WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

TACTICAL CYBER REPORT: OIL & GAS

SER. NO.: IR-18-250-002

Activity Summary - Week Ending 7 September 2018:

- The top keylogged email is: "mobilku.com" which is an auto sales service in Java, Indonesia
- Sality and Corkow remain the SOC's top malware variants seen for the past 4 weeks
- Blockchain technology is emerging as an effective solution to oil and gas production
- Acrid Rain is an infostealer that targets many browsers
- Iran continues to sabre rattle in light of the US sanctions against Iranian oil trade
- Recent riots and government turmoil in Tripoli Libya will likely affect Libyan oil exports
- China has become Africa's largest trade partner; beware of the BlackOasis hacker group
- #OpCatalonia (Anonymous) is targeting ree.es, or the Red Eléctrica Group, an energy infrastructure component of Spain
- Analysis of the recent DoD Report, which highlights Chinese expected cyber hacking
- Point of Sale (POS) cyber theft expected to raise in India
- Japan's LNG imports will fall in the coming months as the restart of nuclear reactor restarts; hacktivism continues

COMPROMISED EMAIL ACCOUNTS

Below are the Top 10 Keylogger emails and the Top Attacker Servers (C2) observed on 5 September 2018 through our Wapack Labs proprietary data.

Keylogger: Email	Times Seen
sales@mobiku.com.tw	7
naomynathaly@outlook.com	7
grace@so-easy.com.tw	7
info@duketoms.com	6
invest@alshoumoukh.com	5
ronunis1@gmail.com	4
redmaknetwork@gmail.com	4
prathanaalloys@gmail.com	4
peter_2633@hotmail.com	4
moin@orenme.com	4

Attacker Server (C2)	Times Seen
okey@cosascco.com	186
pintoulixou@gmail.com	67
super.keylogge@yandex.ru	33
beninomo@gmail.com	27
elecopter.spy@yandex.ru	19
hboy0001@yandex.ru	15
avitgap4@mail.com	5
thisswry@mail.com	3
idontwantits@mail.com	3
Lazarouz@post.com	1

Table 1: The top observed compromised emails from our keylogger operations. The top keylogged email is: sales@mobiku.com.tw This appears to be a typo-squatted domain of "mobilku.com" which is an auto sales service in Java, Indonesia. As of 6 SEP the true web site remains down. So-easy.com.tw is a Taiwan site that encourages school teachers to

guide students to produce creative animation. Naomy Nathaly is a keylogged teenage female from Vera Cruz MX. The 2nd ranked keylogged email is: info@duketoms.com DukeToms.com is a dairy producer: iDewasNaka - Niranjanpur, Scheme 78 Part 1 Phase 2, Indore, Madhya Pradesh 452010 and reported as a top compromised email address last week. That site is now down. The above emails should be block as compromised accounts.

Table 2: Top observed Attacker Servers (C2), **for a fifth week is from Cosascco**, 11841 Smith Avenue, Santa Fe Springs, California 90670 USA. Cosascco is a corrosion and erosion monitoring technology company.

COMPROMISED (C2) IP'S

IP	Contacts
145.249.107.170	17
171.221.136.95	12
212.62.208.209	9
172.245.244.28	8
192.40.95.17	7
137.59.252.170	6
83.31.191.43	5
82.102.20.183	5
82.102.20.179	5
46.246.123.36	5

The top C2 IPs seen from keylogger collection. 145.249.107.170 and is an ip address located in Amsterdam, Netherlands through Liberty Services / Quasinet CIDR: 145.249.107.170.0/22, ISP: AS29073; IP: 171.221.136.95 is from Chengdu, Sichuan, China, CIDR: 171.221.136.95.0/25 ISP: AS4134

MALWARE ACTIVITY

Below tables contains both the Top 10 Malware Variants and the Top IP addresses observed on 6 September 2018 through our Wapack Labs proprietary data.

Malware Variant	Times Seen
sality	13438
corkow	1093
loki	126
betabot	47
poweliks	46
sykipot	41
kazy	23
koobface	15
maudi	14
citadel	13

Top 10 Malware Variant and number of contacts. Sality and Corkow remain the top malware variants for the past 4 weeks. See 31 AUG 2018 report for description of top two variants.

