The Anthem Hack: All Roads Lead to China

Posted February 27, 2015 by ThreatConnect Intelligence Research Team (TCIRT)[1] filed under Threat Research[2].

UPDATE: Premera Latest Healthcare Insurance Agency to be Breached[3]

When news of the Anthem breach was reported on February 4th, 2015, the security industry quite understandably went wild. A breach of this magnitude was certainly unprecedented. Naturally, many industry professionals were keenly interested in digging into this incident to see what could be uncovered, and the research team at ThreatConnect was no exception. Thanks to our powerful API[4] and third-party partner[5] integrations, we were able to use ThreatConnect to quickly uncover a wealth of intelligence even when initially hindered by a relative lack of investigative lead information and context, a key requirement of any Threat Intelligence Platform[6] (TIP). However, before we delve into what we were able to uncover, let's briefly review the facts as they stood in the wake of the initial discovery announcement.

What We Know:

On the morning of February 4th, 2015, several major news outlets broke the story[7] that Anthem, Inc.'s network defenses had been breached. According to a statement from Anthem's CEO[8], the company fell victim to a "very sophisticated external cyber attack," and the hackers "obtained" the personally identifiable information (PII) of approximately 80M customers. This included social security numbers, birthdays, street addresses, phone numbers and income data – plenty of information to enable identity theft. This was a significant event for several reasons:

- Anthem, formerly known as Wellpoint, is the largest managed healthcare company in the Blue Cross Blue Shield Association, and by extension, one of the largest healthcare organizations in the United States. As such, any compromise, no matter how insignificant, would likely impact countless individuals.
- Blue Cross Blue Shield provides healthcare coverage for about half the U.S. federal workforce. This means that their information was potentially compromised too.
- Unlike the Sony hack which was destructive in nature and meant to send a message for coercive purposes, the Anthem compromise was purportedly very covert, a fact which may suggest something about the adversary's motives.
- As of late February 2015, there have not been any indications that the exfiltrated PII data was immediately commoditized on the black market for the purpose of enabling identity theft, as was the case in the Home Depot Breach.

Filling the Gaps:

Obviously, these high-level observations do not provide cybersecurity researchers a great deal of information to work with. However, when presented within the context of a Threat Intelligence Platform (TIP), an incomplete trail of evidence can highlight intelligence gaps, a study of which can orient threat researchers towards their analytic objectives. To this end, let's examine what we wanted to discover in the context of the Anthem breach:

- Who was responsible for the attack?
- What was the objective of the attack? Was it cyber theft, an espionage operation, or something different?
- Who was targeted in the attack? The answer to this question, obscured as it may be, would likely shed some light on the objective of the breach.
- What was the timeline of the activity?

The real power of a Threat Intelligence Platform is demonstrated when you are able to collect and maintain a robust dataset of threat indicators, both past and present, which can help orient you in the right direction in the wake of a newly discovered breach. Even when you do not have a good deal of information to start with (for example a file hash, or an IP address), you may find leads by pivoting through archived datasets until you uncover key pieces of the puzzle. In the case of the Anthem breach, we were able to do just that.

Anthem Themed Infrastructure & Signed Malware:

In September 2014, the ThreatConnect Intelligence Research Team (TCIRT)[9] observed a variant of the Derusbi APT malware family, MD5: 0A9545F9FC7A6D8596CF07A59F400FD3[10], which was signed by a valid digital signature from the Korean company DTOPTOOLZ Co. Derusbi is a family of malware used by multiple actor groups but associated exclusively with Chinese APT. TCIRT began tracking the DTOPTOOLZ signature for additional signed malware samples and memorialized them within our Threat Intelligence Platform over time.

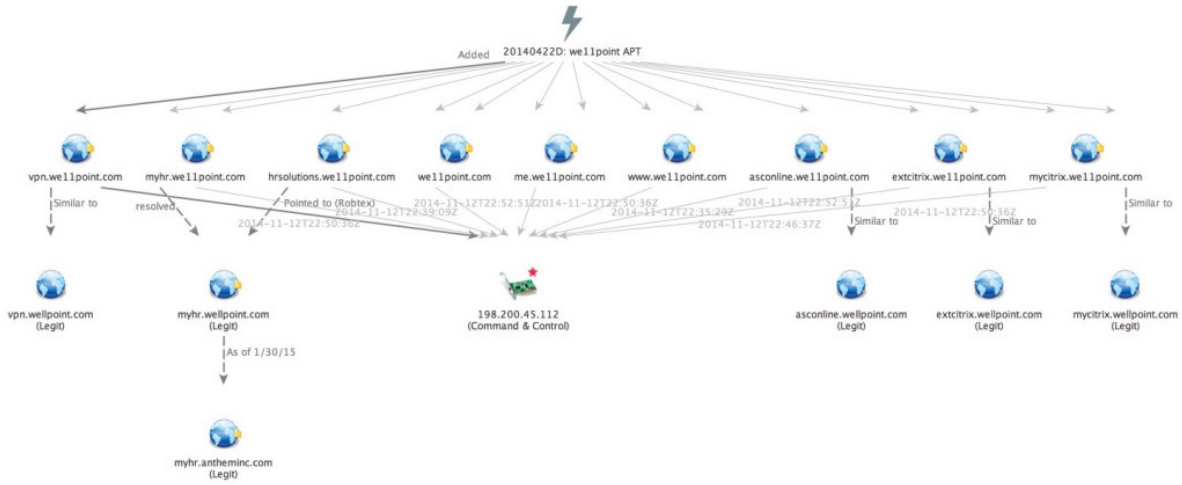
Analyst Comment: The DTOPTOOLZ signature has also been observed in association with Korean Adware that is affiliated with the actual DTOPTOOLZ Co. This adware should not be confused with the APT malware that is abusing the same digital signature.

Later, in mid-November we discovered another implant that was digitally signed with the DTOPTOOLZ signature. This implant, MD5: 98721c78dfbf8a45d152a888c804427c[11], was from the "Sakula" (aka. Sakurel) family of malware, a known variant of the Derusbi backdoor, and was configured to communicate with the malicious command and control (C2) domains extcitrix.we11point[.]com and www.we11point[.]com. Through our Farsight Security passive DNS[12] integration, we uncovered that this malicious infrastructure was likely named in such a way to impersonate the legitimate Wellpoint IT infrastructure.

