05.19.14

Piercing the Cow's Tongue: China Targeting South China Seas Nations

IN STAR WARS, THREAT RESEARCH | BY THREATCONNECT RESEARCH TEAM

Executive Summary:

The term "Cow's Tongue" is a reference to the Chinese recognized nine-dashed line which demarks a highly contested region also known as the South China Sea (SCS). Between July 2013 and May 2014, the ThreatConnect Research Team identified and shared multiple instances of Chinese Advanced Persistent Threats (APT), targeting numerous Southeast Asian entities, with our ThreatConnect community members. The perpetrators of these attacks utilized malicious attachments containing subject matter associated with many Southeast Asian related topics such as military doctrine and maritime operations. These efforts are likely the direct operational result of the People's Republic of China (PRC) government's interest in gaining intelligence connected to the deep-rooted, multi-national disputes that are ongoing in the South China Sea (SCS) region. A sampling of the many weaponized documents reveals sensitive classification markings and candid insights within certain decoys, suggesting that these documents had been previously obtained by Chinese cyber operations against commercial, diplomatic, and military targets associated with the region and then used as bait for further targeting.

Significant real world events such as clashes between China and other nations within the SCS, noteworthy popular public demonstrations against regional Chinese aggression, U.S. diplomatic shows of support to opposition of China's growing assertiveness, attempts by Southeast Asian nations attempts to draw outside influence to counter Chinese pressure in maritime territorial disputes, and Chinese military posturing in the East China Sea, will serve as a catalyst for Chinese cyber espionage, of which will likely continue against Southeast Asian and western military and diplomatic targets in addition to any commercial entities that maintain economic interests within the region.

As newsworthy events within the SCS have unfolded, ThreatConnect Research has consistently aggregated and analyzed details of targeted attacks using related bait documents directed against SCS nations. ThreatConnect Research has shared this threat intelligence with ThreatConnect Communities, allowing members to quickly collaborate and act on this information. Organizations that maintain equities within the region are encouraged to develop or leverage threat intelligence within ThreatConnect to monitor the threats that are actively using cyber espionage to influence their strategic interests.

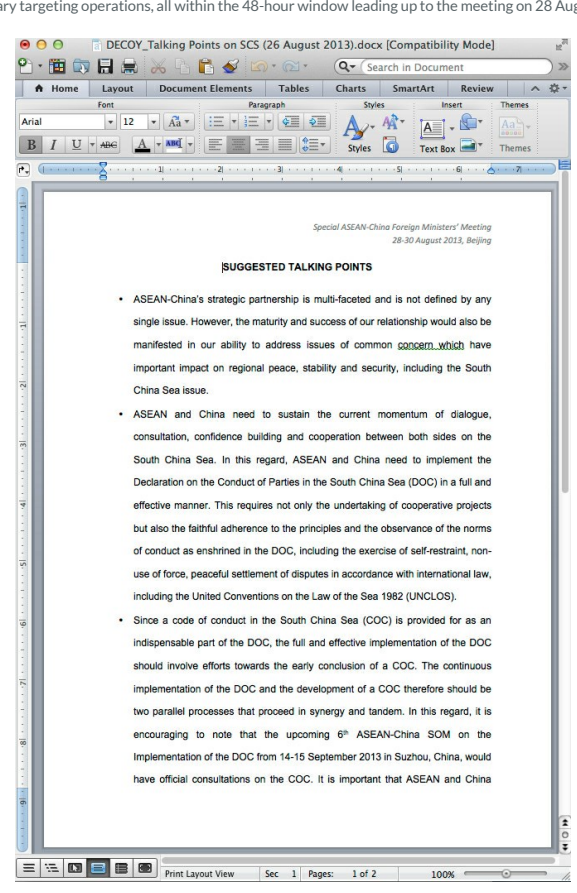
ASEAN Talking Points Exploitation:

Technical Analysis:

In late August 2013, ThreatConnect Research identified a weaponized CVE-2012-0158 Microsoft Word document exploit that was likely originally authored by Hoang Thi Ha, an Association of Southeast Asian Nations (ASEAN) Senior Officer. ASEAN is a geo-political and economic organization of ten countries located in Southeast Asia, which was formed on 8 August 1967 by Indonesia, Malaysia, the Philippines, Singapore and Thailand. Since then, membership has expanded to include Brunei, Burma (Myanmar), Cambodia, Laos, and Vietnam. Its goals include accelerating economic growth, social progress, and cultural development among its members as well as the protection of regional peace and stability and opportunities for member countries to peacefully discuss differences.

The document was related to an early stage, internal talking points memo that was prepared for the Special ASEAN-China Foreign Ministers' Meeting held in Beijing, China from 28 – 30 August 2013. This malicious document, "Talking Points on SCS (26 August 2013).doc" (MD5: 38391CE0A667979EC69F732DBE610AFA) was engineered to drop a "Naikon" APT implant variant (MD5: 69C173C122B0A653CCFD74F2BC953C64) that calls out to the malicious command and control (C2) domain free.googlenow[.]in.

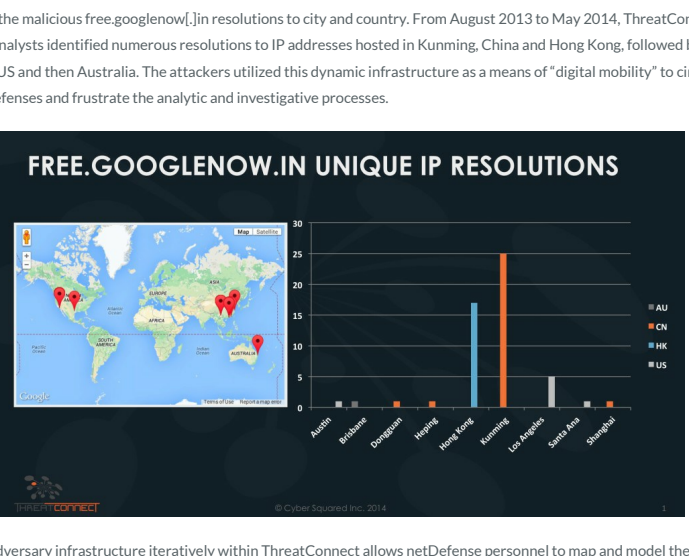
According to document properties, the talking points document was created on the 26th of August, meaning the attackers likely maintained persistent access to the ASEAN networks prior to that date, then accessed a computer or storage medium that housed the draft document, exfiltrated the legitimate document, weaponized it with an exploit and payload implant, then finally conducted secondary targeting operations, all within the 48-hour window leading up to the meeting on 28 August.



