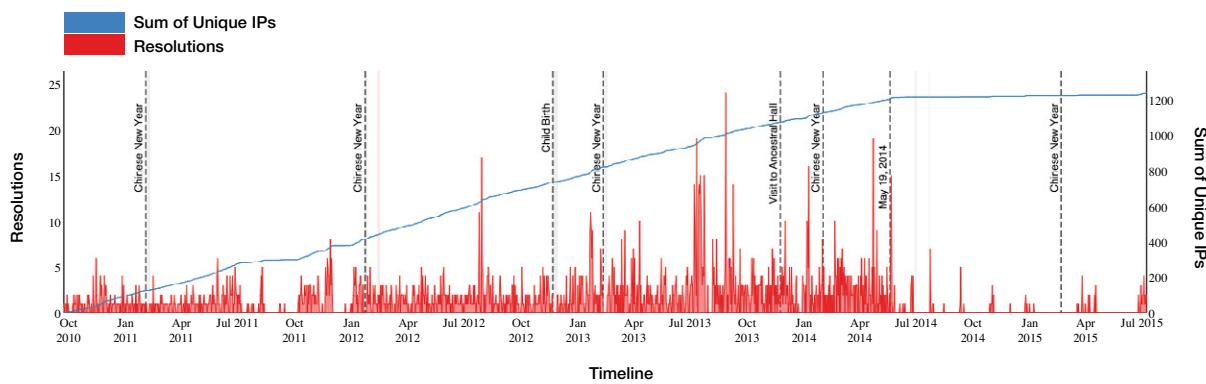

Figure 38: Timeline of infrastructure activity and adversary-relevant events.

The red line denotes the number of times the greensky27.vicp.net domain changed IP addresses in a day. A spike on the red line indicates the domain was extremely active, jumping around to avoid detection by IP-based filters when carrying out its evil deeds. A glimpse of the chart gives you four distinct time periods: heavy activity from late October 2010 to July 2011, followed by a more or less dormant period until October 2011. The domain resumed high operational tempo until June 2014, after which we see extended periods of dormancy with occasional bursts of activity.

The blue line shows the cumulative rise in number of unique IP addresses the domain has resolved to over the five-year period. There is a clear correlation between the red and blue lines: whenever the domain is dormant (absence of activity on the red line), you see the blue line flattening (no rise in usage of new IP addresses) and conversely a steady increase in the blue line whenever the domain is highly active.

The vertical lines represent certain "pattern of life" events tied to Ge Xing and show a remarkable correlation with the timeline of the greensky27.vicp.net domain infrastructure. But don't squint too hard, we are going to dive deep into each of the events.

The Year of the Rabbit, the Dragon, and the Snake

The Chinese New Year is responsible for the single biggest human migration every year, with upwards of one billion road and public-transit trips estimated within China during this period.[54] Given the centrality of Chinese New Year with its emphasis on visiting family, we would expect to see the greensky27.vcip.net domain to become inactive during this period. The graphs below provide a zoomed-in timeline around the Chinese New Year events of 2011 (the Year of the Rabbit), 2012 (the Dragon), and 2013 (the Snake). As expected, the domain is dormant for almost a whole week in each of the three cases, the length of time an individual may be expected to be on leave during this event. By July 2014, the domain remained consistently dormant, so the 2014 and 2015 Chinese New Year events showed nothing irregular.
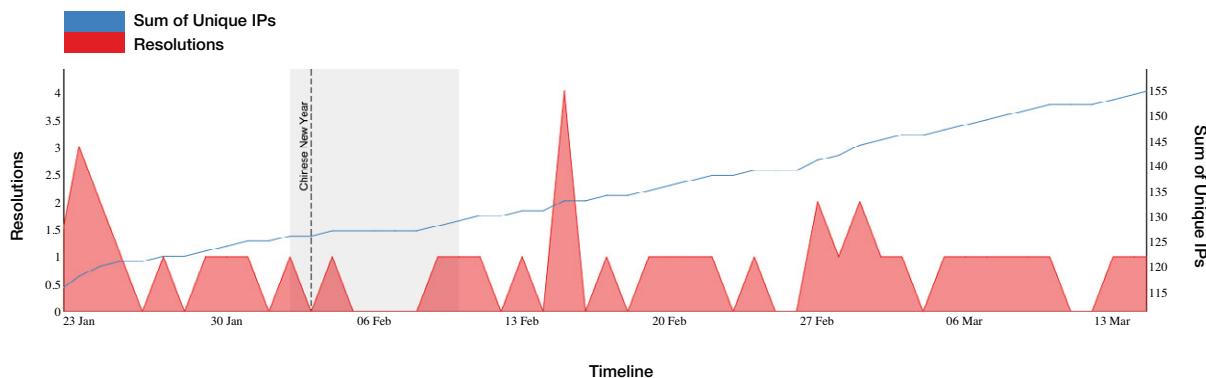

Figure 39: Infrastructure activity around Chinese New Year 2011 (Thursday, February 3).
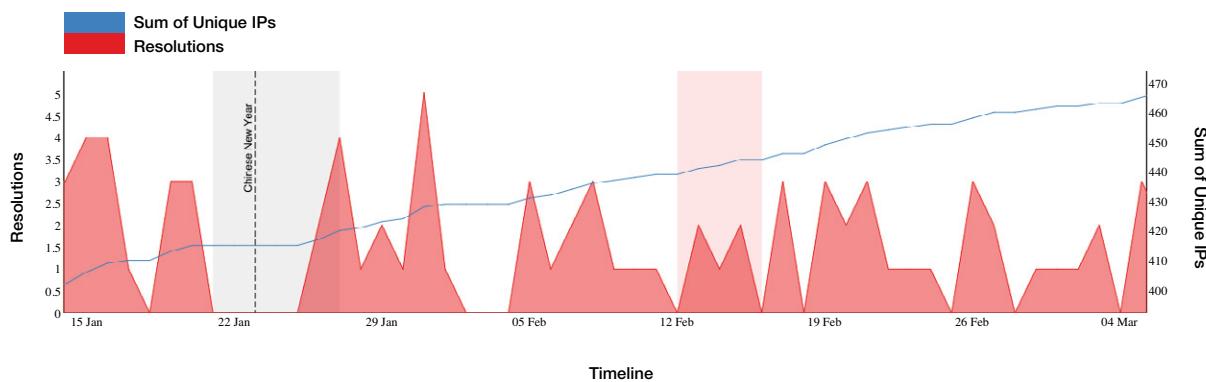

Figure 40: Infrastructure activity around Chinese New Year 2012 (Monday, January 23).
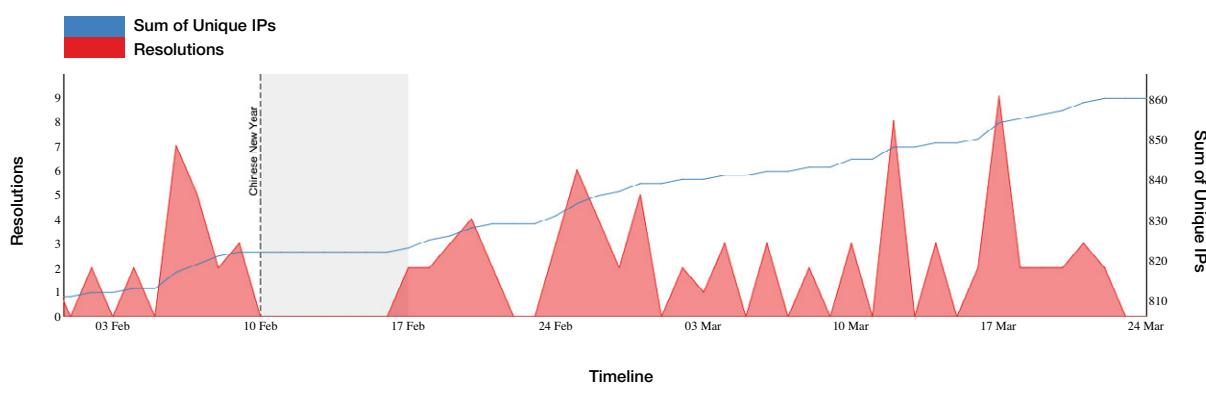

Figure 41: Infrastructure activity around Chinese New Year 2013 (Sunday, February 10).

. . . .

Of these three examples, 2012 is of particular interest. Chinese New Year was celebrated on January 23, 2012. We saw the expected lull in activity, but it was cut short. On Friday, January 27, 2012 at 10:55 AM China Central Time, the greensky27.vicp.net domain reactivated, making resolution changes until Thursday, February 2 and then going inactive again over the weekend before resuming activity on Monday, February 6, 2012.

Our working hypothesis is the holiday may have been interrupted by news of the bilateral U.S.-Philippines negotiating broader military cooperation. On January 26 and 27, 2012, Western media outlets such as the *New York Times*[55], Reuters[56], and *Time Magazine*[57] reported on a high-level Philippine delegation visiting Washington, D.C. The visit was part of preliminary talks with U.S. officials aimed at strengthening military cooperation in support of the Obama administration's strategic "pivot" to Asia. We suspect reports of the Philippine delegation's visit to Washington may have interrupted New Year festivities and forced resumption of active work.

We acknowledge dormancy during the Chinese New Year holiday does not on its own prove the person behind the greensky27.vcip.net infrastructure is Ge Xing specifically, since practically the entire country takes vacation during this time. To further prove that out, we plotted certain events in Ge Xing's life from his social media postings as described in Chapter Three, which correlate closely to lulls in activity within our timeline.

Beijing Resolutions Coincide with a February 2012 Visit to the Capital
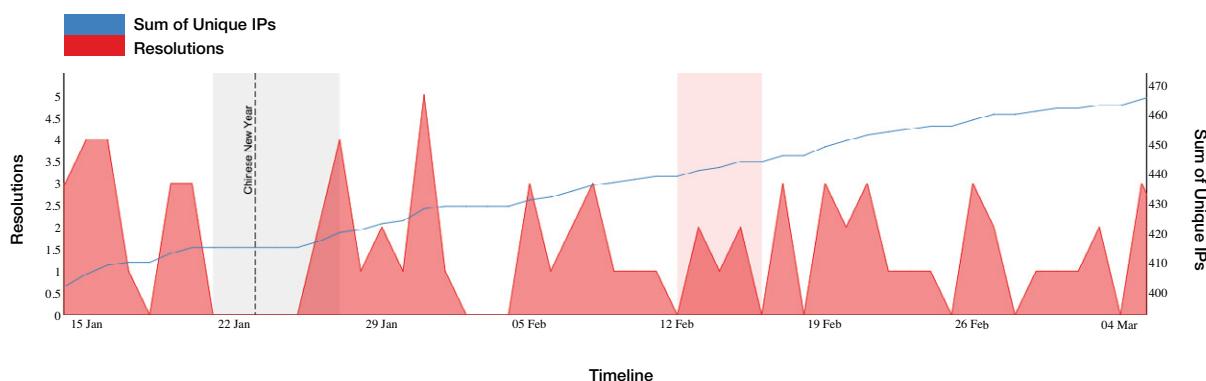
Figure 42: Infrastructure activity around Ge Xing's Febuary 2012 visit to Beijing. The twin peaks in the red-shaded region are two of the very rare Beijing resolutions.