WEB FILTERING

Malicious Domain Name	Type	IP	Description
api.retargetly.com	Malicious Website	104.20.139.67 104.20.138.67	Multiple malicious Win32 trojan executables as well as malicious Win32 dll's are known to communicate with this
peliculashd.site	Malicious Website	104.27.168.52 104.27.169.52	Free movie/video streaming website
northghost.com	Proxy Avoidance	23.236.62.147	This domain is website for Touch VPN which is a free VPN service which uses SSL encryption with very little restrictions allowing users to access inappropriate websites/exfiltrate data subvariant.
movable-ink-6071.com	Spam	52.36.92.66	This domain does not contain any web pages: it is used for serving email content for Movable Ink customers
client_monitor.isnssdk.com	Phishing	18.213.226.234 52.5.203.2 34.195.127.158 52.73.87.138 34.195.108.39 54.209.158.74 52.45.210.159 54.84.255.180	This site has been identified as the source for Android phishing malware

CYBER TRENDS

Blockchain – Oil and Gas industry. As cybersecurity threats to the oil and gas industry have grown exponentially, various strategies have been deployed to safeguard companies' computer and control systems. One new technology in particular, blockchain, which has emerged as a highly innovative and effective solution.[1]

Designed as a distributed system, blockchain delivers complex services securely, with enforcement capabilities woven directly into distributed oilfield facilities and equipment. This enables different equipment and vendors to work together by functioning as an electronic communication medium for the connected systems. Blockchain is as decentralized as the oilfield itself, providing protection across the industrial edge, edge to center or center to edge and back again. Blockchain is a multi-faceted, foundational technology on which a company can build its in-field identity and access management, remote access system, enrollment and transient device control, and Industrial Control Systems (ICS) protection.

Pivotal to blockchain technology is its consensus system. When a hacker attempts to enter a system surreptitiously, the many different nodes, or computers, within the blockchain and "vote" on whether or not to allow the requested operation. Policies can be instituted and enforced by the blockchain, to allow the nodes to automatically determine authorized and unauthorized activities.[2] If some nodes are compromised, the vote alerts the system that nodes have gone rogue, allowing the blockchain to expel the compromised nodes and self-heal. Even if a node is destroyed, others nodes pick up the slack with minimal disruption. Unlike traditional cyber security systems, the more nodes that are deployed, the stronger the system becomes. With the single point of

[1]

[2] https://www.worldoil.com/news/2018/9/4/blockchain-quickly-becoming-oilfield-cybersecurity-standard

failure eliminated and multitudes of nodes forming a consensus, the more difficult (and cost-prohibitive) it becomes for a hacker to compromise enough nodes simultaneously to overwhelm the system.

The blockchain design employs a tamperproof, self-healing, self-replicating and highly redundant architecture provides the oil and gas industry with many unique benefits. Since blockchain is not limited by, but rather benefits from scale, companies employing blockchain can be assured they will have the flexibility to operate in a dynamic, digitized, and tamperproof manner.

With more and more oilfield operators putting machines, instead of humans, in charge of production, it is critical to ensure that these highly connected and digitized systems are appropriately secured. Blockchain will resolve vital cybersecurity issues, such as remote access, role-based access control, password rotation and ICS finger printing.

AcridRain – There is a new infostealer being observed named AcridRain. First appearing on the underground forums in July 2018, Acrid Rain is an infostealer that targets many browsers. AcridRain can steal various credentials including cookies, and credit cards from multiple browsers like: Amigo, Google Chrome, Vivaldi, Yandex browser, Kometa, Orbitum, Comodo, Torch, Opera, Mail.ru, Nichrome, Chromium, Epic Privacy browser, Sputnik, CocCoc, and Maxthon 5.[3] It has the ability to steal telegram and steam sessions, FileZilla connections, and probably more. AcridRain can also dump credentials from the browsers it attacks, and search for several popular cryptocurrency wallets (Armory, Bitcoin, Electrum, Ethereum, Doge, Dash, Litecoin, Monero, mSIGNA). Researchers also observed is that the malware appears to make use of various malicious tools by borrowing code from known repositories, and incorporating into its own source.