Passive DNS and historic DomainTools Whois data also provided insights that helped establish an initial timeline dating back to April 2014, when the faux domains came into existence and were later operationalized by the attackers. A Threat Intelligence Platform should allow for analysts to easily put together and organize such insights, collaborate around relevant analysis internally, and share the finished analysis with external industry groups and organizations. In the hopes that our community members could benefit from or provide further insight into this suspicious incident, we immediately shared our threat intelligence including indicators, signatures and analytical context to the ThreatConnect Medical and Health Community[13] on November 13, 2014. This included sending out a notification to all stakeholders as well as our followers on Twitter[14].

When the Anthem breach later came to light in early February, we re-shared the signatures, indicators and context freely to the entire ThreatConnect user base. As we dug further, we expanded our understanding of the malicious we11point[.]com infrastructure, taking particular interest to the subdomains such as “extcitrix.we11point[.]com and “hrsolutions.we11point[.]com”. Note the “citrix” and “hr” (human resources) prefixes that the adversary used to mirror legitimate remote infrastructure and employee benefits resources in the May 2014 timeframe. This provided initial insights as to the likely targeting themes and or vectors in which the adversary may have used when initiating their targeting campaign.

[15]



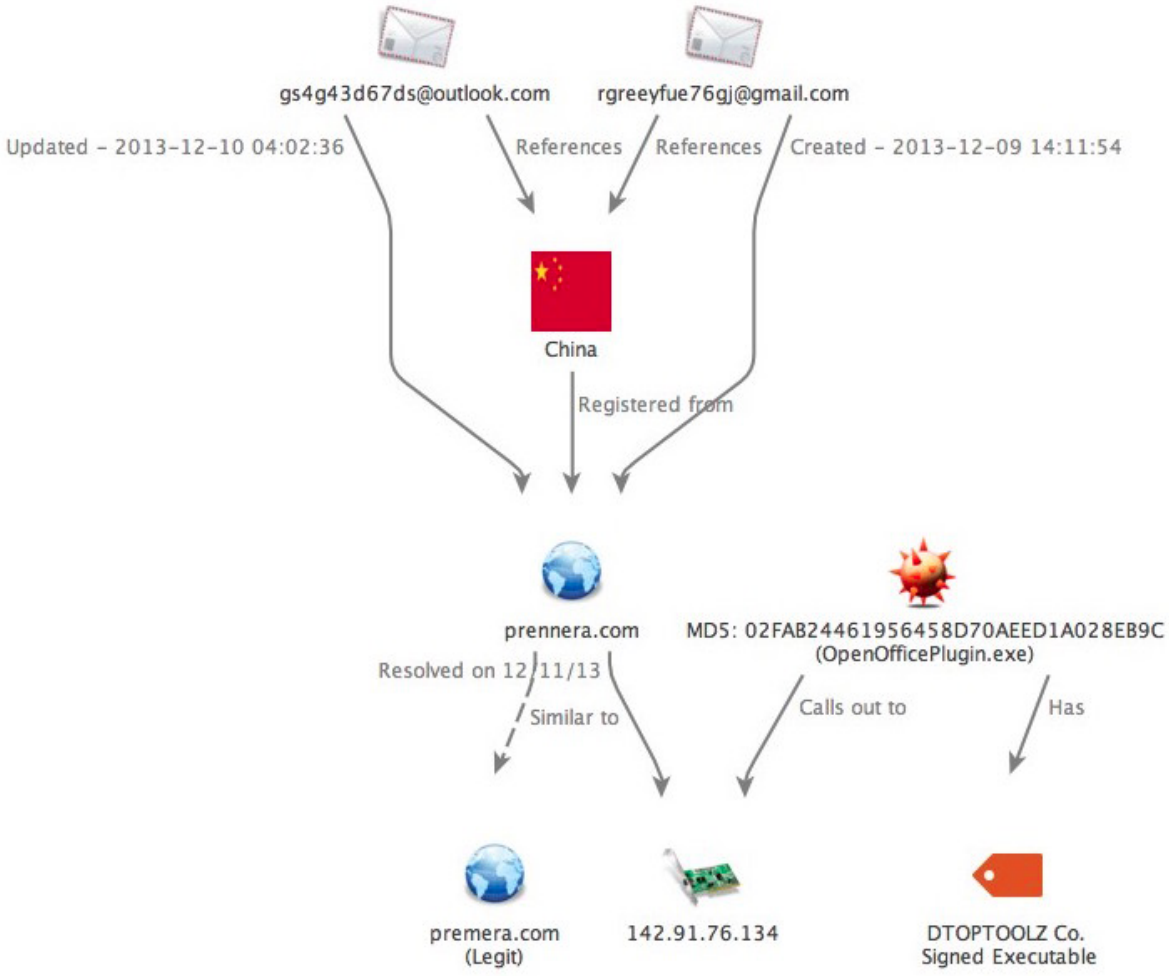
[16]

The fact that the malicious infrastructure closely mirrored other legitimate Wellpoint infrastructure supported our hypothesis that the Derusbi / Sakula malware was configured to operate and persist within a specific target enterprise.

Possible Premera Blue Cross Infrastructure:

Retrospective analysis of other targeted malware samples using the DTOPTOOLZ Co. digital signature led to the identification of an “HttpBrowser” / “HttpDump” implant MD5: 02FAB24461956458D70AEED1A028EB9C[17] (OpenOfficePlugin.exe), which was first observed on December 11, 2013. Although this malware sample is not Derusbi / Sakula, it too is strongly believed to be associated with Chinese APT activity and in fact may have also been involved in a Blue Cross Blue Shield

targeting campaign as early as December 2013.



[18]

This particular binary is configured to connect to the static IP address 142.91.76[.]134. Passive DNS of this IP indicates that on December 11th, 2013, the same date as the malware sample was observed, the domain prennera[.]com also resolved to 142.91.76[.]134. It is believed that the prennera[.]com domain may have been impersonating the Healthcare provider Premera Blue Cross[19], where the attackers used the same character replacement technique by replacing the “m” with two “n” characters within the faux domain, the same technique that would

be seen five months later with the we11point[.]com command and control infrastructure.