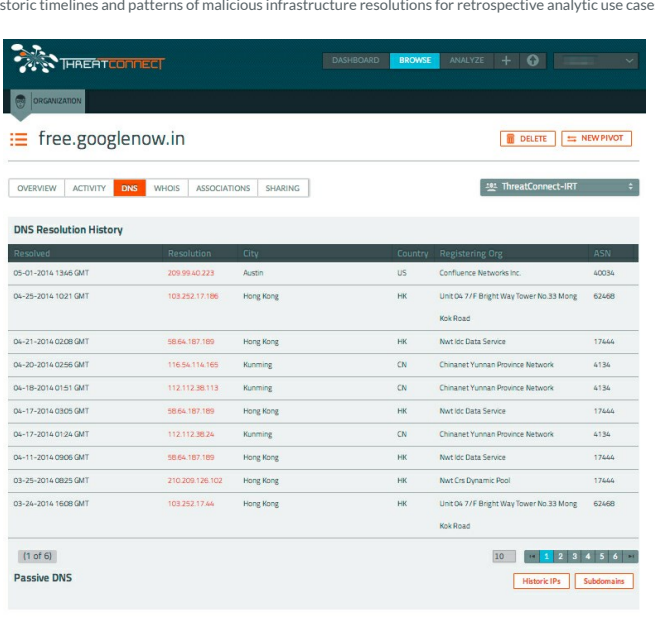
During this meeting, it was agreed that discussions on the development of the Code of Conduct of Parties in the South China Sea (CoC), which aims to be a rule-based framework in managing the conduct of parties in the SCS, would commence in September 2013. This would coincide with the 6th ASEAN-China Senior Officials' Meeting on the Declaration on the Conduct of Parties in the South China Sea (6th ASEAN-China SOM on DOC).

Infrastructure Analysis:

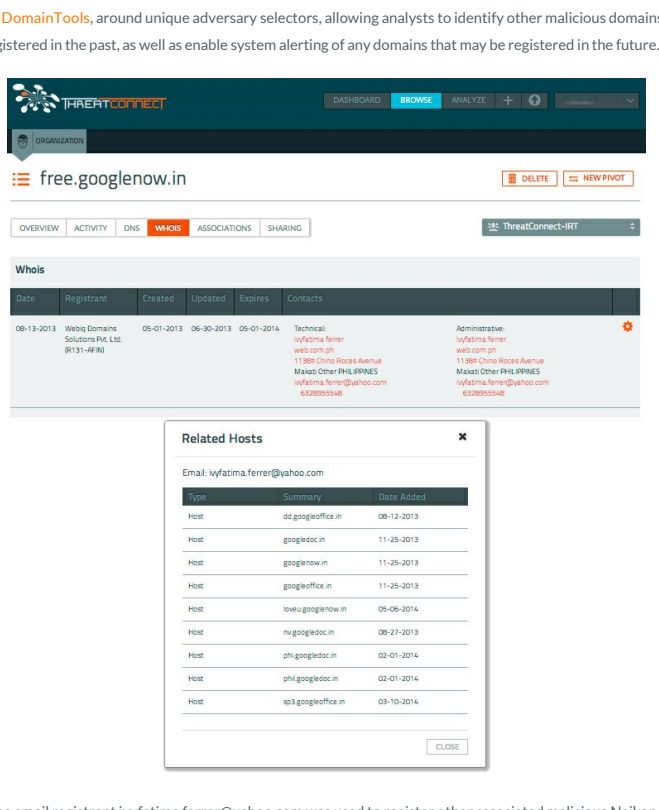
ThreatConnect Research analysts were able to export historic resolutions by pivoting on the malicious domain of interest and filtering on DNS resolutions as a relation type. In the following example, ThreatConnect Research simply applied a frequency analysis of the malicious free.googlenow[.]in resolutions to city and country. From August 2013 to May 2014, ThreatConnect Research analysts identified numerous resolutions to IP addresses hosted in Kunming, China and Hong Kong, followed by cities within the US and then Australia. The attackers utilized this dynamic infrastructure as a means of "digital mobility" to circumvent network defenses and frustrate the analytic and investigative processes.



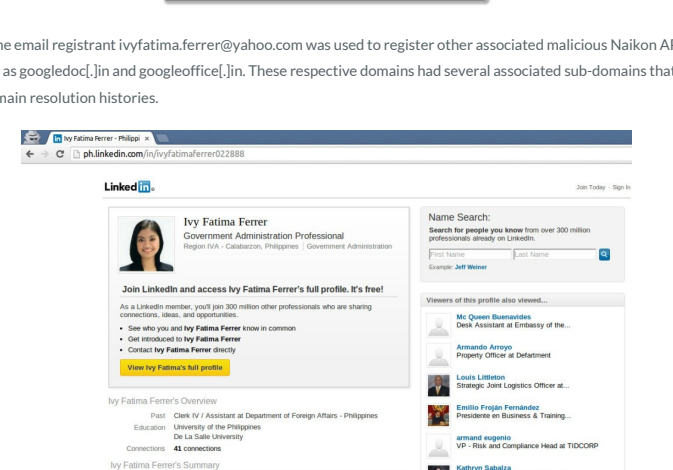
Mapping adversary infrastructure iteratively within ThreatConnect allows netDefense personnel to map and model the infrastructure in which the adversary is likely to use over time. Organizations are then better enabled to develop policies and access controls, not only around infrastructure such as domains or IP addresses, but also attributes associated with that infrastructure such as Country, Service provider or Autonomous Service Number. ThreatConnect domain tracking coupled with Farsight Passive DNS Database (DNSDB) integration allows analysts to not only track adversary infrastructure in real time but to build historic timelines and patterns of malicious infrastructure resolutions for retrospective analytic use cases.