Figure 43: Photos within Beijing posted to social media by Ge Xing during his Febuary 2012 visit.

55   http://www.nytimes.com/2012/01/27/world/asia/manila-negotiates-broader-military-ties-with-us.html
56   http://www.reuters.com/article/2012/01/26/us-philippines-us-idUSTRE80P22320120126
57   http://world.time.com/2012/01/27/time-exclusive-president-benigno-aquino-on-u-s-philippine-military-ties

Shortly after the Chinese New Year, Ge Xing visited Beijing from February 12 to 16, 2012, shown in a red vertical band in the figure above. We suspect the visit was official business, during which we observed the greensky27.vcip.net domain resolve to an IP address in Beijing. Of the nearly 2,500 DNS record changes in our entire data set, less than half of one percent ever resolved into a Beijing IP address – a third of which fell within this time period. The rarity of the domain in question resolving to Beijing combined with the corresponding visit by Ge Xing prevents us from accepting this as mere coincidence.

Birth Announcement for Ge Xing's Child: November 2012

A November 21, 2012 post on Baidu Tieba by "greensky27" states: "A [child], surnamed Ge, born November 20, 2012, at 11:36 PM: seeking recommendations for a three-character name."[58] The public post was made to four forum threads within Baidu Tieba at roughly the same time. As we look at the resolution activity, we can clearly see an eight-day gap in activity from November 21 to November 29.
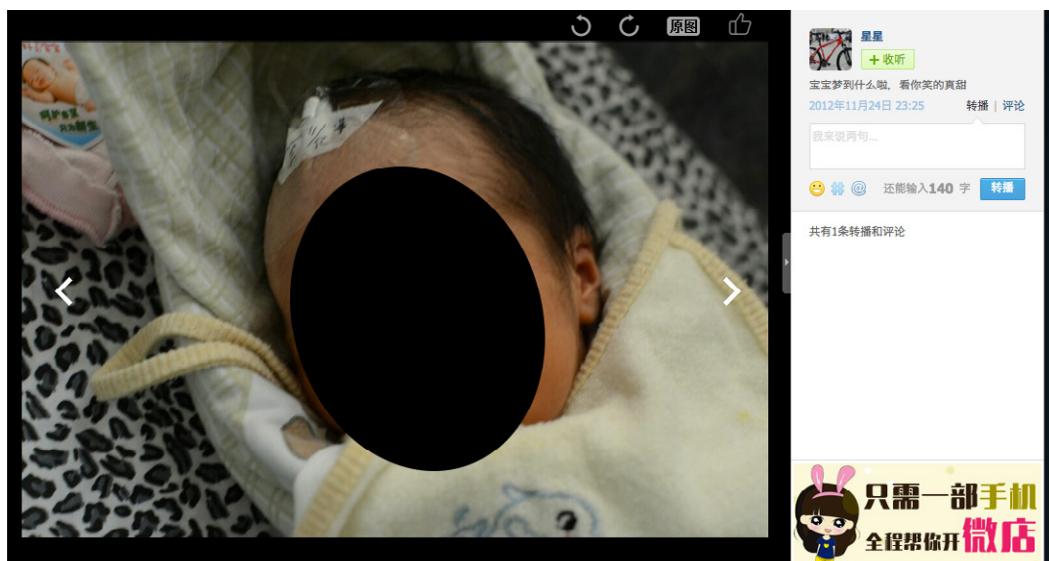

Figure 44: Photo of Ge Xing's newborn child.
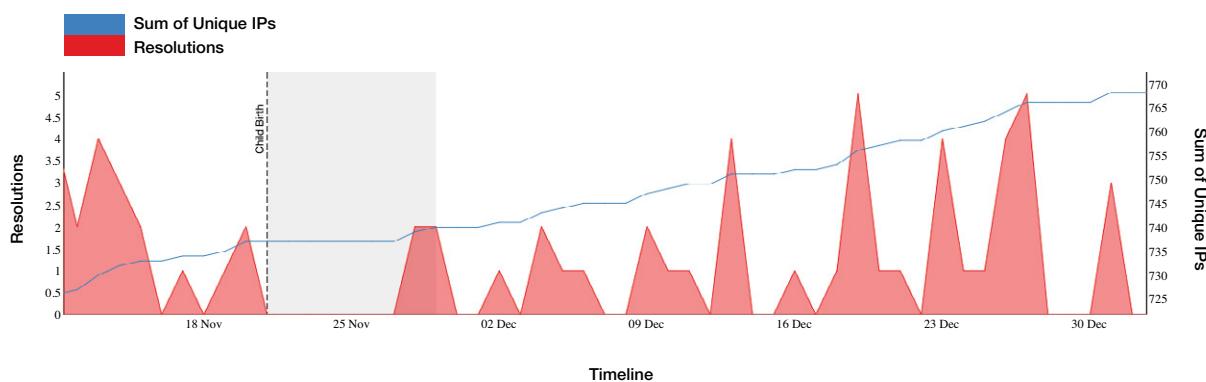
Figure 45: Infrastructure activity around the birth week of Ge Xing's child.

This fact coupled with the evidence tied to other events presents compelling evidence of Ge Xing's connection to the activities of the greensky27.vcip.net domain.

. . . .

58   tieba.baidu.com/p/1928480963?pn=21, accessed July 9, 2015.

Domain Goes Dormant During 2013 Visit to Ge Ancestral Hall

On November 23, 2013 Ge Xing visited the Ge family's ancestral memorial hall. These images show the exterior of a memorial hall devoted to remembrance of the Ge family's deceased ancestors, as well as individual tablets and inscriptions within the hall bearing the Ge family name. The figures below show several of these images accompanied by translations. The QQ Weibo caption common to all of these photos reads, "Returning home to pay respect to the ancestors, this ancestral memorial hall is not bad."

Figure 46: Plaque and memorial within the Ge family memorial hall. The heading on the plaque at left reads, "Ge family ancestral hall epitaphs" (葛氏宗祠碑誌). The inscription on the memorial at right reads, "Memorial to Ge family past generations and deceased parents" (葛氏歷代宗祖考妣之神位).

Infrastructure analysis of greensky27.vicp.net highlights Ge was active using infrastructure from Kunming and Thailand for the week prior to his weekend trip to his ancestral hall on November 23, 2013. However on November 23, the greensky27.vicp.net infrastructure was inactive, parked in Seoul and Denver. Note the gap is only 28 hours, so the infrastructure was active on both of the calendar days with a gap of 28 hours between them. The chart below at daily resolution is not able to completely capture the inactivity, but the parking is evident by the flat line prior to the event.
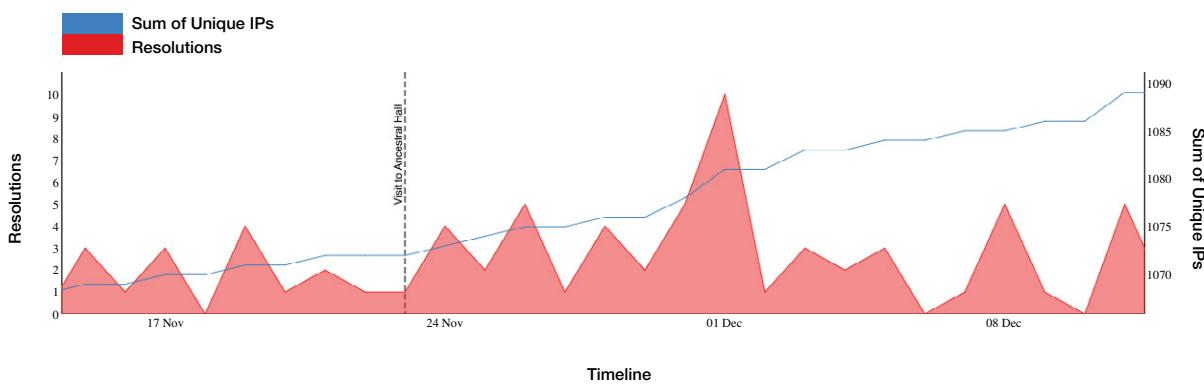
Figure 47: Infrastructure activity around the Ge ancestrial hall visit.

Domain "Parked" During Ge Xing's Two Trips in Summer 2014

Ge posted photos on his QQ account of his road trip outside of Kunming from June 28 to July 1, 2014 and a separate trip to Nanjing from July 21 to 22. Regarding the Nanjing trip on July 22, Ge posted, "Can only post pictures, can't elaborate, look for yourself." The two trips are marked with gray bands in the figure below. During these dates, we note "parking" resolutions to Seoul with four days of inactivity prior to June 30 with an abrupt start date on July 24 after his trip to Nanjing.
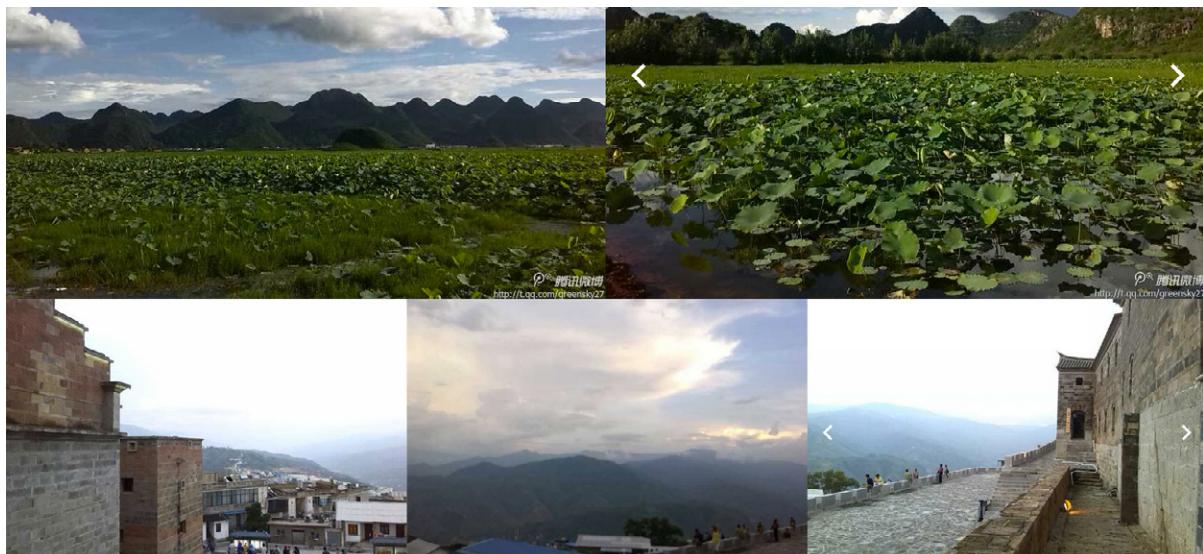
Figure 48: Photos of road trip taken outside of Kunming.