Section Summary:

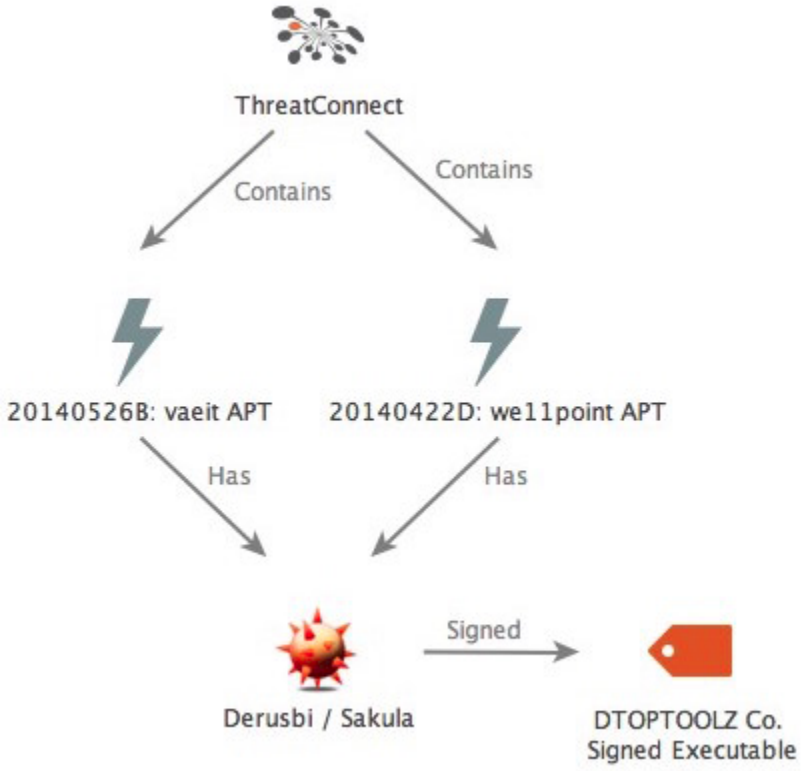
- The Derusbi / Sakula malware implant types are unique in that they have traditionally been seen within Chinese APT espionage campaigns.
- The “HttpBrowser” / “HttpDump” malware implant (while a different family of malware than Derusbi / Sakula) is also believed to be of Chinese origin, and was also digitally signed with the DTOPTOOLZ digitalsignature. This implant connected to a C2 node that overlapped with prennera[.]com.
- We believe that the prennera[.]com domain may be impersonating Premera Blue Cross (premera.com), using a similar character replacement technique seen in the we11point[.]com campaign.

VAE Inc. Themed Infrastructure & Signed Malware

Another powerful attribute of ThreatConnect is the ability for analysts to logically group items such as atomic indicators, related documents or signatures, all of which may include individualized custom context enrichments and associations. Over time, the ability to memorialize groupings of related or like activity allows analysts to quickly uncover non-obvious relationships within their private datasets. This is exactly what happened as we continued to

investigate these incidents.

As industry analysts and media speculated Chinese APT involvement[20] in the Anthem breach, our focus into the Derusbi / Sakula malware signed with the DTOPTOOLZ Co. digital signature shifted from the we11point[.]com incident to another cluster of activity that occurred later in May 2014. We immediately reviewed Incident 20140526B: vaeit APT[21], an incident that we initially shared to our Subscriber Community on September 29, 2014 after conducting retrospective analysis.
[22]



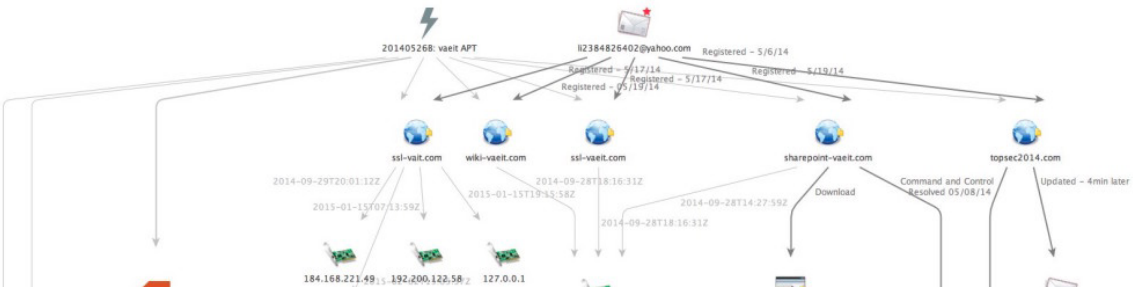
[23]

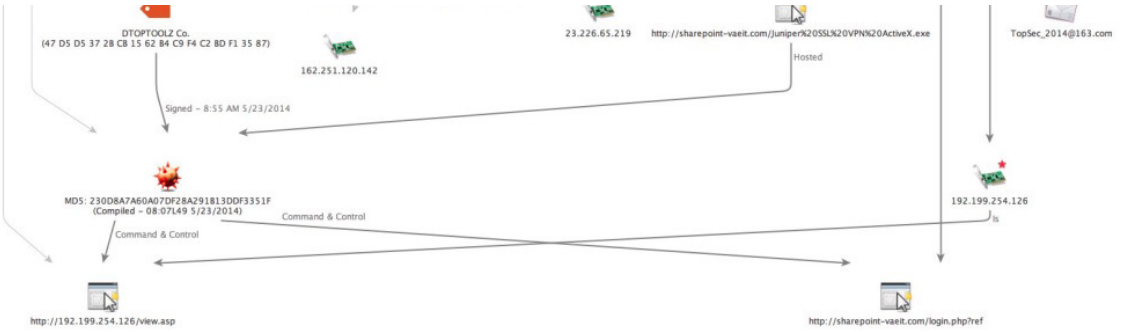
Just as was the case with the we11point[.]com and prennera[.]com

incidents, the VAE, Inc. incident is also believed to be associated with Chinese APT espionage activity. In this case the adversary also used Derusbi / Sakula malware that was signed with the DTOPTOOLZ Co. digital signature and configured to communicate with faux infrastructure appearing to be masquerading as internal resources for the Department of Defense Contractor VAE, Inc. Additionally, in response to an inquiry from KrebsOnSecurity, VAE, Inc. would later confirm[24] that it had indeed been a target of a failed spearphishing attempt in May 2014 which used the malicious faux VAE, Inc. themed domain.