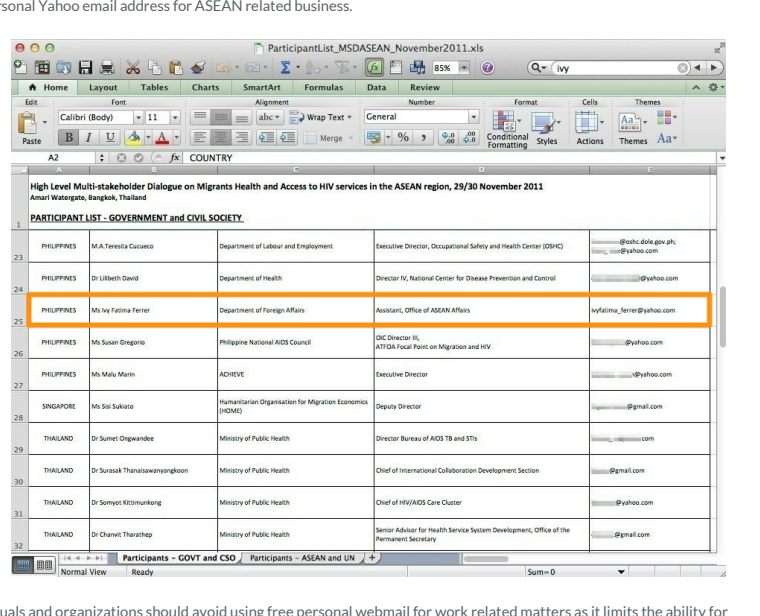
The malicious domain googlenow[.]in is registered by the email address ivyfatima.ferrer@yahoo.com. ThreatConnect Research analysts established a ThreatConnect Track, using integrated Reverse Whois and Registrant Alerts data services from DomainTools, around unique adversary selectors, allowing analysts to identify other malicious domains that may have been registered in the past, as well as enable system alerting of any domains that may be registered in the future.



In this case, the email registrant ivyfatima.ferrer@yahoo.com was used to register other associated malicious Naikon APT domains such as googledoc[.]in and googleoffice[.]in. These respective domains had several associated sub-domains that all had their own domain resolution histories.



The faux "ivyfatima.ferrer@yahoo.com" email address was likely created to masquerade as the legitimate email address belonging to the real Ivy Fatima Ferrer, an Assistant in the Department of Foreign Affairs, ASEAN, who uses the real email address of "ivyfatima_ferrer@yahoo.com". In the example below, ThreatConnect Research was able to validate that Ivy Fatima Ferrer uses her personal Yahoo email address for ASEAN related business.

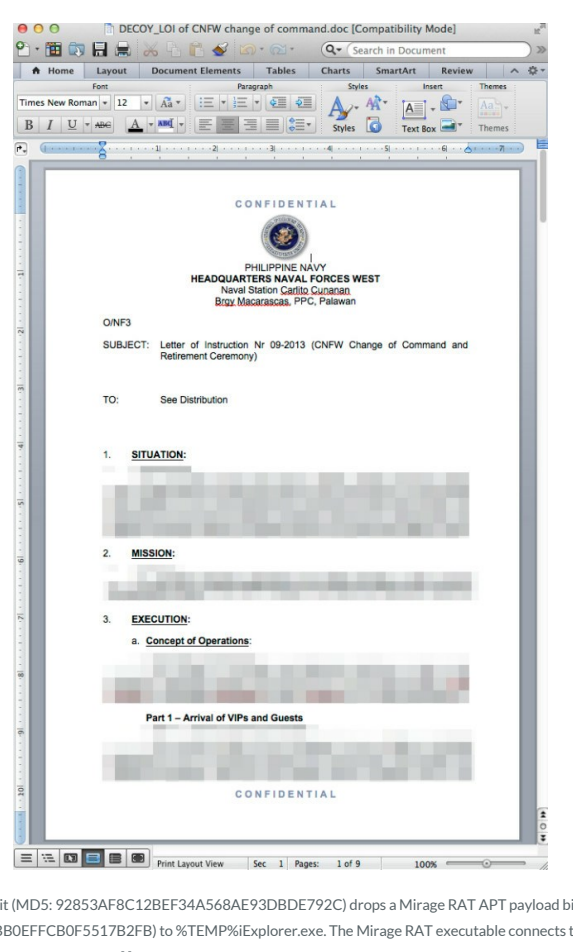


Individuals and organizations should avoid using free personal webmail for work related matters as it limits the ability for organizational netDefense providers to deliver security services around corporate assets. Also, converging public/private accounts may also increase the surface area in which persistent adversaries may target a given user. If compromised, an unwitting user may introduce costly security risks from their personal accounts, personal computing platforms or personal mobile devices into a cooperate network.

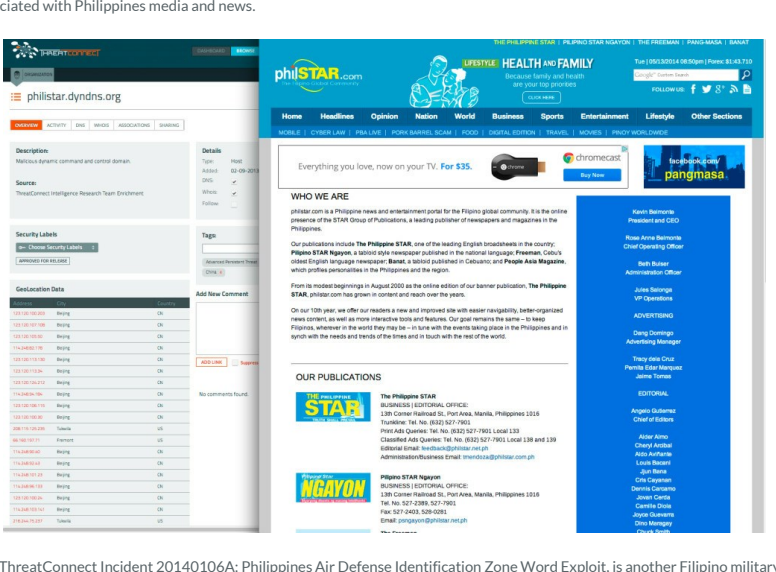
Additionally, users who work for organizations that are often targeted, such as ASEAN, should also avoid providing such a specific email to individuals or organizations that are to likely publish attendance rosters that are publicly available. Such rosters serve as excellent targeting lists for attackers to use within spearphishing operations.