Figure 49: Photos taken during a visit to Nanjing, PLA International Relations Academy (left & center) and Zifeng Tower (right).
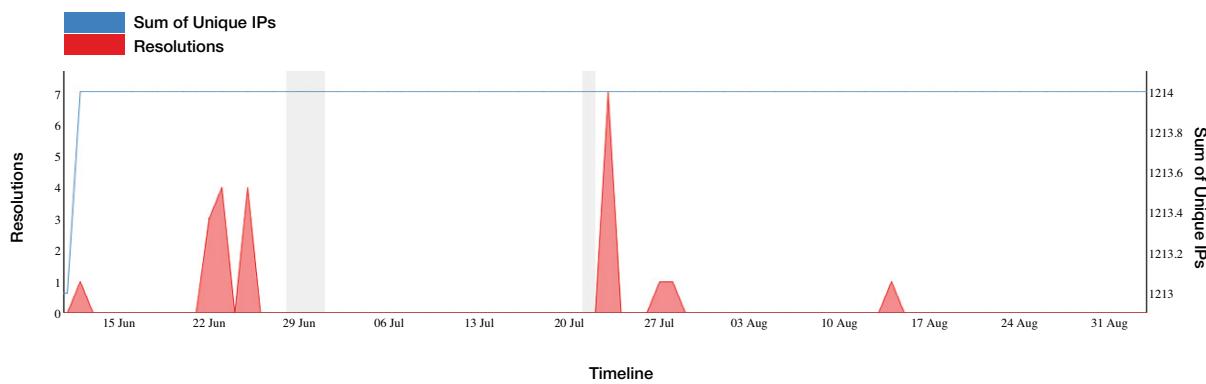
Figure 50: Infrastructure activity around Ge Xing's two trips in summer 2014.

Drastic Changes in Late May 2014

Thus far, we have shown how short-term changes in the greensky27.vicp.net domain correlate with personal events in Ge Xing's life, documented via social media. Overall, however, the domain was active from October 2010 to May 2014 with an increasing cumulative number of unique IP addresses associated. The blue line in Figure 51 illustrates this trend with a drastic flat-lining starting in late May 2014. This notable decline in the rate of unique IP addresses resolved is accompanied by an overall drop in activity.
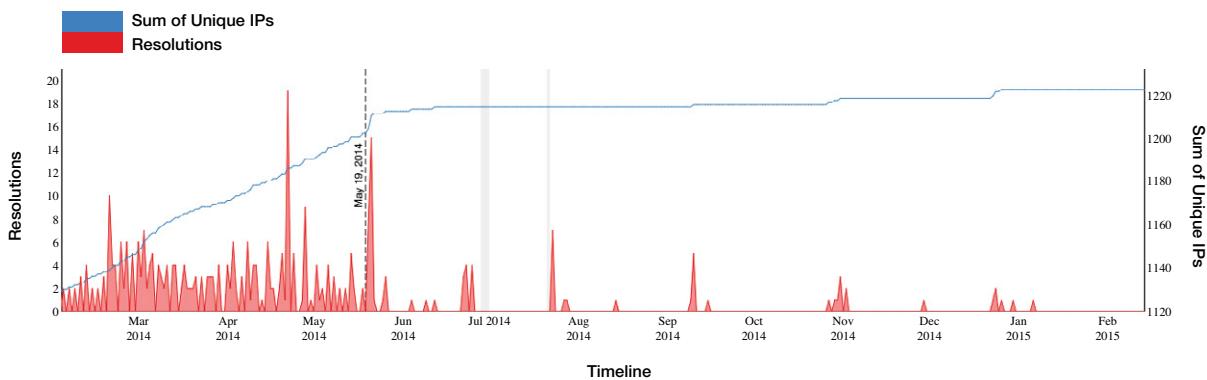
Figure 51: Infrastructure activity before and after May 19, 2014.

One possible theory for this stark change is the May 19, 2014 indictments[59] that the U.S. Department of Justice levied against five Chinese military officers within Unit 61398. On that same date, ThreatConnect published a blog post "Piercing the Cow's Tongue: China Targeting South China Sea Nations" which detailed Naikon activity.

59   http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Ge Xing's Workday

Another interesting set of observations can be made by studying the time of day during which the greensky27.vcip.net domain made DNS record changes. One possible counterargument to our case is the person operating the domain is a freelancer. However, the distribution of the DNS record changes shown in Figure 52 strongly suggests a normal workday. Times are shown in China Standard Time (CST), the time zone used in Kunming. This distribution is a very good indicator of the work hours (+0800 Kunming time) that Ge likely keeps. For example, we can see a spike of activity around 9:00 AM with a mid-day break in activity for lunch, where Ge likely ends his day at various times in early evening between 6:00 and 8:00 PM. The mean of the distribution falls around noon, and it would seem that a substantial portion of the data falls inside 9:00 AM to 5:00 PM.[60]
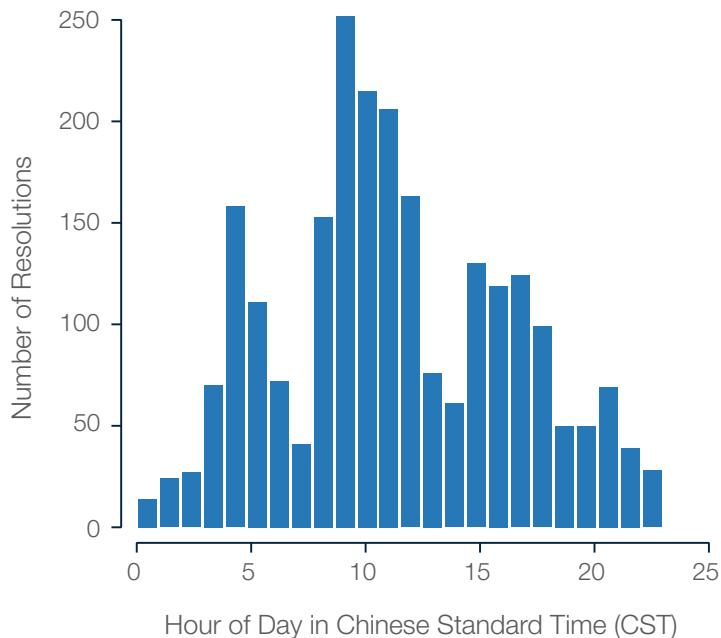
Figure 52: Total count of resolution activity by hour of day (China Standard Time) between 2010 and 2015.

Looking at time of day data for other key cities such as Bangkok, Denver, and Seoul reinforces our conclusions about their role in the adversary's network. As discussed earlier, Ge Xing's academic background focused on Thailand. Bangkok is the second-most resolved city with a high number of resolutions but low time spent resolved. The times are concentrated during the workday and appear centered on the morning work hours. A possible scenario is Ge arrives at work around 9:00 AM, establishes a VPN tunnel into Naikon's operational remote C2 infrastructure, updating his Oray Peanut Shell client manually or setting it to automatically resolve to the respective Bangkok C2 IP address, the same geography where his targets are most likely located.

---

60   The unusual propensity for earlier times before 9:00 AM is due to a series of resolutions into Kunming in 2010 and 2011. During these years, Ge made very few resolutions after 10:00 AM.
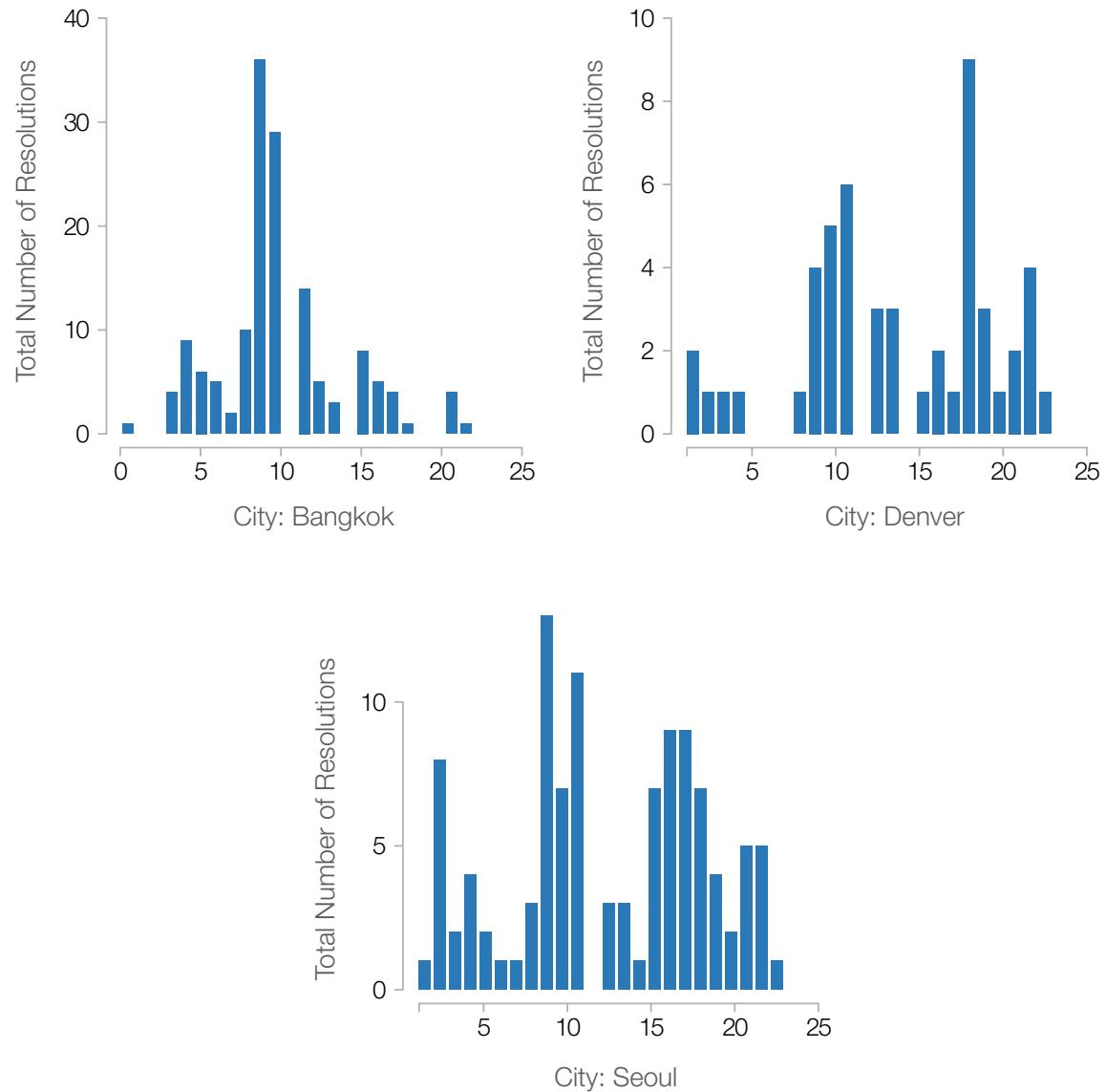
Figure 53: Total count of resolution activity for Bangkok, Denver, and Seoul by hour of day (China Standard Time) between 2010 and 2015.