The targeted incident relied upon the Sakula executable MD5: 230D8A7A60A07DF28A291B13DDF3351F[25] which had a XOR 0x9A encoded C2 callbacks to the IP address 192.199.254[.]126 (registered to Wehostwebsites[.]com – "Tom Yu" of Baoan, Shenzhen City, Guangdong Province, China) as well as a hardcoded callback to sharepoint-vaeit[.]com. Passive DNS of the static C2 IP 192.199.254[.]126 revealed a single suspicious domain of interest – topsec2014[.]com. This domain had historic resolution around May 8, 2014 within a month of the first observed Sakula activity using the IP 192.199.254[.]126 as C2.

[26]



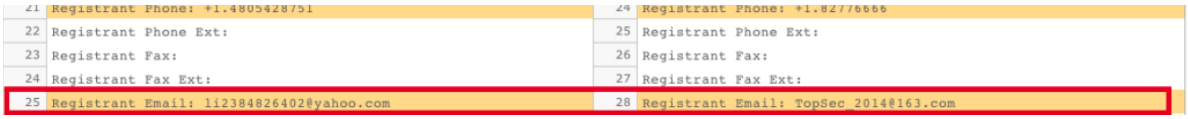


[27]

Using historic Whois, we discovered that topsec2014[.]com was initially registered by li2384826402@yahoo[.]com on May 6th, 2014. Although the li2384826402@yahoo[.]com registrant is likely a reseller given that it has been observed registering several thousands of other domains, the fact that it was used to register both the faux VAE, Inc. C2 infrastructure and the overlapping domain topsec2014[.]com within the same month suggests that there may be a relationship between the client of the reseller for the VAE, Inc. infrastructure and the client for topsec2014[.]com.

[28]

Domain Name: TOPSEC2014.COM	Domain Name: TOPSEC2014.COM
Registry Domain ID: 1857525015_DOMAIN_COM-VRSN	Registry Domain ID: 1857525015_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com	Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com	Registrar URL: http://www.godaddy.com
Update Date:	Update Date: 2014-05-06 04:52:21
Creation Date: 2014-05-06 04:48:49	Creation Date: 2014-05-06 04:48:49
Registrar Registration Expiration Date: 2015-05-06 04:48:49	Registrar Registration Expiration Date: 2015-05-06 04:48:49
Registrar: GoDaddy.com, LLC	Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146	Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com	Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.480-624-2505	Registrar Abuse Contact Phone: +1.480-624-2505
Domain Status: ok	Domain Status: clientTransferProhibited
	Domain Status: clientUpdateProhibited
	Domain Status: clientRenewProhibited
	Domain Status: clientDeleteProhibited
Registry Registrant ID:	Registry Registrant ID:
Registrant Name: li ning	Registrant Name: Top Sec
Registrant Organization:	Registrant Organization: TopSec
Registrant Street: guangdongsheng	Registrant Street: china
Registrant City: guangzhoushi	Registrant City: china
Registrant State/Province: Alabama	Registrant State/Province: china
Registrant Postal Code: 54152	Registrant Postal Code: 100000
Registrant Country: United States	Registrant Country: China



[29]

Just four minutes after the initial registration of topsec2014[.]com, the Whois records were updated from the initial registrant, Li Ning – li2384826402@yahoo[.]com to TopSec China – TopSec_2014@163[.]com. This domain record has been unchanged since May 7th 2014. The we11point[.]com infrastructure and by extension the faux VAE Inc. infrastructure is associated with Cluster 2 of the ScanBox framework[30] by PwC. The latest PwC update to ScanBox states that there are *"links between the domain allegedly used in the Anthem hack (we11point.com) to Cluster 2 through shared WHOIS details."*

OPM Themed Infrastructure

One notable pattern was how the domain Whois registration information for the VAE, Inc. themed infrastructure was quickly updated and obfuscated with pseudorandom 10 character gmx.com email addresses and using the names of various comic book characters from the Iron Man franchise. This comic-themed naming convention has been previously documented by our friends at Crowdstrike[31] in what they characterize as being associated with a Chinese APT group they have dubbed "Deep Panda".

Leveraging our DomainTools partnership, we were able to

correlate the outlier domain opm-learning[.]org. This domain was also purportedly registered by the Iron Man movie hero "Tony Stark" on July 28, 2014. This infrastructure naming convention suggests a possible Office of Personnel Management (OPM) theme. However, in this case we lacked any specific sample of malware to verify our initial suspicions that this infrastructure was operational. The possible OPM reference in the domain name is noteworthy considering it was revealed in July of 2014 that OPM had been compromised[32] by a likely state-sponsored Chinese actor in mid-March of that year. The fact this domain was registered after the breach occurred suggests that OPM could be an ongoing direct target of Chinese state-sponsored cyber espionage activity.

Our attention then turned to the FBI Flash Report A-000049-MW[33] that was publicly reported by Brian Krebs [34]on February 6th, 2015. This FBI Flash Report was issued on January 27th, 2015, the same day an Anthem administrator detected suspicious activity according to an internal memo[35]. This memo goes on to indicate that the FBI would not be party to the Anthem breach until they were notified on January 29th, 2015; based on these facts we assess with high confidence that it is very unlikely that the FBI Flash Report was directly related to the Anthem breach. Rather, we suspect that the FBI flash report likely references the USIS breach that was announced[36] on August 6, 2014, or the previous OPM breach, considering the statement that the breach involved *"compromised and stolen sensitive business information and Personally Identifiable Information (PII) from US commercial and*

government networks through cyber espionage."

The malware referenced within the FBI Report is associated with a Derusbi backdoor subvariant named "InfoAdmin" / "Kakfum" where the FBI specifically references open source reporting of "Deep Panda" as being related to the malware observed in the attack. The malicious infrastructure highlighted in the report are the domains images.googlewebcache[.]com and smtp.outlookssl[.]com. Both of these top level domains were included with other related domains, all of which were shared on September 16th, 2013 to the ThreatConnect Subscriber Community in Incident 20130823C: Some.Trouble APT Domains[37], roughly a year and half prior to the FBI Flash report.