Classified Filipino Document Exploitation:

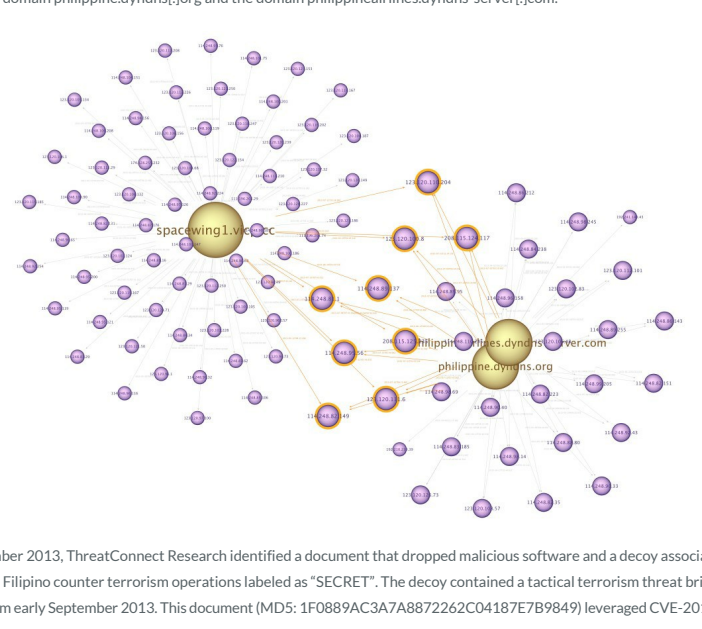
ThreatConnect Research has identified significant targeting of Filipino military and diplomatic entities by China based threat groups. One such incident contains indicators associated with a targeted CVE-2012-0158 exploit that carries a decoy document classified "CONFIDENTIAL", which was a Letter of Instruction referencing a change of command for Philippines Commander Navy Forces West, who are responsible for an area of operations that includes the South China Sea.



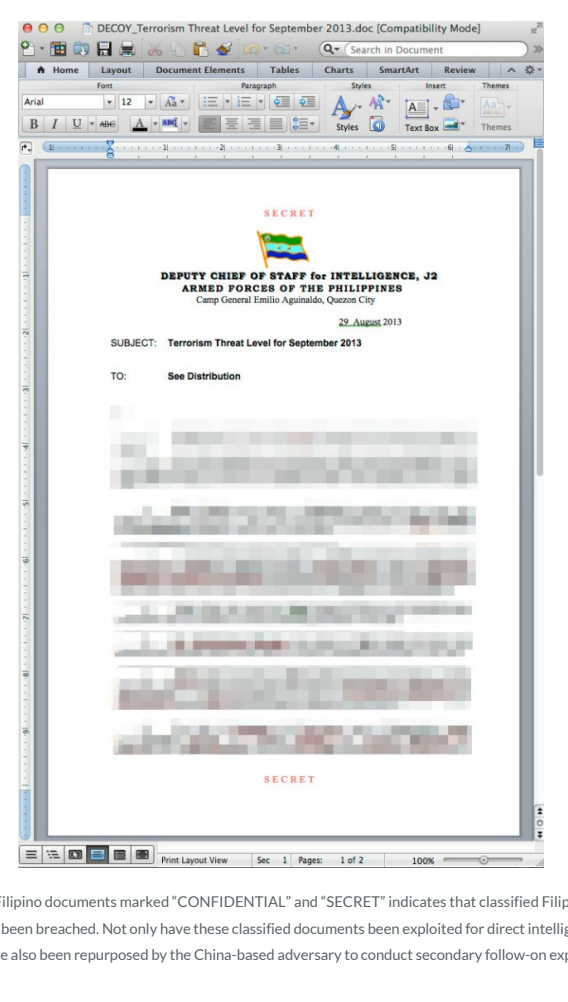
This document exploit (MD5: 92853AF8C12BEF34A568AE93DBDE792C) drops a Mirage RAT APT payload binary (MD5: C4068DC6A813E9BB0EFFCB0F5517B2FB) to %TEMP%iExplorer.exe. The Mirage RAT executable connects to the dynamic command and control domain us.mylftv[.]com. This C2 overlaps with other suspicious dynamic domains such as philistar.dyndns[.]org and phimodel.vicp[.]net, all of which carry a Philippines themed naming convention, suggesting the likelihood of targeting Filipino interests and introduces the possibility of broader targeting of individuals and organizations associated with Philippines media and news.



The ThreatConnect Incident 20140106A: Philippines Air Defense Identification Zone Word Exploit, is another Filipino military themed incident that has been shared within ThreatConnect Subscriber Community. This Incident highlights a targeted CVE-2013-3906 Word exploit (MD5: 3651CA104557572206956C00E4B701B7) that downloads a Mirage self extracting dropper executable (MD5: 1DCD7489F14362BFA96074A64A16D215) from the URL http://mirefocus[.]com/kb2484033.exe. This downloaded payload deployed a Mirage RAT implant (MD5: 3532D7F41D162D0F1B1484938C5A34BA) that connected to the C2 domain spacewing1.vicp[.]cc. This dynamic C2 overlaps with other known Filipino related dynamic domains, such as the sinkholed domain philippine.dyndns[.]org and the domain philippineairlines.dyndns-server[.]com.