Signatures: *W32/Agent.PMO!tr.spy, W32/Agent.OYI!tr.spy*

PseudoGate – Researchers have discovered a new banking campaign called PseudoGate. It is observed using multiple delivery vectors to accomplish its infection routine. PseudoGate uses the RIG exploit kit as well as the GrandSoft exploit kit to ultimately infect victims. It has been observed targeting Japan. PseudoGate is a campaign that uses malvertising in a drive-by download attack that ultimately redirects the victim to compromised sites, which contain various Adobe Flash exploits to ultimately compromise the victim machine. Once the victim is compromised, the Trojan downloader, Smoke Loader, will then download either Panda or Kronos banking trojans.

Additional vulnerabilities observed being exploited: RIG Exploit Kit, CVE-2015-2419 (IE) & CVE-2016-0189 (IE), & CVE-2018-8174 (IE), & CVE-2018-4878 (Adobe Flash). In the GrandSoft Exploit Kit, only CVE-2018-8174 (IE) was observed during the exploitation process.

Signatures: W32/Propagate.GJEV!tr, W32/GenKryptik.CGKR!tr, W32/Kryptik.GITY!tr, W32/NeutrinoPOS.37B!tr, W32/GenKryptik.CIIB!tr, W32/GenKryptik.CEMD!tr, W32/Kryptik.GJUV!tr.ransom, W32/Kryptik.GKEK!tr, W32/Kryptik.GKDT!tr, W32/GenKryptik.CFGU!tr.

Indicator(s):
hxxp://185.219.81.232/Libs.zip
hxxp://141.105.71.82/Libs.zip
hxxp://185.219.81.232/Upload/
hxxp://141.105.71.82/Upload/

[3] Fortinet Research: www.fortinet.com

GEOGRAPHIC TRENDS:

MENA – Iran

Iran continues to sabre rattle in light of the US unwavering sanctions against Iranian oil trade. Iran's most senior general is again threatening to shut down the world's busiest oil chokepoint if the US manages to completely cut Iran's oil and gas trade. On 30 August 2018, Major General Mohammad Hossein Bagheri, the head of the Iranian military's chief of staff, told naval commanders of the country's elite Revolutionary Guards that a third of the world's oil passes through the Persian Gulf's Strait of Hormuz, and would be stopped, in the event that President Trump's policies succeed in reducing Iran's oil exports to zero. US Defense Secretary James Mattis responded and warned that "Iran has been put on notice" due to its regional activities and threats to close the Strait of Hormuz. General Bagheri countered, "the US army and other foreign forces in the Middle East region are well aware of this issue, that if they make the slightest mistake in the region, they will pay a heavy price." Bagheri further warned that the, "movements of US forces in the Persian Gulf are monitored closely and if any move is made by the US forces, contrary to the international law, their act will be prevented harshly."[4] On 5 November 2018 further sanctions will be re-imposed including sanctions on:

- Iran's port operators, and shipping and shipbuilding sectors, including the Islamic Republic of Iran Shipping Lines (IRISL), South Shipping Line Iran, or their affiliates;
- Petroleum-related transactions with the National Iranian Oil Company (NIOC), Naftiran Intertrade Company (NICO), and National Iranian Tanker Company (NITC), including the purchase of petroleum, petroleum products, or petrochemical products from Iran;
- Transactions by foreign financial institutions with Iran's Central Bank and other designated Iranian financial institutions;
- The provision of specialized financial messaging services to Iran's Central Bank and other designated Iranian financial institutions;
- The provision of underwriting services, insurance, or reinsurance for transactions with Iran;
- Iran's energy sector.[5]