It is important to mention that both the domains images.googlewebcache[.]com and smtp.outlookssl[.]comas were also previously identified in an October 2014 PwC blog post[38] as seen within Cluster 1 of the Scanbox framework, while the Sakula activity with we11point and VAEIT is contained within Cluster 2 of that report. This implies that the actor referenced within the FBI Flash report uses shared capabilities (in this case the ScanBox kit) with the Sakula / we11point actor.

Section Summary:

- The Derusbi / Sakula malware seen in both the we11point[.]com and VAE Inc. campaigns were structurally the same and digitally signed with the DTOPTOOLZ signature.

- The emerging theme is that this particular signature and family of malware is highly indicative of a particular Chinese APT activity.
- Within this web of malicious infrastructure, there is an interesting overlap with the topsec2014[.]com domain and attack infrastructure.
- TCIRT identified a domain opm-learning[.]org that had a similar superhero themed WHOIS registrant to the Sakula / VAE Inc. infrastructure. The possible OPM reference is noteworthy considering the Office of Personnel Management (OPM) was compromised in March 2014. Additionally, an FBI Flash Report 0000-49MW referenced indicators that were possibly associated with the USIS hack and a Derusbi variant called “Kakfum” / “InfoAdmin”. Both the FBI Flash infrastructure and the Sakula / VAE Inc. infrastructure are tied to the capability usage of the ScanBox framework, residing in Clusters 1 and 2 respectively.

Unveiling Song Yubo and Southeast University:

The Professor

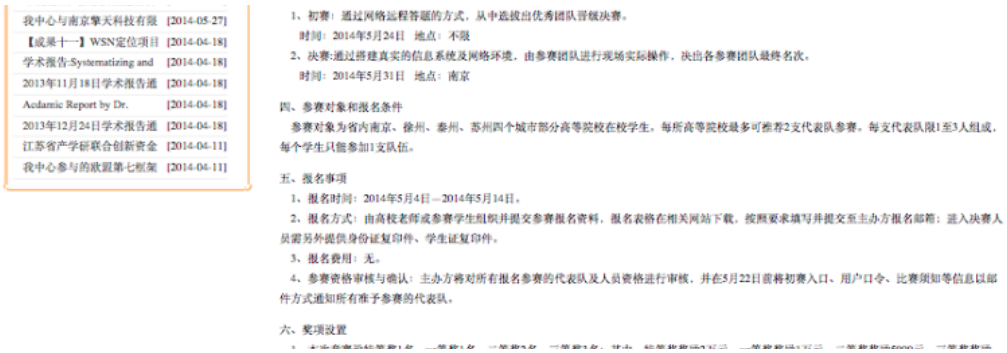
We conducted open source research in pursuit of further information on the TopSec_2014@163[.]com email registrant. A keyword search returned several results for “topsec2014@163[.]com” in association with a number of academic institutions in Nanjing, China. Although the email

address wasn't an exact match to the topsec2014[.]com domain registrant (notice the absence of the underscore), such a similarity warranted further investigation.
[39]

[40]

We examined the links for any relevant intelligence, and discovered that nearly all of the search results led to pages that contained an announcement for an information security competition sponsored by the Southeast University-Topsec Information Security and Mobile Internet Technology Joint Research Center. This entity appears to be a joint research venture between the University and Chinese networking giant Beijing Topsec Network Security Technology Co., a.k.a. Beijing Topsec.

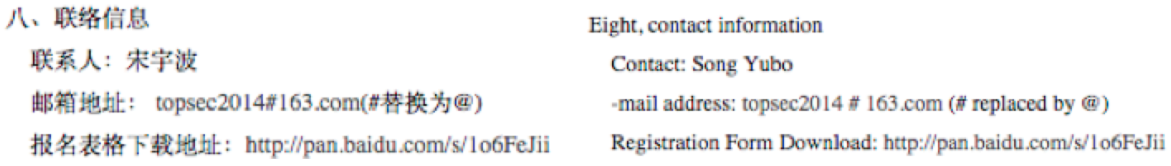
[41]



[42]

The announcements list a Professor “Song Yubo” as the point of contact for the event, and directs interested parties to his email address, topsec2014@163[.]com, for further questions.

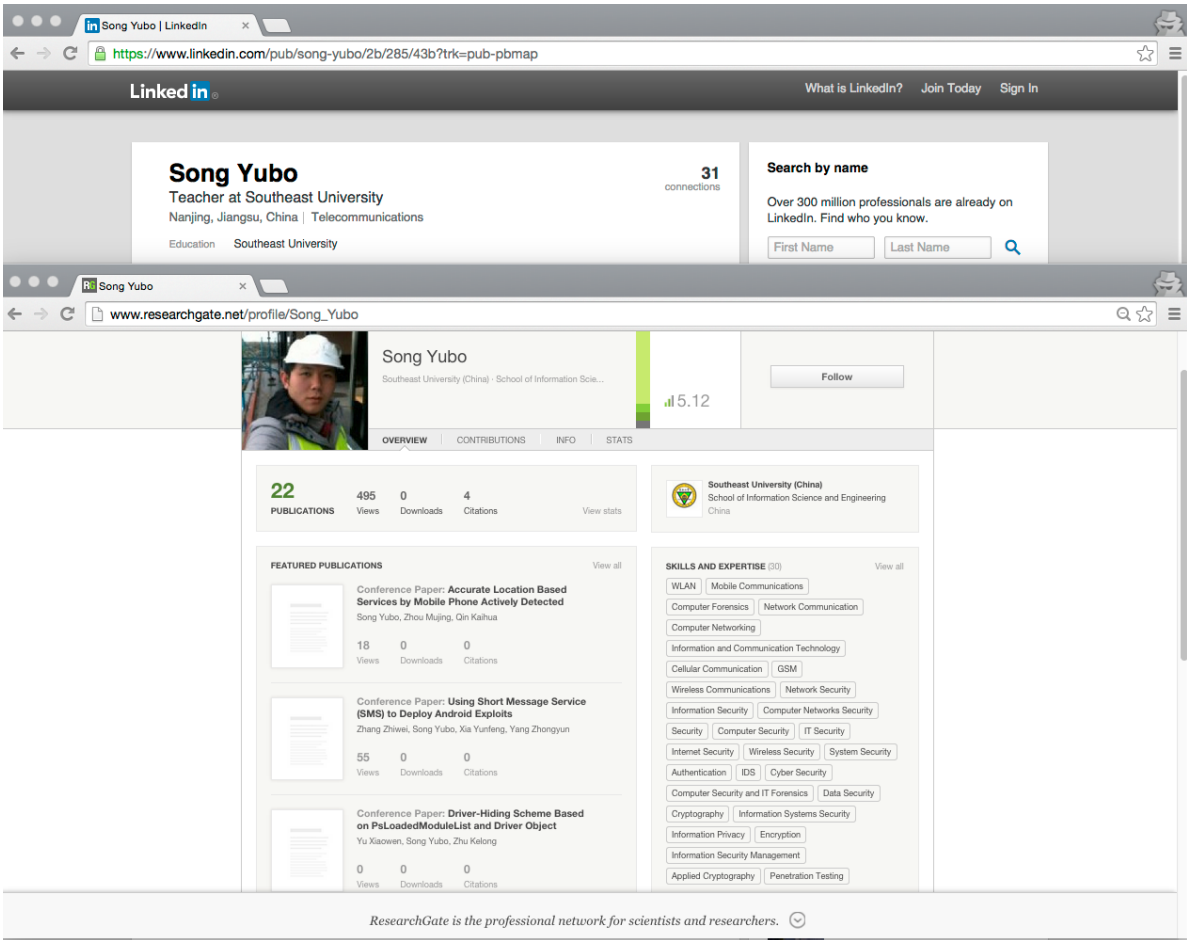
[43]