In September 2013, ThreatConnect Research identified a document that dropped malicious software and a decoy associated with Classified Filipino counter terrorism operations labeled as "SECRET". The decoy contained a tactical terrorism threat briefing report from early September 2013. This document (MD5: 1F0889AC3A7A8872262C04187E7B9849) leveraged CVE-2012-0158 and dropped an implant with an MD5 hash of 7FDCB9B679DE04B8C68C504E3FFCCC89 that initiated C2 communication with the dynamic domain ebookedit.ticp[.]net.



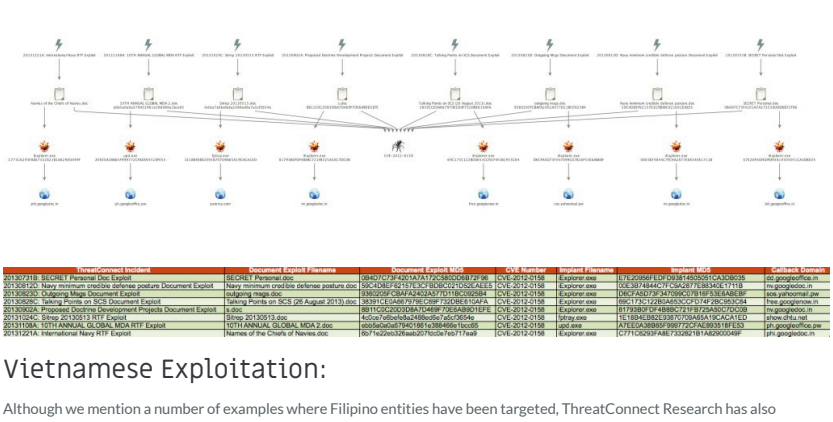
The compromise of Filipino documents marked "CONFIDENTIAL" and "SECRET" indicates that classified Filipino government networks have likely been breached. Not only have these classified documents been exploited for direct intelligence gathering activity, but they have also been repurposed by the China-based adversary to conduct secondary follow-on exploitation campaigns.

From a strategic security perspective, this introduces the possibility that regional partners, as well as international partners like the US Departments of Defense and State, who may currently be sharing classified information or participating in joint operations within the Philippines, may also be subject to compromises of classified digitally stored information, or may find themselves subjected to similar secondary targeting operations. Western and regional military and diplomatic organizations should be wary of sharing classified information with their Filipino counterparts until they can ensure that classified communications and handling process are indeed safeguarded within these sensitive environments.

The "Naikon" Targeting Campaign & "HardCore Charlie":

Additional ThreatConnect Research analysis has identified more document exploits also related to the Philippines Navy. These exploits dropped similar implants interfacing with overlapping infrastructure. The documents were identified as being part of the "Naikon" APT threat campaign. This Chinese APT group primarily targets personnel and organizations who maintain interests within Southeast Asia.

In April 2012, numerous documents were released online by a hacktivist using the online moniker of "Hardcore Charlie." These documents appear to have been sourced and possibly stolen from various businesses and governments in different countries, including the United States, the Philippines, Myanmar, Vietnam, and others. The documents were purported to have been taken by Hardcore Charlie from the Beijing based military contractor China National Import & Export Corp (CEIEC). Many of these stolen documents also contained malicious software that initiated C2 communications with domains that resolve to the same infrastructure as the Filipino military themed campaigns described above.

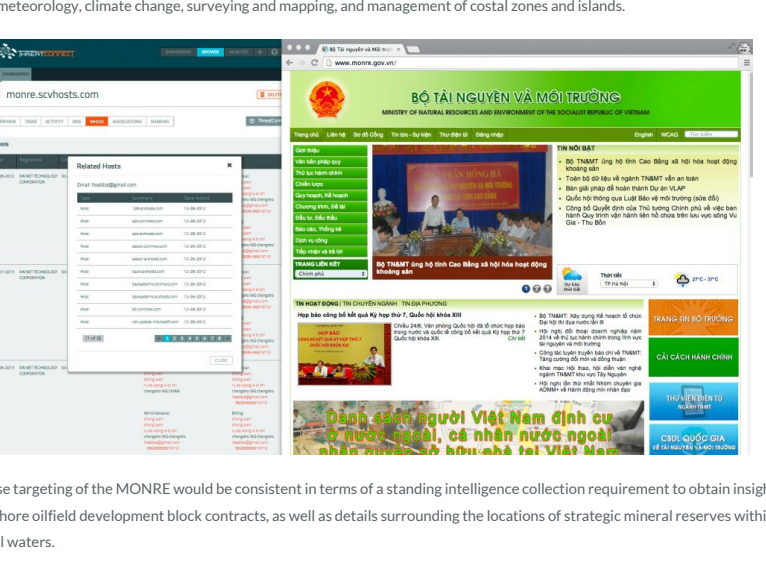


Vietnamese Exploitation:

Although we mention a number of examples where Filipino entities have been targeted, ThreatConnect Research has also consistently observed Vietnamese entities being targeted. This includes individuals and organizations associated with Vietnamese energy development and natural resources. A key observation across several of the campaigns is the naming conventions used by the perpetrators and demonstrate a likely interest in several Vietnamese organizations.