Whereas the Bangkok graph suggests collections activity, the time of day data for Denver and Seoul is consistent with parking. The majority of Denver resolutions occurs before lunch or at closing time. Seoul has a higher number of resolutions and a less pronounced ratio of resolutions versus time spent. It mimics the Denver graph except for a few early-morning resolutions. Again, we see a majority of resolutions occurring before noon and at closing time, albeit with a less extreme bias than Denver.

CAMERASHY
CONCLUSION

China's incremental yet determined march into the South China Sea is clearly underway. These overt efforts by multiple pillars of Chinese national power are an outward manifestation of their intent to influence and control regional interests. However, operations occurring in the shadows are equally important to what we see conventionally. All of China's activities in the South China Sea, whether military, diplomatic, or economic, have been long supported by a well-resourced covert signals intelligence and digital exploitation unit that maintained deep access within China's Southeast Asian neighbors' public and private sector enterprises.

China's justification in leveraging the military grade signals intelligence Unit 78020 for these operations goes far beyond exploiting countless enterprise networks to acquire proprietary data. Unit 78020's network intrusions are just a ways to a means, and the greensky27.vcip.net infrastructure analyzed in this report is just one small cog in the machine. What is really at hand is a broader national objective of physically intruding into the 1.4 million square miles that make up the South China Sea. It is likely that China does not view this behavior as criminal in nature, insofar as it cannot be stealing if you already consider something to be yours. But the targets of this activity most certainly do not share that view.

This aggressiveness clearly comes at an expense to China's reputation regionally and internationally as credible proof of these operations continues to mount. As this report adds its testimony to the trial, we expect – and have already seen – a temporary cessation in greensky27.vcip.net activity and broader Naikon activities. What we do not expect to see is any change in policy, rhetoric, or operations; China will undoubtedly continue their routine of blasé denials and dismissals of all allegations. Such a position becomes harder to maintain, however, when one of their own – albeit unwittingly – offers the incriminating evidence. We hope the evidences revealed in this report serve as a catalyst for greater awareness and improved diplomacy within the South China Sea region and around the globe.

Takeaways for Intelligence Analysts

While the big picture of this report addresses regional and international affairs, our intent is to speak at a more tactical level to the technical analysts who read it. A love of analysis is not only at the core of our DNA as a company, but has deep personal roots as well. We enjoyed doing this analysis and hope that shows in the final product.

Our goal with this report is to demonstrate the merits of a comprehensive approach to intelligence that strongly connects knowledge about an adversary with their capabilities, infrastructure, and target victims. In that sense, the greensky27.vcip.net domain merely serves as a convenient example to make that case; we realize it's only a small shard in the tip of the Naikon iceberg. There are many public instances of single-dimensional analysis gone wrong, and we offer the structure and rigor of pivoting around the Diamond Model for Intrusion Analysis as a counter to that. Another takeaway for analysts, especially those newer to the field, is how a relatively small set of initial indicators can (with the right platform and processes) be developed into a much larger body of intelligence.

• • • • • • •

> Another takeaway for analysts, especially those newer to the field, is how a relatively small set of initial indicators can (with the right platform and processes) be developed into a much larger body of intelligence.

We began this analysis from a few open source reports and one domain referenced in a handful of malware samples. And that brings up another key takeaway. The principles of science hold that useful research must be shared and reproducible so that findings can be vetted by peers to advance the knowledge of the community. Those same principles apply to threat research, and we commend all of you who hold to them.

Finally, if you enjoyed reading about this analysis, why not participate in expanding and enriching it? Log in or sign up for a free ThreatConnect account to access intel referenced in this report and add findings from your own research.

Takeaways for InfoSec Professionals

This report is first and foremost an intelligence product. But that does not mean it has no relevance to those living "in the trenches" who have the difficult job of defending enterprise networks day in and day out. Intelligence that is never operationalized is arguably not intelligence at all.

With respect to operational defensive efforts, the aim of this analysis is to showcase possibilities enabled through a broad collection of human and technical intelligence. As stated in Chapter Two, we see limited value in the endless game of IP whack-a-mole. Half of all IPs tied to greensky27.vcip.net were seen only once and a quarter of them remained active for less than an hour. A much more efficient approach lies in creating diverse sets of associated indicators along with established tactics, techniques, and procedures and leveraging smart automation to enable them holistically through all layers of defense.

· · · · · · ·

> A much more efficient approach lies in creating diverse sets of associated indicators along with established tactics, techniques, and procedures and leveraging smart automation to enable them holistically through all layers of defense.

On that note, we believe defensive "layers" matter. When approaching the task of stopping badness in your network, many potential options exist. Some are inherently more efficient than others. As one example, the ability to block an entire domain like greensky27.vcip.net as malicious at the DNS layer is much more effective and much less effort than endless firewall rule changes to deny thousands of associated IPs added daily from all over the world.

Unit 78020's tactic of leveraging current regional events in combination with malicious decoy documents demonstrates that attacks against hardware and software often target wetware first. So, it's key to defend at the human level first and foremost. See this as an opportunity to educate all staff to recognize and respond to suspicious activity, files, and incidents. Knowing that they target the vulnerable user over the vulnerable asset is especially critical during periods of increased tensions, diplomatic summits, or other events of strategic interest to potential state or state-affiliated actors.

Takeaways for Business Leaders

Last but certainly not least, we'd like to offer some parting thoughts to the executives, decision makers, and managers who invested their time to review this report – or to those who will brief them. ;)

The inherent unfairness of the security game should be plainly obvious from the scope of this investigation. Those who still picture the adversary as hoodie-wearing teens crouched over a computer in their mom's basement are doing their organizations a disservice. In many cases, as evidenced in this document, the adversary thinks well beyond even your "long-term" strategic plan and is far better resourced than your entire organization. That is not meant as an insult, merely as fact to make the point that your security teams need consistent support from the top to help level the playing field. Giving them that support in combination with sufficient resources to do their job is the most important thing you can do to minimize risk to your organization.

Related to that, understanding the complex array of industry, regional, and international dynamics at play is critical to properly assessing that risk. We hope this report demonstrates that the likelihood of being targeted may not merely be a function of the sensitivity of your intellectual property. There are many socioeconomic and geopolitical factors that drive exploitation campaigns, their impact to victim organizations, and far beyond. Savvy leaders will make every effort to understand these factors in light of their business and take steps to mitigate them as best as possible. It would be disingenuous of us not to recommend solid threat intelligence products like DGI's BLUE HERON, PassiveTotal's passive DNS dataset, and powerful platforms like ThreatConnect as ways to help accomplish that.

APPENDIX A:
NAIKON & GAS-THEMED EXPLOITATION ACTIVITY

ADVERSARY:
Unit 78020

CAPABILITIES

- Tran Duy Linh Exploit Kit
- CVE-2012-0158
- MD5: de8a242af3794a8be921df0cfa51885f

INFRASTRUCTURE

- kyawthumyin.xicp.net
- sayakyaw.xicp.net

1

2

VICTIMS

Individuals and organizations that maintain strategic energy interests within the South China Sea.

1 Possible targeting of individuals and organizations that maintain strategic energy interests within the South China Sea.

2 Spear phishing document with oil & gas themed decoy document.

THREAT CONNECT™

DGI Bh BLUE HERON

We found an instance of Unit 78020 (Naikon) activity with an indirect overlap with the greensky27.vicp.net infrastructure. It came in the form of a "Tran Duy Linh" CVE-2012-0158 exploit kit document MD5: de8a242af3794a8be921df0cfa51885f[61] and was observed on April 10, 2014. This kit deploys a malicious decoy *The Economist* article[62] dated March 29, 2014, which describes the status of off-shore oil drilling bids in Myanmar. Among the companies listed in the article as bid competitors are Total, Shell, Statoil, and Chevron.

Figure 54: Naikon decoy document obtained from a March 2014 *The Economist* article.

The C2s associated with this Naikon malware are kyawthumyin.xicp.net and sayakyaw.xicp.net, both of which have resolved to over 120 common IP addresses since 2013.