[44]

According to his LinkedIn page, Song is a Teacher at the Southeast University, specifically interested in the field of telecommunications. Additionally, he is an avid researcher, and has published numerous academic papers on computer network exploitation on various e-journal publication sites, such as Google Scholar[45]. Further, he lists skills such as “cryptography,” “penetration testing” and “computer network security,” etc. on his Research Gate profile[46].

[47]



[48]

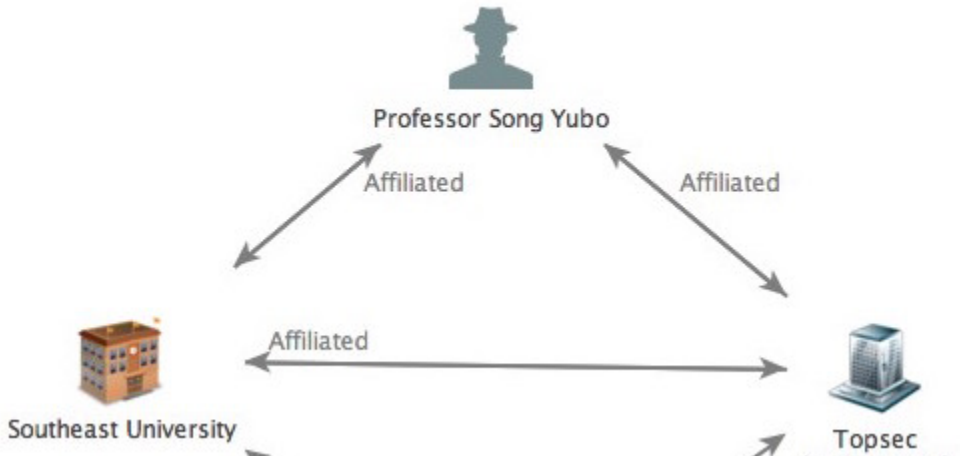
As we continued to develop a profile on Professor Song, we began to have the sense that his interest in information security research strongly overlapped with that of someone who might be interested in or at least capable of conducting sophisticated cyber attacks. However, interests alone are not enough to warrant reasonable suspicion, so we had to do more digging.

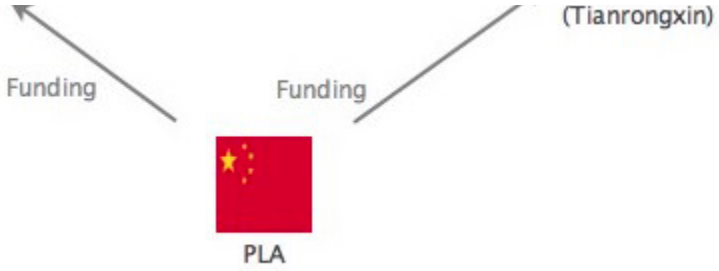
Additionally, the soft link between TopSec_2014@163[.]com and topsec2014@163[.]com alone was not sufficient to make

associations with any reasonable confidence, but as it turns out, Yubo has in fact been previously named as a person of interest in the context of offensive Chinese cyber activity.

The University

In March 2012, Northrop Grumman presented a commissioned report to Congress[49] detailing Chinese cyber warfare capabilities. The report asserts with high confidence that both Song and the Information Security Research Center at Southeast University have received numerous state-sponsored research grants, and by extension, cooperated with the Government of China in conducting information security research and development (R&D). As stated on Southeast University's own website, the main purpose of these grants are to develop technical acumen amongst its students via providing support for "state-owned scientific research institutions, state key enterprises, government agencies and People's Liberation Army (PLA) units."
[50]





[51]

Southeast University is one of only three Chinese academic institutes that receives funding from all five of the State grant programs. Song himself has also conducted his fair share of state-sponsored research, notably under the National Ministry of State Security 115 Program – a highly sensitive research grant to fund ambiguous information warfare R&D, almost certainly in support of PLA programs.

The Competition

As we can see, the evidence continued to stack up. The real smoking gun, however, was when we began to notice a strong temporal overlap with the various stages of the TOPSEC Cup that Song and Beijing Topsec were organizing, and the registration dates of malicious infrastructure as well as the malware compilation dates.

[52]

Competition Timeline	topsec2014 Infrastructure	VAE Inc. Juniper SSL Malware	Faux VAE Inc. Infrastructure
	May 6, 2014: topsec2014[.]com registered by li2384826402@yahoo[.]com at 04:48:49; email registrant		**May 17, 2014**: ssl-vaeit[.]com registered by li2384826402@yahoo[.]com at 06:51:01; changed to "Dubai Tycoon" at 06:56:27.