MONRE.scvhosts.com and Vietnamese Ministry of Natural Resources

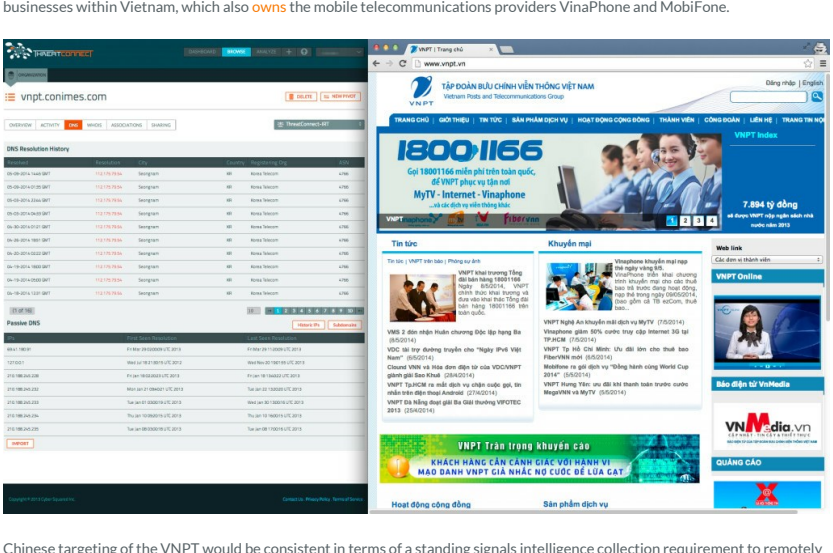
ThreatConnect Research has been tracking the domain "monre.scvhosts[.]com" since December 2012 after enriching infrastructure initially reported within Artem Baranov's analysis of the Chinese backdoor Zegost. The scvhost[.]com domain was registered by the malicious registrant llssddzz@gmail.com that was also identified as being responsible for registering other malicious C2 domains. This sub-domain has likely been used within targeting campaigns against those associated with the Vietnamese Ministry of Natural Resources (MONRE). The MONRE is a Government ministry in Vietnam which responsible for managing natural resources such as land, water, minerals, geology, environmental protection, waste management, hydrometeorology, climate change, surveying and mapping, and management of costal zones and islands.



Chinese targeting of the MONRE would be consistent in terms of a standing intelligence collection requirement to obtain insights to offshore oilfield development block contracts, as well as details surrounding the locations of strategic mineral reserves within coastal waters.

VNPT.conimes.com and Vietnam Posts and Telecommunications Group

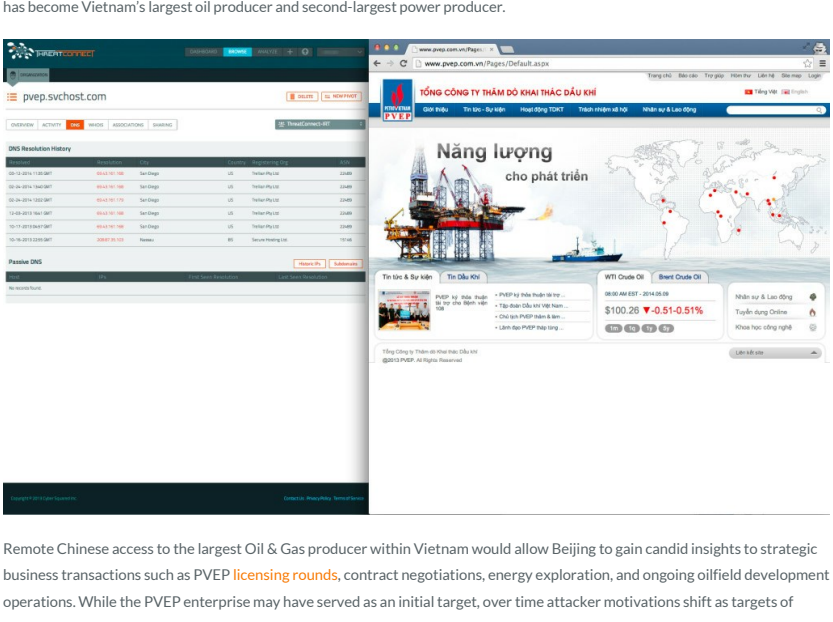
ThreatConnect Research has been tracking the domain vnpt.conimes[.]com since December 2012, which was also identified as an infrastructure enrichment based on the Zegost backdoor analysis. The conimes[.]com was also was registered by the malicious registrant llssddzz@gmail.com. This sub-domain has likely been used within targeting campaigns against individuals and organizations associated with the Vietnam Posts and Telecommunications Group (VNPT). The VNTP is a telecommunications company and the national post office, which is owned by the Vietnamese Government. VNPT is listed as one of the seven largest businesses within Vietnam, which also owns the mobile telecommunications providers VinaPhone and MobiFone.



Chinese targeting of the VNPT would be consistent in terms of a standing signals intelligence collection requirement to remotely obtain digital communications. Remote access to a centrally controlled mobile telecommunications service provider would allow Beijing to leverage a significant voice, data and SMS intercept capability within Vietnam.

PVEP.scvhosts.com and PetroVietnam

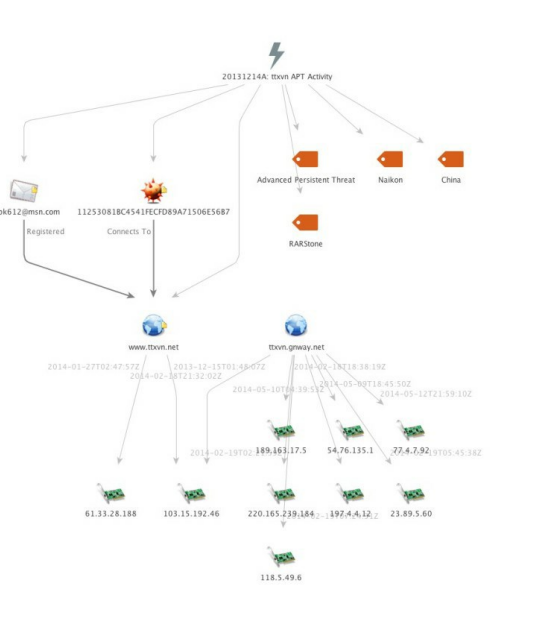
ThreatConnect Research has been tracking the domain "pvep.scvhosts[.]com" since December 2012, which was also identified as an infrastructure enrichment based on the Zegost backdoor analysis. This sub-domain has likely been used within targeting campaigns against those associated with PetroVietnam (PVEP). PetroVietnam is the trading name of Vietnam Oil and Gas Group which is wholly owned by the Vietnamese central government. It is responsible for all oil and gas resources within the country and has become Vietnam's largest oil producer and second-largest power producer.