61   https://www.virustotal.com/en/file/0e2ee528f56a77e4ce0d074ac36d919e484a2cfdbc6fb109bb7cd0b1406a8a62/analysis/
62   http://www.economist.com/news/business/21599810-companies-will-soon-find-out-how-much-oil-and-gas-there-really-offshore-drilling-dark
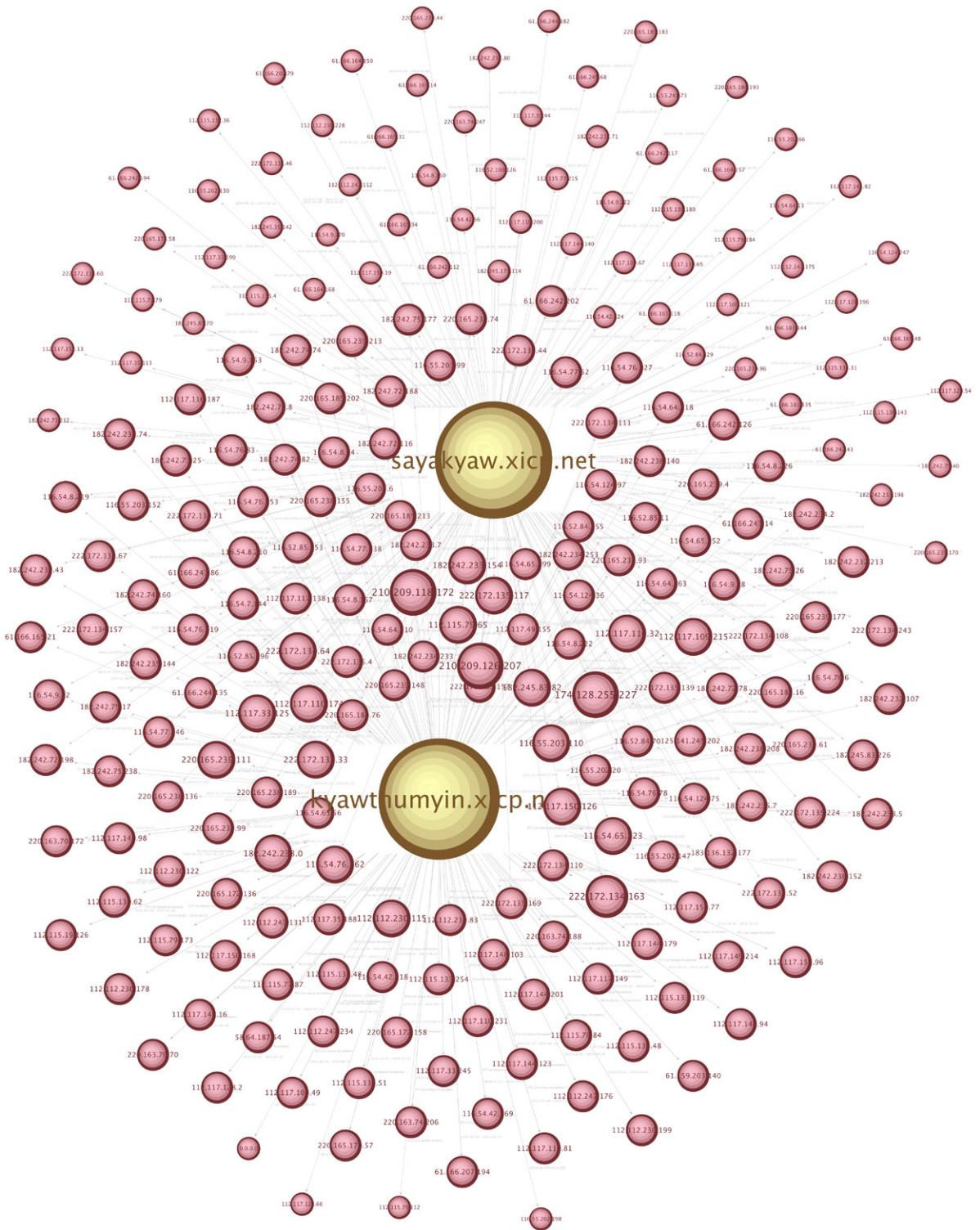
Figure 55: Shared infrastructure between malicious Naikon dynamic domains kyawthumyin.xicp.net and sayakyaw.xicp.net.

As we begin to enumerate across Naikon infrastructure using ThreatConnect active DNS fused with passive DNS data sets, we can see Naikon's proclivity to reuse infrastructure across several campaigns. In the example below, clusters of unique and common infrastructure emerge around just a subset of Naikon C2 domains.
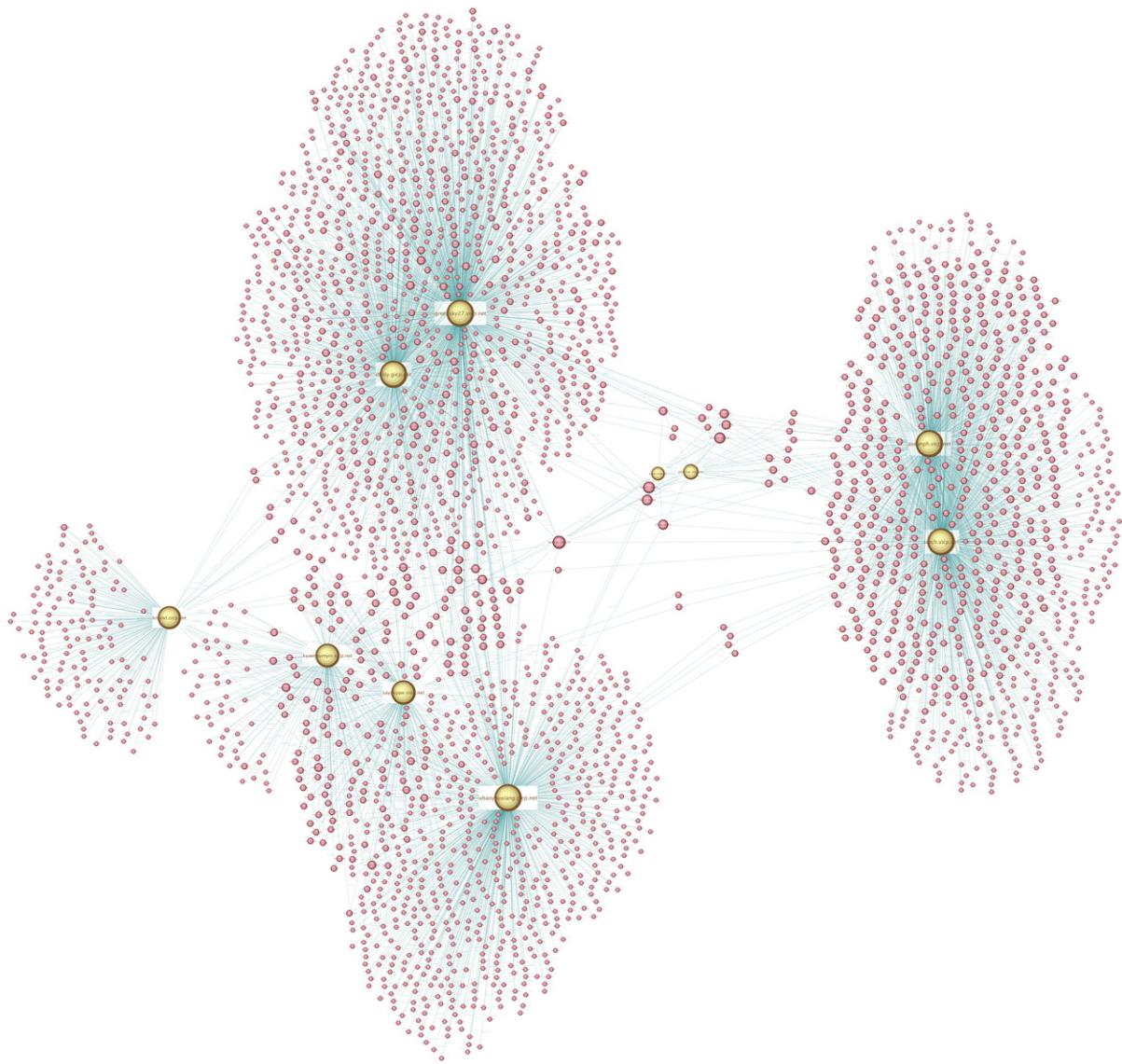
Figure 56: Subset of Naikon dynamic domains and overlapping infrastructure.

The comparison of the kyawthumyin.xicp.net and sayakyaw.xicp.net domains seen within MD5: de8a242af3794a8be921df0cfa51885f reveal expansive associations across shared infrastructure and between other Naikon domains – including greensky27.vicp.net.