May 4 - 14 2014: Registration period	changed to TopSec_2014@163[.]com at 04:52:21. **May 8, 2014**: topsec2014[.]com resolves to 192.199.254.126. **May 10, 2014**: topsec2014[.]com does not resolve.	***	**May 19, 2014**: wiki-vaeit[.]com registered by li2384826402@yahoo[.]com at 22:38:41; changed to "Tony Stark" at 22:40:02. **May 19, 2014**: sharepoint-vaeit[.]com registered by li2384826402@yahoo[.]com at 01:06:10; changed to "Natasha Romanov" at 01:09:48.
May 24, 2014: Preliminary remote access round	**May 22, 2014**: topsec2014[.]com resolves to 123.1.157.179. **May 24, 2014**: Changed name server from "NS11.DOMAINCONTROL.COM" to "NS1.JIASULE.NET".	**May 23, 2014**: Juniper SSL VPN ActiveX.exe compiled at 08:07:49, signed at 08:55:00; configured to call out to sharepoint-vaeit[.]com and 192.199.254.126.	***
May 31, 2014: Final round	***	***	***

[53]

Based upon the translated registration form that we obtained from Song Yubo's personal Baidu document sharing account, open registration for the "TOPSEC Cup" began on May 4th, 2014 and would close on May 14th, 2014.

The details of the competition that were shared on the announcement are extremely ambiguous, and probably for good reason. The introductory paragraph mentions that the primary goal of the event is to facilitate the training and discovery of new talent, noting that exceptional participants would receive priority consideration for internships and jobs with Beijing Topsec.

The event itself was broken down into several distinct rounds of competition. Firstly, the preliminary round required that all eligible registrants would attempt to remotely access and navigate through the network. Should a participating team perform exceptionally in the preliminary qualifying round, they would be invited to participate in the final round on-site in Nanjing.

In this final round, participants would be required to build their own "information systems and network environments." The announcement notes that the students must rely upon their own laptop and software tools to accomplish this task. Further, the announcement notes that participants are prohibited from attacking the provided server as well as their competitors.

Section Summary:

- Song Yubo and his research center at Southeast University appear to be central players in this narrative, as highlighted by their financial connections to the government of China, in particular the Ministry of State Security (MSS), China's premier human intelligence agency.
- If the MSS was involved, we can deduce that the Anthem hack could have been for the purposes of gathering sensitive information for follow-on HUMINT targeting via blackmail, asset recruitment or technical targeting operations against individuals at home.
- Song's use of the topsec email alias suggests a greater association w/ TOPSEC.
- It seems as if the competition is almost certainly the cause for the topsec2014[.]com domain. What is very curious, however, is the initial registration by the reseller li2384826402@yahoo[.]com, which is a tactic seen within the confirmed malicious faux VAE Inc.infrastructure.
- The overlap between the competition website and the static command and control infrastructure seen in the Derusbi /

Sakula implant is was likely an error made by the attackers.

Tianrongxin, a.k.a. Beijing Topsec Technology Co:

The Company

To enhance our open-source capabilities, we partnered up with Dr. James Mulvenon[54] and his team of China experts at Defense Group, Inc. (DGI)[55]. We shared with them everything that we knew at the time, walking through the technical details which led us all the way to Song Yubo and the competition announcement. From there, they were able to uncover a wealth of very consequential background information on Beijing Topsec Technology Co (Beijing Topsec), the sponsoring organization for Song Yubo's information security competition.

DGI's research indicated that Beijing Topsec is one of the largest information security hardware providers in China. In 1996, they were the first Chinese company to break into the market with the release of China's first indigenously-manufactured firewall. Since then, they have expanded their business to include a consulting practice focused on issues such as vulnerability mining, software code analysis, threat intelligence, and encryption R&D, amongst other things.

The company served as a core technical support unit for network

security at the 2008 Olympic Games – an event which was tightly controlled by the state. Additionally, Beijing Topsec is a known partner of the Chinese military. Since 2009, the company has possessed information publication credentials for military network procurement. Since 2013, they have been publicly recognized as the Chinese equivalent of a cleared defense contractor.

The links between Beijing Topsec and the Chinese government are fairly substantial, highlighted by long-standing partnerships between even the most shadowy elements of the Chinese military.

The Leaked Cable

A very compelling piece of evidence is found in the contents of a leaked 2009 diplomatic security cable from the Department of State, published by The Guardian.[56] The cable is a daily digest of Diplomatic Security alerts – essentially a situational awareness primer for State Department employees to inform them of new and existing threats. In one section, the cable highlights that the Founder of Beijing Topsec, He Weidong, had openly talked about receiving directives from the PLA in an interview with China News Network. In the interview, the founder quite curiously states that Topsec is less a commercial entity, but rather a research institute, and that the company received about half of its start-up capital directly from the PLA. The cable further claims that Topsec actively recruits for the PLA cyber army.

[57]

[58]

It would also appear that not only does Beijing Topsec have deep ties to state-run cyber activity, but also within the independent hacker community as well. Of note, the company hired the notorious hacker Lin Yong, a.k.a. "Lion" (of the Honker Union of China[59]) in the early 2000s as a security service engineer and to conduct network training.

Section Summary:

- It is not surprising that the Chinese government would be interested in partnering with a private organization such as Beijing Topsec for use as a front for state-sponsored activity.
- The association between Southeast University and Beijing Topsec as manifested in the joint information security research center highlights the possibility of growing links between

state-sponsored activity and academic institutions, particularly those that receive funding from the central government.
- All in all, it would seem that China is pursuing a unified approach to cyber operations, relying on all unique facets of the workforce: academia, private industry, and independent hackers, as well as the PLA to achieve their strategic goals.

Conclusion:

The Anthem breach exposes the insidious reality of modern Chinese cyber espionage as it continues its unrelenting strikes at the soft underbelly of the American way of life. Moreover, it demonstrates the imposing yet increasingly common reality of conducting threat intelligence analysis without substantial threat intelligence to start with. Fortunately for us, we were able to deduce informed answers to some of the outstanding questions to this breach by scrutinizing our archival data troves that are efficiently stored within our Threat Intelligence Platform and partner integrations. In the field of cyber security, industry professionals must learn to play the long game in order to generate a proactive sense of situational awareness, allowing for greater efficiency and flexibility in mitigating future threats.

Additionally, this incident underscores the frustrating disparity of the industry when it comes to naming conventions. With so many threat actors and indicators floating around, it is can be frustrating to keep track of all the disparate pieces of evidence,

especially when countless naming conventions are applied. Without the use of a Threat Intelligence Platform to keep track of the flood of incoming threat data, this task would be extraordinarily time consuming at best and crippling at worst.