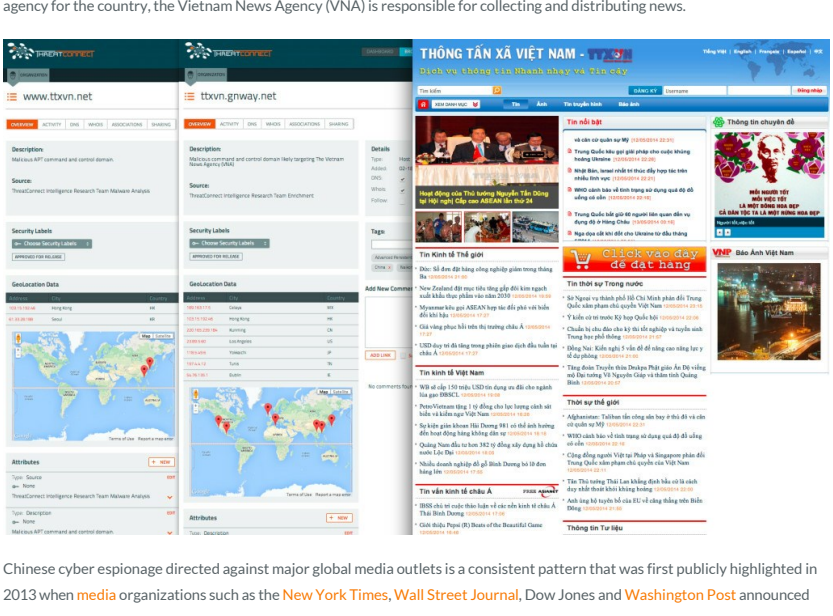
Remote Chinese access to the largest Oil & Gas producer within Vietnam would allow Beijing to gain candid insights to strategic business transactions such as PVEP licensing rounds, contract negotiations, energy exploration, and ongoing oilfield development operations. While the PVEP enterprise may have served as an initial target, over time attacker motivations shift as targets of opportunity present themselves. For example, the Lan Do and Lan Tay gas fields and subsea pipelines are jointly owned by organizations such as British Petroleum and ConocoPhillips and supported by sub-contractors, all of whom are affiliated with majority held PVEP projects. Together, these organizations could easily fall victim to a single threat from one organizational point of entry due to the interwoven and integrated nature of the oil and gas industry's business operations.

TTXVN.gnway.net, TTXVN.net and Thong Tan Xa Viet Nam (Vietnam News Agency)

ThreatConnect Research has been tracking the malicious C2 domains "ttxvn.gnway[.]net" since February 2014 and "www.ttxvn[.]net since December 2013.



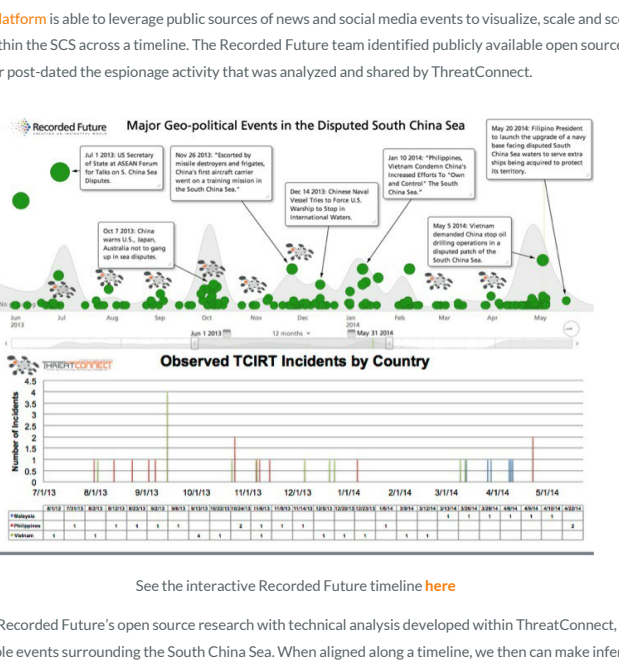
These sub-domains have likely been used within targeting campaigns against individuals and organizations associated with Thong Tan Xa Vietnam (TTXVN), an official Vietnamese Government Agency and the official news provider. As the central news agency for the country, the Vietnam News Agency (VNA) is responsible for collecting and distributing news.



Chinese cyber espionage directed against major global media outlets is a consistent pattern that was first publicly highlighted in 2013 when media organizations such as the New York Times, Wall Street Journal, Dow Jones and Washington Post announced that they all were victim to Chinese cyber espionage. Remote access to individual journalists, as well as larger media organizations, allow attackers to obtain candid insights to sensitive information such as journalists' sources or the production schedules of news stories that may be perceived as negative or derogatory to China.

ThreatConnect & Recorded Future Joint Collaboration:

Armed with this analysis, ThreatConnect Research shared our findings with our friends at Recorded Future. Recorded Future's web intelligence platform is able to leverage public sources of news and social media events to visualize, scale and scope geo-political events within the SCS across a timeline. The Recorded Future team identified publicly available open source content that either pre-dated or post-dated the espionage activity that was analyzed and shared by ThreatConnect.



See the interactive Recorded Future timeline here

When we overlay Recorded Future's open source research with technical analysis developed within ThreatConnect, we can visualize the notable events surrounding the South China Sea. When aligned along a timeline, we then can make inferences as to the likely cause and effects in which attackers may have used network exploitation campaigns to leverage information from several South China Seas nations. These complementary views deliver key perspectives that analysts may leverage to better understand context and deliver effective decision support for todays technical and business leaders.

Likely Attacker Motives:

History of Conflict in the South China Sea

According to the think tank, Council on Foreign Relations, China, Taiwan, Vietnam, Malaysia, Brunei and the Philippines all have historical territorial claims in the South China Sea, particularly over rights to exploit oil and gas reserves. The Philippines and Vietnam have most prominently disputed Chinese territorial claims. Vietnam and the Philippines consider territories in the South China Sea important to national security, trade routes, traditional fishing grounds and a source of offshore energy resources.