On 3 September 2018, the Iranian rial hit a record low against the US dollar, within a deterioration in their economic situation and the imposition of US lead sanctions. The US dollar was being offered for as much as 128,000 rials. The currency has been volatile for months because of a weak economy, financial difficulties at local banks and heavy demand for dollars among Iranians. Much of the economy in Iran is based on their oil industry, which is due full sanctions in November (see above). Iran fired their Minister of Economic Affairs and Finance a week ago. In early August 2018, Iranian lawmakers voted out the Minister of Labor and in July 2018, President Rouhani replaced the head of their central bank. Both physical and social media protests linked to the current economic situation in Iran erupted in December of 2017, spreading to more than 80 cities and towns. Sporadic protests, led by truck drivers, farmers and merchants in Tehran, have continued.[6]

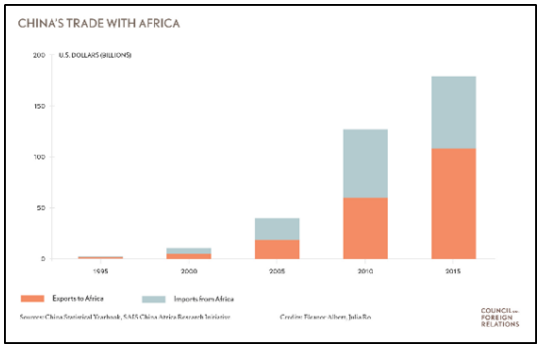
[4] https://www.newsweek.com/iran-warns-no-oil-will-pass-through-worlds-most-important-route-if-us-plan-1098047
[5] http://www.hfw.com/Sanctions-Update-US-sanctions-on-Iran-8-May-2018
[6] https://www.businessinsider.com/irans-currency-plummets-to-a-record-low-of-128000-to-the-dollar-2018-9

Libya

Close to 400 prisoners have escaped from a jail in Tripoli, Libya amid conflicts between rival factions fighting for control of the city. After riots broke out, inmates at Tripoli's Ain Zara prison stormed their way out. Many of the prisoners were supporters of the late Libyan leader Moammar Gadhafi, who was accused of war crimes against the Libyan people. The jailbreak comes after Libya's UN backed government declared a state of emergency in Tripoli. At least 47 people have been killed in the capital and surrounding areas recently, prompting the UN and several Western nations to call for an immediate end to the violence. Facebook has been blocked in Tripoli and other Libyan cities. Facebook is the main platform for news in Libya with both government officials and armed groups effectively controlling postings. The blockade started on 3 September 2018 and confirmed by Libyan users. No group is claiming the social media blockade. It is being reported that Facebook was being used to buy and sell arms and to offer attack tactics.[7] It is reported that other websites were available for these activities. Earlier this summer, fighting closed down two Libyan oil ports. In July 2018 they were re-opened, but this current round of fighting will likely negatively affect oil production and exports. On 4 September 2018 a ceasefire agreement was reached through the UN.

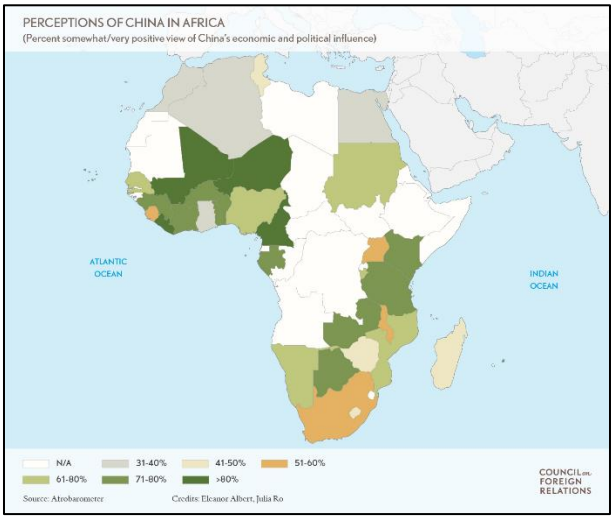
Africa – Chinese Colonialism: Angola, Republic of Congo & South Sudan

China has become Africa's largest trade partner and has greatly expanded its economic ties to the continent, but its growing activities there have raised questions about its noninterference policy.[8] China's economy, which had averaged an annual growth rate of 10 percent for three decades until 2010, requires substantial levels of energy to sustain its momentum. It has become the world's largest energy consumer and producer [PDF] in the world. Though China relies on coal for much of its energy needs, its oil consumption is second worldwide. Once the largest oil exporter in Asia, China became a net importer in 1993 and has surpassed the United States as the world's largest importer of oil in recent years. China's second-largest source of crude imports after the Middle East is Africa, from which it receives 1.4 million barrels per day, or 22 percent [PDF]. Angola was China's third-largest oil supplier in 2016/2017. Other African oil suppliers include the Republic of Congo and South Sudan.