As we filter the dataset to focus on the subset of primary overlapping nodes, we see curious relationships between infrastructure used by malware embedded in oil- and gas-themed decoy documents. We also observe infrastructure that maintains unique naming conventions, such as aseanph.vicp.net, pnoc.vicp.net, pnoc-ec.vicp.net, and serch.vicp.net.
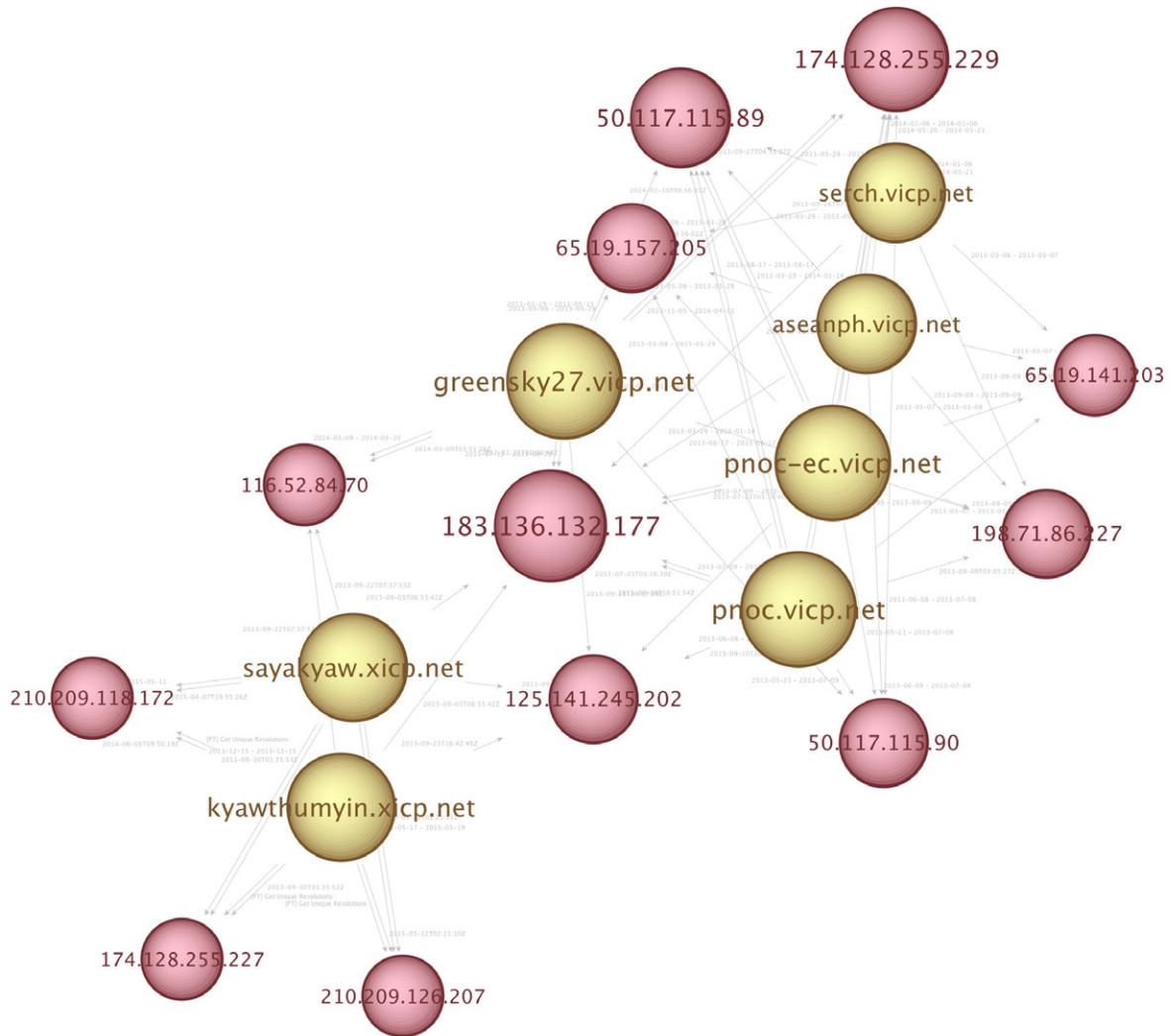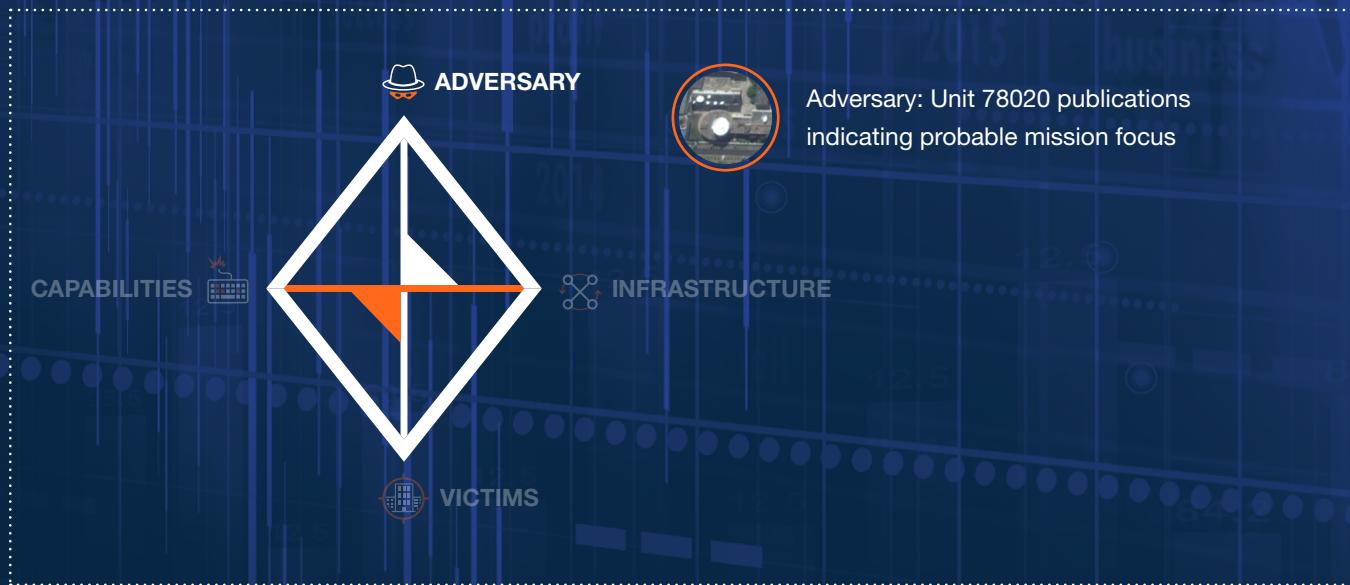
Figure 57: Example of commonly shared Naikon infrastructure between malicious dynamic domains that maintain ASEAN and or oil & gas themes.

The naming convention applied within aseanph.vicp.net is clearly a reference to the Association of Southeast Asian Nations, while pnoc.vicp.net and pnoc-ec.vicp.net are likely impersonating the Philippine National Oil Company[63] (PNOC) and its subsidiary Exploration Corporation (www.pnoc-ec.com.ph) respectively. The oil and gas infrastructure nexus observed in connection with greensky27.vicp.net and other Unit 78020 (Naikon) infrastructure suggests targeting patterns supportive of the PRC's strategic interests over energy resources within the South China Sea and Southeast Asia.

....

63   http://www.pnoc.com.ph/

APPENDIX B:
TECHNICAL RECONNAISSANCE BUREAUS

ADVERSARY

Adversary: Unit 78020 publications indicating probable mission focus

CAPABILITIES

INFRASTRUCTURE

VICTIMS

Military region TRBs located near China's borders are thought to support local border defense forces in addition to their military region commands.[64] In the case of the Kunming TRB, this mission would naturally engender a regional focus on Southeast Asia. This hypothesis is supported by the topics of research papers authored by TRB personnel (Appendix C: Summary of publications written by Unit 78020 personnel), several of which discuss Southeast Asian politics. The Kunming TRB is one of 10 military region TRBs as listed in the below chart.
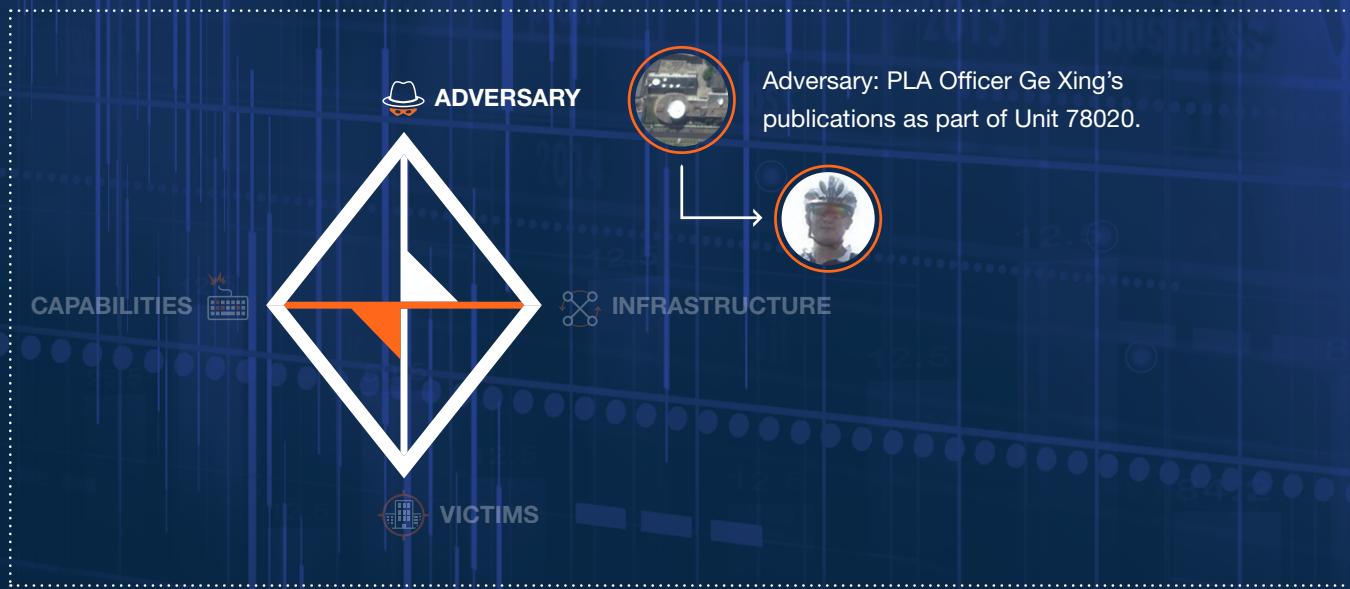
MILITARY REGION (MR)	UNIT DESIGNATOR	LOCATION	MILITARY UNIT COVER DESIGNATOR (MUCD)
Shenyang MR	Technical Reconnaissance Bureau	Shenyang, Liaoning Province	Unit 65016
Beijing MR	Beijing MR Technical Reconnaissance Bureau	Beijing	Unit 66407
Lanzhou MR	1st Technical Reconnaissance Bureau	Qilihe District, Gansu Province	Unit 68002
Lanzhou MR	2nd Technical Reconnaissance Bureau	Urumqi, Xinjiang Uyghur Autonomous Region	Unit 69010
Jinan MR	Technical Reconnaissance Bureau	Jinan, Shandong Province	Unit 72959
Nanjing MR	1st Technical Reconnaissance Bureau	Nanjing, Jiangsu Province	Unit 73610
Nanjing MR	2nd Technical Reconnaissance Bureau	Fuzhou, Fujian Province	Unit 73630
Guangzhou MR	Technical Reconnaissance Bureau	Guangzhou, Guangdong Province	Unit 75770
Chengdu MR	1st Technical Reconnaissance Bureau	Chengdu, Sichuan Province	Unit 78006
Chengdu MR	2nd Technical Reconnaissance Bureau	Kunming, Yunnan Province	Unit 78020

Table 2: Military region technical reconnaissance bureaus, with location and military unit cover designators.[65]

....

64   Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute, November 11, 2011.
65   Brian Krekel, Patton Adams, George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," report for the US-China Economic and Security Review Commission prepared by Northrop Grumman Corp, March 7, 2012.

SUMMARY OF PUBLICATIONS WRITTEN BY UNIT 78020 PERSONNEL

ADVERSARY

Adversary: PLA Officer Ge Xing's publications as part of Unit 78020.