Moving forward, it is important to bear in mind that the adversary, regardless of country of origin, shall almost certainly leverage our every weakness against us. Even something as seemingly innocuous as confusion over names can easily consume analytical bandwidth, creating a window of opportunity to strike. We – that is security professionals, private industry and governments alike – must proactively harden our network defenses and hasten our incident responses as a united, synchronous entity.

We have shared details on Song Yubo[60] and affiliated indicators within the ThreatConnect Common Community. This share also includes the full-text DGI "BLUE HERON" research[61] which provides greater insight into Song Yubo, Southeast University and Beijing Topsec.

All things considered, industry must learn to adopt a cooperative defense mindset in the hopes of rebuffing future attacks. The most resolute defense we have is each other, so be like the TCIRT and start actively defending your own community from the next big breach. Register for a free ThreatConnect account today[62] to get started sharing and analyzing your threat intelligence.

1. http://www.threatconnect.com/news/author/the-square/

2. http://www.threatconnect.com/news/category/threat-research-tcirt/
3. http://www.threatconnect.com/news/premera-latest-healthcare-insurance-agency-to-be-breached?utm_campaign=Anthem-Hack-Blog-Post&utm_source=from-anthem-post
4. http://www.threatconnect.com/product/threatconnect_API
5. http://www.threatconnect.com/partners
6. http://www.threatconnect.com/why_threat_connect/what_is_threat_intelligence_platform
7. http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720
8. https://www.anthemfacts.com/ceo
9. http://threatconnect.com/why_threat_connect/threatconnect_intelligence_research_team
10. https://www.virustotal.com/en/file/77421106548e69e9666c538ad628918cad7cfcf8f6aa7825f71a4fc39e522a7d/analysis/
11. https://www.virustotal.com/en/file/8d168092d5601ebbaed24ec3caeef7454c48cf21366cd76560755eb33aff89e9/analysis/
12. http://www.threatconnect.com/news/press-releases/cyber-squared-inc-announces-expansion-data-services-powerful-domain-passive-dns-intelligence/
13. http://www.threatconnect.com/news/threatconnect-enables-healthy-networking-biomed-life-sciences-industry/
14. https://twitter.com/threatconnect

15. http://www.threatconnect.com/news/wp-content/uploads/2015/12/wellpoint-evil2legit1.jpg
16. http://www.threatconnect.com/news/wp-content/uploads/2015/12/wellpoint-evil2legit1.jpg
17. https://www.virustotal.com/en/file/3fe208273288fc4d8db1bf20078d550e321d9bc5b9ab80c93d79d2cb05cbf8c2/analysis/
18. http://www.threatconnect.com/news/wp-content/uploads/2015/12/premera-update.jpg
19. http://www.premera.com/
20. http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html
21. https://app.threatconnect.com/tc/auth/incident/incident.xhtml?incident=708926
22. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Well-VAE-Overlaps.jpg
23. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Well-VAE-Overlaps.jpg
24. http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/
25. https://www.virustotal.com/en/file/d4be6c9117db9de21138ae26d1d0c3cfb38fd7a19fa07c828731fa2ac756ef8d/analysis/
26. http://www.threatconnect.com/news/wp-content/uploads/2015/12/li-reg-overlaps1.jpg

27. http://www.threatconnect.com/news/wp-content/uploads/2015/12/li-reg-overlaps1.jpg
28. http://www.threatconnect.com/news/wp-content/uploads/2015/12/topsec2014-hist.png
29. http://www.threatconnect.com/news/wp-content/uploads/2015/12/topsec2014-hist.png
30. http://pwc.blogs.com/files/cto-tib-20150223-01a.pdf
31. http://blog.crowdstrike.com/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/
32. http://www.washingtonpost.com/world/national-security/chinese-hackers-go-after-us-workers-personal-data/2014/07/10/92db92e8-0846-11e4-8a6a-19355c7e870a_story.html
33. http://krebsonsecurity.com/wp-content/uploads/2015/02/FBI-Flash-Warning-Deep-Panda.pdf
34. http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/
35. http://www.csoonline.com/article/2880352/disaster-recovery/anthem-confirms-data-breach-but-full-extent-remains-unknown.html
36. http://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html
37. https://app.threatconnect.com/tc/auth/incident/incident.xhtml?incident=39083
38. http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html
39. http://www.threatconnect.com/news/wp-content/uploads/2015/12

/Screen-Shot-2015-02-25-at-5.20.37-PM.png

40. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Screen-Shot-2015-02-25-at-5.20.37-PM.png
41. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Screen-Shot-2015-02-23-at-9.22.35-AM.png
42. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Screen-Shot-2015-02-23-at-9.22.35-AM.png
43. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Translation.png
44. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Translation.png
45. https://scholar.google.com/citations?user=BoorASIAAAAJ&hl=zh-CN
46. http://www.researchgate.net/profile/Song_Yubo
47. http://www.threatconnect.com/news/wp-content/uploads/2015/12/yubo-stacked.png
48. http://www.threatconnect.com/news/wp-content/uploads/2015/12/yubo-stacked.png
49. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-066.pdf
50. http://www.threatconnect.com/news/wp-content/uploads/2015/12/relationships.jpg
51. http://www.threatconnect.com/news/wp-content/uploads/2015/12/relationships.jpg
52. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Screen-Shot-2015-02-26-at-4.12.20-PM.png

53. http://www.threatconnect.com/news/wp-content/uploads/2015/12/Screen-Shot-2015-02-26-at-4.12.20-PM.png
54. http://www.uscc.gov/sites/default/files/Mulvenon_Bio.pdf
55. http://www.defensegroupinc.com/index.html
56. http://www.theguardian.com/world/us-embassy-cables-documents/214462
57. http://www.threatconnect.com/news/wp-content/uploads/2015/12/lin-yong-lion.png
58. http://www.threatconnect.com/news/wp-content/uploads/2015/12/lin-yong-lion.png
59. http://blogs.wsj.com/chinarealtime/2011/10/05/patriotic-chinese-hacking-group-reboots/
60. https://app.threatconnect.com/tc/auth/adversary/adversary.xhtml?adversary=726175
61. https://app.threatconnect.com/tc/auth/document/document.xhtml?document=726190
62. http://www.threatconnect.com/product/product_editions