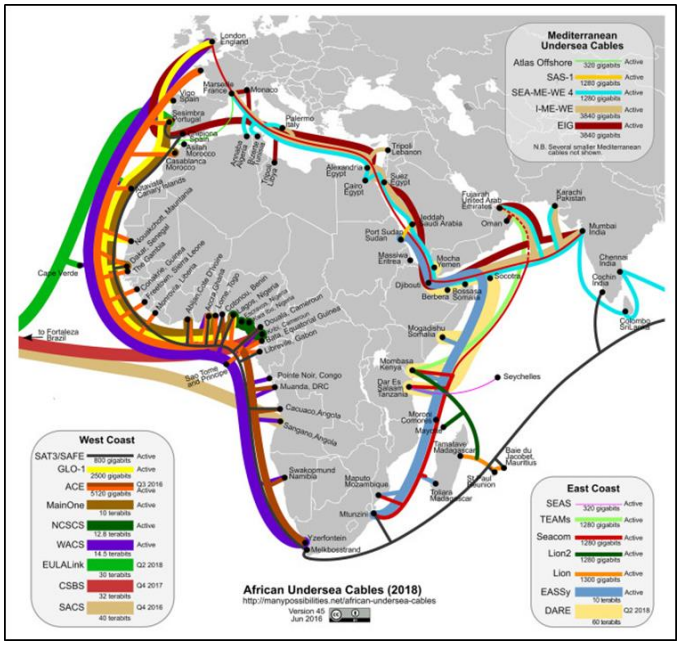
On 3 September 2018 at a summit for African leaders, Chinese President Xi Jinping pledged $60 billion in financing for projects in Africa in the form of assistance, investment and loans, as China furthers efforts to link the continent's economic prospects to its own. Some African leaders have expressed fears of new colonialism being

[7] https://www.seattletimes.com/nation-world/in-libya-facebook-is-used-to-buy-arms-locate-foes-and-kill-them/
[8] https://www.cfr.org/backgrounder/china-africa



employed by China within the continent of Africa. China's latest pledge comes on top of a 2015 promise to provide African countries with $60 billion in funding that Xi said had either been delivered or arranged. Xi promoted Beijing's initiative to build ports and other infrastructure as a tool for "common prosperity" in a world facing challenges from trade protectionism.

Less than one year ago, a likely Middle East based hacker group named “BlackOasis.” was observed exploiting an Adobe Flash Player zero-day vulnerability (CVE-2016-4117) to remotely deliver the latest version of “FinSpy” malware. FinSpy, a final-stage payload that allows for an attacker to covertly learn what a target is talking about and who they are communicating with, is associated with Gamma Group. BlackOasis in recent months sent a wave of phishing emails. These emails contained malicious Microsoft Word documents with the aforementioned Flash Player zero-day hidden inside an embedded ActiveX object. In the past, BlackOasis messages were designed to appear like news articles about political relations between Angola and China. BlackOasis group operations were active in the countries of: Iraq, Afghanistan, Bahrain, Jordan, Saudi Arabia, Iran, Netherlands, United Kingdom, Russia, **Nigeria**, **Libya**, **Tunisia**, and **Angola**. This is a stark reminder of groups targeting African oil and gas associated countries with who possess malicious malware.