Vietnam and the Philippines have supported the U.S. pivot to Asia, while also reaching out diplomatically to garner support to counter China's growing aggression in the SCS. The Philippines have been utilizing assistance from Japan and the U.S. to augment its defense and maritime law enforcement capabilities while Vietnam looks to India and Russia to counter China in the region. Both countries also plead their case in the SCS dispute to ASEAN.

In early 2014, the Philippines went to the United Nations to arbitrate their dispute over China's nine-dashed line, which has been widely considered a weak basis for extensive Chinese claims in the SCS. This increased tensions with China, who has been insistent on negotiating territorial disputes in the SCS with other countries individually.

International Oil Interests in the South China Sea

According to the U.S. Energy Information Administration (EIA), "Asia's robust economic growth boosts demand for energy in the region projects total liquid fuels consumption in Asian countries outside the Organization for Economic Cooperation and Development (OECD) to rise at an annual growth rate of 2.6 percent, growing from around 20 percent of world consumption in 2008 to over 30 percent of world consumption by 2035. EIA expects China to account for 43 percent of that growth. With Southeast Asian domestic oil production projected to stay flat or decline as consumption rises, the region's countries will look to new sources of energy to meet domestic demand. China in particular promotes the use of natural gas as a preferred energy source and set an ambitious target of increasing the share of natural gas in its energy mix from 3 percent to 10 percent by 2020. The South China Sea offers the potential for significant natural gas discoveries, creating an incentive to secure larger parts of the area for domestic production."

China ADIZ in East China Sea

On 23 November 2013, the New York Times reported that "the Chinese government claimed the right to identify, monitor and possibly take military action against aircraft that enter a newly declared "air defense identification zone," (ADIZ) which covers sea and islands also claimed by Japan and threatens to escalate an already tense dispute over some of the maritime territory." Following that the New York Times reported that "two long-range American bombers flew through contested airspace over the East China Sea, days after the Chinese announced they were claiming the right to police the sky above a vast area that includes islands at the center of a simmering dispute with Japan." DoD officials claimed this was a training exercise scheduled long in advanced of China's newly declared air defense identification zone. According to a Japanese report in late January 2014, China is considering declaring a new ADIZ over the SCS, a move likely to increase tensions in the area.

Recent Tensions in the South China Sea

In May of 2014, nearly a week after China National Offshore Oil Corporation drilling rig (HD-981), deployed 120 nautical miles off the coast of Vietnam in an area that Vietnam claims is within its exclusive economic zone, Vietnamese officials revealed a video of Chinese vessels using water cannons and ramming Vietnamese fishing ships. This came just a day after Philippines authorities seized a Chinese fishing boat, eventually charging its crew for poaching endangered sea turtles near the Parcel Islands. This recent clash has caused regional uncertainty and instability, both of which have negatively impacted the Vietnamese stock market with a significant 13% decline.

Regional entities are not the only ones to fall victim to increased Chinese aggression within the SCS. In December 2013, China deployed its first aircraft carrier, the Liaoning, to the SCS. According to reports, during this deployment, the USS Cowpens, A U.S. guided missile cruiser operating in international waters within the SCS was forced to take evasive action on December 5, 2013 to avoid a collision with a Chinese warship maneuvering nearby. The incident came as the USS Cowpens was operating in the vicinity of the Liaoning.

Conclusion:

As fissures erupt along geographic boundaries within the SCS, those affiliated with regional interests should expect to see an increase in cyber activity surrounding real world events. International bodies such as ASEAN and the United Nations, as well as individual nations, should expect to see targeted attacks from sophisticated operators seeking to monitor internal communications or bi-lateral / multi-lateral exchanges between member nations. China's ability to maintain a remote persistence within these targeted enterprises and exploit information provides Beijing with the agility to influence or counter regional policy developments or international arbitration.

Individuals affiliated with national level military, diplomatic or economic interests within the SCS should seek to safeguard any communications, including classified material, when engaging in information exchanges with their Filipino counterparts. Filipino entities responsible for safeguarding classified information should review their classified networks and validate that there are indeed no network breaches or cross-domain violations. International partners, for example USPACOM or USSOCOM, who may be actively sharing classified data with the Philippines during training exercises or while conducting joint counter-terrorism operations, may want to consider using alternate communication mediums until classified networks and systems can be secured.

As individual SCS nations seek to address China's growing assertiveness they should be mindful that Chinese cyber espionage remains the primary "low risk, high payoff" tactic of choice for the Chinese. While nations like the Philippines have been the most outspoken against Chinese aggression, SCS nations such as Vietnam are now experiencing the effects of Beijing's self interest. The intent is clear, not only will China continue to test physical boundaries but will do so by aggressively seeking to position themselves deep within the digital infrastructure and key centers of gravity of SCS nations.

Although western commercial interests may be geographically insulated from the SCS, they are not immune to regional cyber espionage. Industries such as energy, mining, and transportation may find themselves directly or indirectly impacted as regional tensions ebb and flow. It is important for those within these sectors to actively invest in threat intelligence processes as a standard business practice that supports internal information security operations. It is equally important that technical leaders effectively interpret and articulate such regional threats and the context surrounding them to corporate business leaders.

Organizations must assess and acknowledge the likelihood that they may be target, if not compromised, but without adopting a victim mindset. By proactively seeking to routinely acquire and fuse technical and non-technical geo-political context to seemingly isolated security events, organizations can develop a richer understanding of sophisticated threats and their motivations which ultimately enables organizations with stronger cooperate decision support.

If you are interested in leveraging the industries most comprehensive threat intelligence platform to aggregate, analyze and act on threat intelligence, register for a ThreatConnect account and join our communities, access these incidents and the associated signatures. To contact us directly, please reach out to PR@threatconnect.com.

PREVIOUS POST
05.05.14
ThreatConnect Enables "Healthy Networking" for the Biomed and Life Sciences...

NEXT POST
06.19.14
How To Streamline Threat Intel Sharing Before Lunch

About the Author

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