CAPABILITIES

INFRASTRUCTURE

VICTIMS

TITLE	AUTHORS	PUBLICATION	PUBLICATION DATE
Improved Information Hiding Algorithm Based on Motion Estimation of H.264 (一种改进的H.264运动估计信息隐藏算法)	王炜;林夕杰;李孝琴	计算机科学	2015/06
Research on Computer Network Security Defense Measures (关于计算机网络安全防范措施的研究)	何绍勇;蒋元；许眉扬	电子技术与软件工程	2015/05
On Key Technologies of Industrial Ethernet (浅析工业以太网的关键技术)	宁继鹏;高放；刘捷	通讯世界	2015/02
Exploration of Ethernet Security (关于以太网安全性的探讨)	宁继鹏;高放；刘捷	网络安全技术与应用	2015/02
Social Network Layered Architecture Discovery (社会网络的层次结构发现)	成清；黄森；黄金才	复杂系统与复杂性科学	2015/01
Discussion on Preventing Child Living Donor Liver Transplant Thrombosis (儿童活体肝移植术后血栓的防治措施探讨)	陈应富;刘晓；许峰；胡兰	重庆医科大学学报	2015/01
Levofloxacin Induced Anaphylatic Shock 1 Case (左氧氟沙星致过敏性休克1例)	张志华;刘春艳;张羽；何林	人民军医	2014/10
Cryptanalysis of Image Encryption Algorithm Based on Improved Erdogic Matrix and Pixel Value Diffusion (对"改进遍历矩阵和像素值扩散的图像加密算法"的密码分析)	杨吉云;田维兴;周发贵	计算机应用	2014/09
Submarine Weapons System Maintenance and Protection Plan Evaluation (潜空武器系统维修保障方案评价研究)	许诚；王赫巍；王腾飞；赵葛宏	项目管理技术	2014/09
Moving Low Duty Cycle Sensor Network Neighbor Discovery Algorithm (移动低占空比传感网邻居发现算法)	陈良银;颜秉姝;张靖宇;胡剑波;刘振磊;刘燕；徐正坤；罗谦	软件学报	2014/06
Cognitive Radio Technology Application in Ground-Air Data Link System (认知无线电技术在地空数据链系统中的应用浅析)	高猛；蒋圆；邹健；吕宪凡	中国电子科学研究院学报	2014/06
State Information Visualization Model for Autonomous Web Service and Its Realization Technology (面向自主Web服务的态势信息监视模型及其实现技术)	陈超；张红军；毛新军；尹俊文；侯富	计算机科学	2014/05
Standardize Party Rules of Procedure, Promote Party Democratic Decision-Making (规范党委议事规则 推进党委民主决策)	李巡航;张楠	西安政治学院学报	2014/04

TITLE	AUTHORS	PUBLICATION	PUBLICATION DATE
Multi-Path Optical Fiber Data Synchronization Technology Based on FPGA (基于FPGA的多路光纤数据同步技术)	牛戴楠;史俊宏;黄鏐;方振发	雷达与对抗	2014/04
An LOFDM System Peak to Average Ration Non-Linear Compression and Expansion Algorithm (一种LOFDM系统峰均比非线性压扩算法)	彭斯明;沈越泓;袁志钢;简伟;李慧	军事通信技术	2014/03
Comparative Analysis of Treadmill Exercise Test and Coronary Angiography (平板运动试验与冠状动脉造影的对比分析)	杨桂萍;马燕	云南医药	2014/03
Low Occupancy Ratio Wireless Sensor Network Asynchronous Neighbor Discovery Algorithm Research (低占空比无线传感器网络异步邻居发现算法研究)	王朝龙;徐正坤;殷锋	信息通信	2014/02
Computer Network Worms and Worm Vaccination Research Progress and Trends (计算机网络蠕虫及蠕虫疫苗的研究进展和趋势)	张俊；李家准；游尊勇	数字化用户	2013/08
Dynamic Host Assignment Protocol Technology (动态主机分配协议技术研究)	刘云宏;张俊；许眉杨	数字化用户	2013/08
Performance of Opportunistic Network Based on Low Occupancy Ratio (基于低占空比技术的机会网络性能研究)	卓碧华;郭振乾;徐正坤;张靖宇;陈良银	计算机工程	2013/03
Erasure Coding Algorithm in Mobile Low-Duty-Cycle Opportunistic Networks Based on Energy Awareness (基于能量感知的移动低占空比机会网络纠删编码算法)	陈良银;刘振磊;邹循；徐正坤；郭振乾；张靖宇；袁平；刘燕	软件学报	2013/02

The substantive focus of Unit 78020 can be seen in part through a review of publications written by personnel affiliated with the Unit since 2004. Several topical groupings emerge. Many recent papers focus on network security, data mining, and wireless communications. A number of papers discuss Southeast Asian and Japanese international relations.

APPENDIX D:
ORAY INFRASTRUCTURE

ADVERSARY

CAPABILITIES

INFRASTRUCTURE
Overview of how Ge Xing abuses Oray dynamic DNS infrastructure.

VICTIMS

I n Chapter Two we delved into detail covering the various patterns observed with the dynamic greensky27.vicp. net domain. For those less familiar with this type of infrastructure, it is important to understand the purpose of a dynamic domain, the service provider in which the domain is managed, and how the user (in this case Ge Xing) likely manages the dynamic domain and the associated resolution records.

As we mentioned in Chapter Two, Naikon and online threat actors in general leverage and abuse benign dynamic DNS service providers to obtain affordable means for mobility and redundancy to communicate with their malicious code. The technique is quite simple: the adversary chooses a dynamic DNS service provider of interest and registers for an account. The adversary will create a hostname (greensky27), binding it to one of the service providers domains in which the dynamic DNS services are offered (vicp.net). The domain (greensky27.vicp.net) is then bound to the user account under the adversary's control.

Example of a the Oray Peanut Shell Client.

The attacker will then embed the new dynamic domain (or domains) within a malicious payload of their choice, in advance of the targeting or delivery phase of the attack. Once the malware is deployed and a victim interacts with it, the malicious payload calls home to the dynamic domain, resolving and connecting to the respective C2 IP address the attacker chooses. The attacker maintains the ability to update DNS records, pointing it to infrastructure (IP addresses) at any time and place of their choosing. In the case of Oray DNS records can be updated manually or managed with client applications or embedded devices such as SOHO routers. Oray boasts integrations with a variety of embedded hardware vendors such as D-Link, TP-Link, ZTE, Huawei, and Cisco.[66]

In the use case highlighted above, Ge and the Naikon APT in general opt to use Shanghai Best Oray Information Technology Co., Ltd. (上海贝锐信息科技有限公司) as a dynamic domain infrastructure service provider. In fact, Naikon even makes a casual reference to Oray within their self-registered domains such as oraydns.googlesec.pw.[67]

According to its website, Oray provides online services and software applications. Its "Peanut Shell" (花生壳) services and applications include remote desktop control (远程监控), website and forum maintenance, VPN services, email systems, FTP services, and office automation services.[68] Users do not need to update their dynamic DNS service through a browser. Instead, Oray offers a local client application that allows users to manage the domain and update items such as the A record, MX record, CNAME (alias), and URL redirection.[69]

According to several Oray.net forum posting notifications to its free Peanut Shell dynamic domain service customers and support forum posts, Oray uses the 174.128.255.0/24 IP address range for resolution of offline (离线) domains where the registered user's host or router is not logged into the dynamic domain service[70]. This is an example of "provider parking" as opposed to the Seoul or non-routable resolutions, which we assess as "adversary parking."

....

66   http://hsk.oray.com/embed/
67   https://securelist.com/analysis/publications/69953/the-naikon-apt/
68   http://hsk.oray.com.
69   http://open.oray.com/wiki-en/doku.php
70   http://bbs.oray.com/thread-226666-1-1.html

KEY CHINESE SOURCES FOR GREENSKY27

WEBSITE	URL	NOTES
QQ Weibo (QQ 微波)	t.qq.com/greensky27	Account GreenSky27. Active account with over 300 followers, updated as recently as November 2014. It contains over 700 posts, and an extensive collection of over 500 photographs and images. Contains contains sufficient information to ascertain GreenSky27's full true name, location, and affiliation with the PLA and the Kunming TRB specifically, details which are corroborated by other sources.
Kunming Mothers Network (昆明妈妈网)	http://www.kmmama.com/home.php?mod=space&uid=7668760&do=profile	An account with username greensky27, UID 7668760, was created April 5, 2012 in the newborn infants section of the website.
Baidu Tieba Forums	http://tieba.baidu.com/p/1928480963?pn=21	A posting by user greensky27 on November 21, 2012 states that a child was born on November 20, 2012, at 11:36PM, with surname "Ge." The post seeks advice on naming the child with a three-character name. Additional posts in 2014 discuss bike components and sale of a mountain bike, including photos of the same bike and apartment interior as shown on the GreenSky27 QQ Weibo account.
5IRC.com Model RC Aircraft Forums	http://www.5irc.com/forum.php?mod=viewthread&tid=10476243	Several posts made by a user named GREENSKY27 advertise model aircraft components for sale. One post lists a phone number and QQ number that are connected to the GreenSky27 QQ Weibo account and the name "Mr. Ge" through other sources.
Lincang (临沧) Township Classified Forums	http://lincang.gdsxxw.com/2shou/bencandy-htm-fid-52-id-28836.html	An advertisement for a used mountain bike lists "Mr. Ge" (葛先生) as contact person, with phone number and QQ account number common to other GreenSky27 forum listings. The picture of the bike in the advertisement was clearly taken inside the same apartment shown in photos posted to the GreenSky27 QQ Weibo account.

WEBSITE	URL	NOTES
Jiuhe 3000 Auctions Website	http://www.jiuhe3000.com/web/market_desc?market.id=8a48718b47d04de60148783b8d9c2c12	A 2014 listing by user greensky27 shows the QQ Weibo GreenSky27's smart watch for sale, listing QQ and phone contact numbers tied to the surname Ge and the GreenSky27 QQ Weibo account by other sources.
in189.com Mobile Phone Forums	http://www.in189.com/space-uid-3374056.html	A user named greensky27 holds an account with user ID number 3374056. The account was created on July 20, 2013, at 00:14. The last login was on September 19, 2013, at 14:03. GreenSky27 made 13 post responses using the account. Eight of these responses were made in a forum for the Huawei G610C. Three were in a forum for the Huawei C8813Q. One was in a forum for the Huawei A199. Two were in a forum for the Zhongxing N919.
Android IT Zone at Sohu.com	http://android.zone.it.sohu.com/space-uid-3634493.html	There is a user named greensky27 at the Android IT zone at Sohu.com. The account profile is essentially empty. The account was registered on June 8, 2011 at 21:14, which was also the last login time. The user posted one response to a forum thread on the subject of Angry Birds Rio.
Zhiyoo Forums	http://bbs.zhiyoo.com/home.php?mod=space&uid=625459&do=profile, accessed May 12, 2015	There is a user named greensky27 at the Zhiyoo Forums site, with user ID 625459. This account was registered on May 12, 2011 at 20:32. The last login was on September 19, 2013 at 13:18. Total logged hours are at 14. Greensky27 responded to 19 posts on the forum. Four posts were within a discussion group for Huawei G610S/G610C/G610T. Eleven posts were in the Zhongxing U880 Android forum. Four posts were in the HTC Wildfire G8 forum.