Ghana

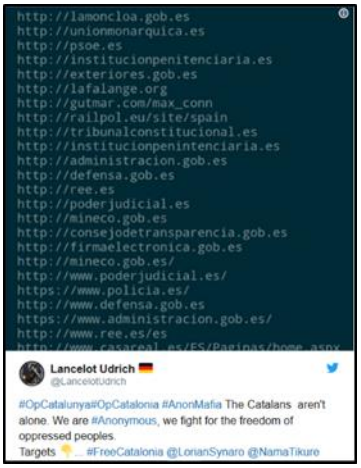
The Nigerian internet service provider Tizeti has raised $3 million in a new round of funding as it expands its unlimited internet service, WiFi.com.ng, into Ghana. This is an example of the continuing efforts from both Europe/Middle East and Asia to connect with the continent of Africa. With the rapid expansion of internet service, comes threat and vulnerabilities from cyber-attacks. Tizeti is expanding its operations outside of Nigeria, launching a new brand titled Wifi.Africa and marketing it to Ghana and beyond.[9] There are currently 16 submarine telecom cables connecting Africa. The current difficulty, is getting internet service to African users. Currently balloons and drones are being used in rural areas, but these are not practical in urban areas. Tizeti has currently signed 3,000 subscribers, with close to $1.2 million in annual recorded revenue increases. There are approximately 1.2 billion people in Africa, yet only 26 percent are online or obtain internet service over mobile phones. At this time, only approximately 6

[9] https://techcrunch.com/2018/09/04/expanding-its-internet-service-to-more-countries-in-africa-tizeti-raises-3-million/

percent of that population has internet service subscriptions. Internet service will only escalate at a very rapid pace, with bad actors likely take full advantage of profits over security.

Europe – Spain

The website of Banco de España, the central bank of Spain, was offline at the beginning of this week due to a DDoS attack claimed by hacktivist group Anonymous Catalonia. The attack started on 2 September 2018 and continued through the 3rd. It is part of #OpCatalonia, a protest against the arrest of Catalan political leaders over the region's fight for independence last year. Anonymous used the famous 'TangoDown' hashtag to announce on Twitter that their distributed denial-of-service attacks were successful, and showed proof that the server hosting the bank's website was down. Their success is more of a statement in this case because apart from blocking access to the website the attack produced no damage. A representative of the bank said that the institution had been hit by a DDoS attack that allowed intermittent access to the website, but it had no effect on the normal functioning of the bank. Because it is a central bank, Banco de España does not offer online banking services. Also, it does not work with commercial customers, so its operations remained unaffected by the attack. #OpCatalonia has multiple websites in sight. Banco de España is just one of the latest victims of the hacktivist group, who started the assault on Spanish government websites on 20 August 2018.



Running DDoS attacks is a common form of protest for hacktivists, who rent the service for a period of time. Once they run out of money, the server suffering the incoming torrent of bad traffic returns to normal activity. One of the targets of #OpCatalonia was *ree.es*, or the Red Eléctrica Group, an infrastructure component of Spain. This demonstrates that the Spanish oil and gas sector is likely a target as well. RepSol is an example of such an oil target.

Spain has frozen the sale of 400 laser-guided bombs to Saudi Arabia, their Ministry of Defense (MoD) confirmed on 4 September 2018. Media reported the decision was taken because the bombs could be used in Yemen, where civilians have been killed in Saudi-led coalition airstrikes. It added that their bombs, which were ordered in 2015 for EUR9.2 million (USD10.7 million), had been paid for and were awaiting collection at a military base in Aragon. The report prompted concern about Saudi Arabia's recent order for five military vessels from the Spanish shipbuilder Navantia.

North America – US

The Department of Defense (DoD) has just published its 2018 Annual Report to Congress on Chinese military forces. It is in part a catalog of the military technologies China is trying to field or is developing for future military systems. This could be seen as a list of the technologies being developed by US industries and corporations that China's espionage and cyber collection entities would try to collect to support China's military modernization. The DoD Report highlighted the People's Liberation Army (PLA) key military systems and technologies currently being developed, including:

- Precision strike ballistic missiles (DF-26)
- Anti-ship ballistic missiles (DF-26 variant)
- Ballistic missile defense (HQ-19 interceptor)
- Aircraft systems (J-20, FC-31)

- Land-attack and anti-ship cruise missiles (YJ-62, YJ-18)
- Long-range UAV's (Xianglong)
- Space and counterspace systems (kinetic-kill missiles)
- C4I systems (using big data, internet of things)
- High-precision artillery (PHL-03 multiple-rocket launcher)

In addition, the DoD Report identified that China is investing heavily in certain technologies for future weapons systems. These technologies are information technology, artificial intelligence, new materials, advanced manufacturing, advanced energy technologies, laser and aerospace technologies, marine technologies, and quantum satellites. The DoD Report emphasized that China is likely to continue its efforts to acquire foreign technologies to support its own technology development programs. In particular, it stated that Chinese cyber elements are being consolidated for greater efficiency, and that cyber intrusions and collection will be a major part of their efforts to acquire foreign military technologies. Military technology is often directly tied to technology in private industry; to include the oil and gas sector. A full report is available upon request.[10]

Analysts have identified a hacker with an alias Mr.Kro0oz.305. KroOoz is likely Saudi Arabian and known for his defacements. Recently he has defaced the North Carolina Anson County website as well as the Iranian transportation company Shayan Trading Co's website. Further research is being conducted to determine if Mr.KroOoz has targeted any oil and gas sector companies.

Asia – India

India's demonetization e-commerce platform, PayTM, has received a $350 million USD investment (or 4% stake) from Berkshire Hathaway. In 2016, PayTM entered into an agreement with Indian Oil Corporation Limited (IOCL) to use their e-commerce to purchase oil products. India is becoming one of the fastest and most strategic open Internet geographies in the World.

Flipkart-owned digital payments player PhonePe has entered into a first-of-its-kind partnership with Indian Oil for adoption of its Point of Sale (POS) device at IOCL retail outlets. As part of this partnership, customers can pay using Unified Payment Interface (UPI), credit and debit cards, a PhonePe wallet and other external wallets like Jio Money and Freecharge for their fuel purchases. These services all through the POS device at IOCL retail outlets. A device powered by Bluetooth, PhonePe's POS device was launched in Bengaluru, India in October, 2017. Meant to serve merchants of all sizes, the POS device works like a traditional calculator. PhonePe is targeting the installation of a million POS devices across 50 Indian cities by the end of 2018.[11]

In a previous cyber security posting, analysts discovered DiamondFox, a credential stealing multipurpose botnet that is available on the black market as MaaS (Malware as a Service). Also known as Gorynych, DiamondFox is still actively leveraged in the wild with in a recent version "Crystal" available in online marketplaces. This dangerous malware can steal information from POS systems with campaigns targeting multi-state healthcare providers, dental clinics, manufacturers and technology companies. To get a picture of the current state of DiamondFox botnets, analysts collected samples and extracted the command and control (C2) information from their configuration files. Analysis discovered that infrastructure from a Russian malware provider was behind DiamondFox botnets. Two C2 domains were added to our sinkhole data for further analysis. Our report[12] provides technical details on DiamondFox, the Russian botnet infrastructure and details regarding the sinkholed

[10] Wapack Labs: IR-18-243-002
[11] https://www.thenewsminute.com/article/indian-oil-partners-phonepe-deploy-pos-devices-iocl-retail-outlets-76597
[12] DiamondFox in the Wild: TIR-011-2017 (Wapack Labs)

domains. As the e-commerce market continues to explode in India, so will the use for oil and gas purchasing through electronic processing modes. POS thefts has long been a threat, with Russian organized crime leading many of these efforts. POS fraud will likely increase, as caution is suggested to those conducting business inside India.