GE XING'S UNIT 78020 AFFILIATED PUBLICATIONS

战后泰国的政治民主化进程的特点及原因分析

葛 星

（中国人民解放军第78020部队 云南 昆明 650223）

摘 要：本文拟通过对战后泰国民主化进程的回顾，对呈现上述特点的原因进行简单分析。
关键词：泰国；政治民主化；特点

1932—1992年的60年间，泰国共发生了19次军事政变，组建了48届政府。60年中有80%的时间处在军人的统治之下，泰国最近的一次(即第20次)军事政变发生在2006年。[1]政治权力更迭频繁，军事政变是这一时期泰国政治的主要特点，但随着国家现代化的推进，战后泰国民主化进程明显加快。

一、战后泰国的政治发展进程

战后泰国第一届政府是1948年第二次上台执政的披汶·颂堪(Phibun Songkram)政府，他发动政变推翻了自由泰民主政府，泰国政治进入新的专制时期。1957年9月，陆军司令沙立·他那叻(Sarit Thanarat)发动了一次不流血的政变，推翻了披汶·颂堪政府。沙立政府解散了议会和所有政党，废除了宪法，开始了泰国政治上的军人集团全面控制泰国的"沙立时代"。整个60年代泰国处于军人独裁政府之下。

进入70年代，泰国国内形势发生了重大变化。随着经济的高速发展，新兴经济集团要求民主，废除军人专制的呼声高涨。1973年10月13日泰国爆发了有史以来规模最大的示威游行，政府出动军警镇压，国王出面干预，执政仅一年的他侬·吉滴卡(Thanom Kittikatchorn)政府垮台。这就是泰国历史上著名的"十一四"事件，它结束了自沙立以来泰国的军人独裁时代，标志着泰国政治由军人专制统治向议会民主制转变的开始。

此后十余年间，军人和职业政客交替掌握政权，民主政治的发展虽举步维艰但在不断发展。1980年3月，陆军司令炳·廷素拉暖(Prern Tinsulanonda)出任总理。炳总理虽是军人出身，但却重视民主和法制建设，减少军队对政治的干预，扩大人民的民主权利。炳总理执政八年，成为他侬垮台后执政时间最长的一位总理。

1992年3月，通过大选成立了五党联合政府，并推举总司令素金达·甲巴允(Suchinda Kraprayoon)上将担任总理。但反对党以素金达非民选为由，掀起了反素金达的民主运动。此后，爆发了五月流血事件，国王再次出面

干预，素金达被迫辞去总理职务。 此后泰国的民主政治进入相对稳定和健康的发展时期，直至2006年9月发生军事政变。

二、战后泰国政治民主化的主要特点及成因分析

泰国政治民主化过程始终与政变相伴，但仍保持社会发展相对平稳，经济政策长期保持连续性，泰国政治发展的这一特点令人惊奇。那么，导致形成此特点的原因是什么呢？

泰国军人政权的出现是泰国特殊条件下的产物。一般来说，任何一个社会在进行转型的时候，都会出现一个动荡的时期。这是因为在这个过渡过程中，要产生一个新的交往形式，不但经济结构发生变化，人群也要发生变化，习惯于旧有依附关系的民众要转变为一种新的交往形式，必然有一个过程。

二战期间，泰国卷入日本的法西斯战争，军人独裁政权得以强化。战后，泰国政府企图仿效西方，实行议会民制，但当时泰国并不具备实行西方议会民主制的基础和条件，因此没有成功，并导致沙立军人独裁政权的建立。

泰国政权中的权力核心除了军人的力量外，官僚的力量不可小视。事实上，无论是独裁政府还是民选政府，泰国经济政策的制定和实施都是由官僚完成的。泰国的官僚政体不同于其他国家的官僚政体，它吸收了西方文官制度的某些优点，建立了具有泰国特色的技术官僚(teehnocrat)政体。

参考文献：

[1] 王士录.从人民力量党的胜出看当前泰国政党政治的特点[J].当代世界,2008(2).

[2] 陈晓律,李国民.经济高速增长中的低度政治发展—泰国模式研究[J].南京大学学报,1999(1).

责任编辑：丰 军

62

Figure 59: Screenshot of a 2008 paper on Southeast Asian politics written by Ge Xing at Kunming TRB (PLA Unit 78020). The paper is titled, "Analysis of Post-War Thailand's Political Democratization Characteristics and Factors." The author line indicates that Ge Xing is affiliated with the PLA's Unit 78020 in Kunming, Yunnan Province (解放军78020部队). The biographical information at the bottom of the page indicates that Ge Xing was born in 1980, is male, and was a graduate student at Yunnan University's School of International Relations studying Southeast Asian international relations.

泰国南部穆斯林分离运动的发展趋势浅析

葛　星

（中国人民解放军第 78020 部队　云南　昆明　650223）

摘　要：本文通过对泰南穆斯林分离运动历史和现状的考察，对其今后可能的发展趋势做一粗浅分析。
关键词：泰国；穆斯林；分离运动；趋势

　　泰国是一个多民族国家，泰国南部的穆斯林分离运动由来已久。13 世纪，伊斯兰教由阿拉伯穆斯林商人传入马来半岛。13 世纪后期，泰族势力南下，马来势力衰落，泰人控制了马来族的一部分地区。17 世纪初，伊斯兰教取得一定地位，据考证，在阿瑜陀耶王朝时期，已有不少清真寺。自从 1767 年缅甸灭亡阿瑜陀耶王朝后，马来各邦纷纷脱离泰国控制。曼谷王朝时，乌巴腊（即副主）亲率军队南下，先后 5 次向北大年宣战，前后延续 46 年，直到 1832 年才成为泰国南部藩属。

　　1902 年，泰国正式兼并北大年，把该地区划分为 5 个府。1909 年后，这一地区正式纳入泰国的行政管理体制之中，一些马来人不服，不断为北大年解放和脱离泰国的统治而斗争。1948 年，北大年王子以"伟大的马来人运动"的名义向联合国提出最后的求助，也没有获得支持。1957 年，马来西亚独立，极大地鼓舞了泰国南部的马来穆斯林，20 世纪 60 年代末 70 年代初开始的伊斯兰复兴运动对泰国南部马来穆斯林是极大的鼓舞，泰国南部马来穆斯林希望独立或并入马来西亚。盛行东南亚的泛马来主义思潮对泰国南部马来穆斯林分离主义运动起到推波助澜的作用，泰国的马来穆斯林分离主义运动达到高潮。

　　目前，泰南穆斯林分离运动的发展趋势有两大特点：一是泰南穆斯林分离运动正向恐怖主义方向迈进；二是泰南冲突短期内看不到和平前景。

　　究其原因，是因为泰南分离运动自从 20 世纪 80 年代以来，便逐渐走上了恐怖袭击的道路，但是泰南冲突从分离主义发展为恐怖主义的危险从 2004 年以来变得尤为明显。

　　首先是由于泰南分离运动的复兴是在国际恐怖主义盛行的背景下出现的。从 2001 年的"9.11 事件"至今，伊斯兰恐怖主义经历了一个由全球向西方世界开战的全球化阶段转向以地区政治夺权为目标的地区化时期，它们利用具体国家的政治、经济和社会争端进行恐怖活动。尽管没有确切证据表明泰南分离运动与国际恐怖势力存在联系，但国际恐怖主义的地区化发展趋势极有可能利用泰南穆斯林分离组织，泰南恐怖活动的突然增多绝不能被看作是一个孤立现象，它可能预示着东南亚的恐怖暴力活动正在从海岛国家蔓延到陆上国家，而伊斯兰祈祷团成员在泰国的活动增加了这种危险。

　　第二，与以前分离活动的杂乱无章、缺乏计划相比较，目前的恐怖袭击更有组织性和计划性。自 2004 年 1 月以来的分离活动大都有严密组织和计划，他们从进攻到撤退井而有序；他们甚至声东击西，让政府执法部门疲于奔命，这些表明他们不再是几年前的乌合之众，而是受过专业训练的战斗小组。

　　第三，袭击目标及手段的恐怖主义化。泰南各分离组织虽然在上个世纪的斗争中也开展暴力袭击和恐怖活动，但一般不针对无辜平民。20 世纪 80 年代末以来，一些新的分离组织如"新北大年联合解放组织"和"北大年伊斯兰圣战组织"袭击的主要对象是国家公务人员、执法人员和教师等被认为对"马来认同"有威胁的人或地点。

　　尽管泰国政府从一开始便对结束南部动乱充满信心，但目前看来，要平息南部动荡似乎仍需时日。泰国政府的一系列政治、经济、文化、军事措施缓解了穆斯林与中央政府的矛盾，促进穆斯林地区的发展，有利于政局稳定，但作为一个长期难题，解决起来不可能一蹴而就，文化宗教的差异是客观存在的，解决经济落后更是关键所在。

参考文献：
[1]韦红.东南亚五国民族问题研究[M].北京民族出版社,2003.
[2]中国现代国际关系研究所民族与宗教研究中心编.周边地区民族宗教问题透视[M].北京时事出版社,2002.

52

Figure 60: Screenshot of another 2008 paper written by Ge Xing at the Kunming TRB, also on the subject of Southeast Asian politics. The title of the paper is "Examination of Development Trends in Thailand's Southern Muslim Separatist Movement." The author byline and the information at the bottom of the page both indicate that Ge Xing is affiliated with the PLA Unit 78020. The biographical data at the bottom of the page states that Ge Xing, born in 1980, was at the time of publication a graduate student at Yunnan University's School of International Relations, researching Southeast Asian international relations.

THREAT CONNECT™

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

www.threatconnect.com
1.800.965.2708

DGI BLUE HERON

DEFENSE GROUP INC.
2650 PARK TOWER DRIVE, SUITE 400
VIENNA, VA 22180-7306

www.defensegroupinc.com
1.571.421.8300