Japan

Japan's liquefied natural gas (LNG) imports are expected to fall in the coming months as the restart of nuclear reactors continues. Kansai Electric Power restarted the 870-MW No. 4 reactor in Takahama last week, followed by Kyushu Electric Power's 890-MW No. 2 reactor in Sendai.[13] Having been shut since the Fukushima nuclear disaster, Japan's nuclear power plants have been gradually coming back online since 2015. Each of the two reactors recently restarted will reduce Japanese LNG imports by 1m tons per year. Japan, the world's largest LNG importing nation, could reduce annual overseas purchases by as much as 9m tons. Japan's LNG imports fell by nearly half last month at 8.4m tons, compared with 16m tons in August of 2017. It has been 7 years since Fukushima, yet strong social media anti-nuclear protest continues to date. Typhoon Jebi hit Japanese land fall on 4 September 2018, fortunately without any damage equal to the Fukushima nuclear incident. On 6 September 2018, a 6.7 earthquake hit the northern part of Japan, causing mud slides from the typhoon rain. No nuclear power plants were reported damaged. North Korea as recent as last February 2018, has set its targets on Japan. This through APT group Reaper (off shoot of the Lazarus Group). Reaper's focus has expanded to include an organization in Japan associated with the United Nations missions on human rights, Japanese sanctions against North Korea and the director of a Vietnamese trade and transport firm.[14] With Japan's current physical and cyber defenses in peril, cyber-attacks are likely.

Figure 1. #Fukushima

China

China is the world's second largest LNG importing nation and saw imports rise 47.6 percent this past year to 28m tons in the January to July 2018 time frame. China's Sinopec, the country's largest energy firm, has guaranteed to continue the expansion of their gas infrastructure in terms of storage and transport to meet rising consumption. Analysts predict that China, India and Pakistan, will continue to rise in LNG consumption in near terms.

ExxonMobil is planning to build an ethylene plant and a liquefied natural gas receiving terminal in the southern Chinese province of Guangdong.[15] ExxonMobil signed a co-operation framework agreement with China's provincial government to advance discussion about the construction of a 1.2m-ton-per-year ethylene flexible-feed steam cracker in the Huizhou Dayawan Petrochemical Industrial Park. Ethylene plants are powered on naphtha or liquefied petroleum gas (LPG). ExxonMobil said this plant would rely on proprietary technologies in direct crude steam cracking. The proposed start-up year is 2023. This project supports current progress toward China's national petrochemical development priorities, which demands self-sufficiency, diversified feedstock sources, rebalancing fuels versus chemicals and advancing new competitive technology. ExxonMobil also announced

[13] https://lloydslist.maritimeintelligence.informa.com/LL1124088/Japans-LNG-imports-set-to-fall
[14] https://www.reuters.com/article/us-northkorea-cyber/lesser-known-north-korea-cyber-spy-group-goes-international-report-idUSKCN1G42CH
[15] https://lloydslist.maritimeintelligence.informa.com/LL1124144/ExxonMobil-unveils-ethylene-and-LNG-projects-in-southern-China

China's support in upgrading the Huizhou LNG receiving terminal, to which ExxonMobil intends to participate (including supply of LNG).

ExxonMobil, a US based oil company, has long sought to expand its presence in China. They jointly own an oil-refining and petrochemical complex with Sinopec and Saudi Aramco facility in Fujian. Interestingly, ExxonMobil's agreement was reached during the current escalation of trade tension between China and the US. China has threatened to impose 25 percent tariffs on US crude and LNG in recent months. ExxonMobil is a constant target of fake purchase orders, used in phishing attempts (last known attempt was 18 August 2018 in Virus Total - *order.distribution@exxonmobil.com*).

South America – Venezuela

As a follow up to the chaos on Venezuela, President Maduro said he is investing part of his *personal* savings in a gold-backed certificates as part of a much-questioned plan to crush hyperinflation and reactivate Venezuela's moribund economy. Maduro and First Lady Cilia Flores were the first in line at the central bank in downtown Caracas on 3 September 2018, as it began selling the certificates. These certificates functions like a fixed-term deposit that matures in a year and is supposedly backed by a 1.5 gram piece of gold held with the Venezuelan monetary authority. Venezuela continues with five-digit inflation, has destroyed savings it remains unclear how many Venezuelans will buy these new certificates.

Figure 2. @VenteVenezuela

Internet and social media continue to actively oppose the Maduro regime. @VenteVenezuela is one such social media site that is vocal about the current economic and political state in Venezuela. Of note, many of these organizations and sites are outside Venezuela.