WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

TACTICAL CYBER REPORT: OIL & GAS SER. NO.: IR-19-081-001

Activity Summary - Week Ending 22 March 2019:

- Wapack Labs identified 74,293 connections to sinkholes from new unique IP addresses
- Proprietary sources identified 830,871 new IP addresses participating in various botnets
- #WinRAR exploit
- Winnti Malware
- 737 Max Aircraft Spam Campaign
- Algeria and the "Shaky Six"
- France's Yellow Vest Protest movement, co-opted and still strong
- The Sunrise Movement still targeting the oil and gas sector
- Tankers in the Med, transferring Venezuelans crude oil

COMPROMISED EMAIL ACCOUNTS

Below are the Top 10 Keylogger emails and the Top Attacker Servers (C2) observed on 18 March 2019 through our Wapack Labs proprietary data.

Keylogger: Email	Times Seen
askmlaveben39@hotmail.com	9
seroja@serojathai.co.th	8
sales@mobiku.com.tw	5
indo.chbacct@gmail.com	5
grace@so-easy.com.tw	5
choongstephen29@gmail.com	5
yusufeefe@hotmail.com	4
vishalbagadiya.gallops@gmail.com	4
taah100302@gallopsautolink.com	4
mhcv@gallopsautolink.com	4

Attacker Server (C2)	Times Seen
youusednspy@yandex.com	116
earner@vivaldi.net	57
beninomo@gmail.com	46
super.keylogge@yandex.ru	14
hboy0001@yandex.ru	11
dan.max89@yandex.com	7
chris.emmanuel2017@yandex.com	3
logs.inbox@yandex.com	1
---	---
---	---

Table 1: Top observed keylogged email: askmlaveben39@hotmail.com ask mikeben39 is related to SoulPlay.co, a music type festival. This may be a spoof of Mikeben39 connecting to a Hotmail email. seroja@serojathai.co.th is a Thailand company called Seroja and is a local Indo China Beverage Company. This email has been reported in past briefs. Both these email addresses could be lures to entice recipients. Caution should be exercised upon receipt of these emails

Table 2: Top observed Attacker Servers is youusednspy@yandex.com may be a lure email, as "dnSpy" is a debugger and .NET assembly editor. This email was observed last week. earner@vivaldi.net Vivaldi is a freeware, cross-platform web browser developed by Vivaldi Technologies, a company founded by Opera Software co-founder and former CEO Jon Stephenson von Tetzchner and Tatsuki Tomita. This is likely a phishing email to lure users. Caution should be exercised and never open any email with this Yandexl name.

On 18 March 2019, Wapack Labs identified **6** 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.

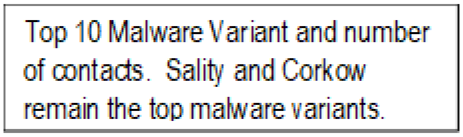
COMPROMISED (C2) IP'S

IP	Contacts
94.177.226.160	23
217.11.155.217	23
212.62.209.82	19
185.124.224.124	19
196.52.34.16	18
51.15.92.212	16
217.11.155.63	16
217.11.153.149	16
91.206.14.10	15
212.62.209.233	14

The top C2 IP seen from keylogger collection. IP: 94.177.226.160, assigned to: CLOUD-DE, Germany through 24036 Ponte San Pietro (BG - Bulgaria), ASN: AS200185 (Aruba), ISP: same, CIDR: 94.177.226.0/29; 217.11.155.217 owned by: HOSTLAB Turkiewicz i Wspolnicy Spolka Jawna, ISP: TeleData GmbH Friedrichshafen Germany, CIDR: 217.11.155.0/29, ASN: AS21263,

MALWARE ACTIVITY

Malware Variant	Times Seen
sality	67621
corkow	4949
nivdort	1400
sykipot	295
loki	290
betabot	274
poweliks	269
maudi	171
black_energy	156
kazy	109


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

On 18 March 2019, Wapack Labs identified **74,293** 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
2019-03-12T06:52:04	smokeloader	1.0.133.249
2019-03-14T01:41:51	Conficker	1.0.134.5
2019-03-13T23:02:25	spam sender	1.0.134.79
2019-03-08T23:25:55	Conficker	1.0.134.170
2019-03-09T02:24:06	smokeloader	1.0.135.14
2019-03-14T05:11:00	HTTP CONNECT (8080)	1.0.135.18
2019-03-17T13:48:01	HTTP CONNECT (8080)	1.0.135.141
2019-03-09T05:16:47	Conficker	1.0.136.152
2019-03-08T22:17:42	Mirai Bot+Mirai	1.0.137.138
2019-03-17T04:33:17	Conficker	1.0.138.199
2019-03-15T06:20:23	Conficker	1.0.139.187

Table 3. On 18 March 2019, Wapack Labs proprietary sources identified **830,871** new IP addresses participating in various botnets. The above list is a sampling ONLY. A full .csv is available upon request.

Blacklists are crucial in proactive network security as they allow companies to defend from network attacks before they are targeted, giving them the opportunity to prevent attacks - versus reacting to them. Our blacklists give IT professional insight into trending attacks and also helps identify sources of malicious emails, malicious websites, and other sources for malware infection. The list above is only the first 11 entries.

Please contact Wapack Labs for prices for complete .csv lists subscriptions.

CYBER TRENDS[1]:

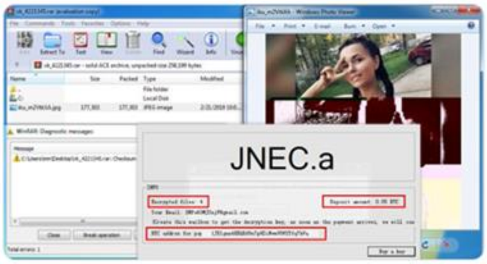


Figure 1. lure

360 Threat Intelligence Center (@360TIC)[2] - VirusTotal is reporting the possible first #ransomware (vk_4221345.rar) spread by #WinRAR exploit (#CVE-2018-20250).

The attacker lures victims to decompress the archive through embedding a corrupt and incomplete female picture. It renames files with .Jnec extension.[3]

[1] Fortinet Research

[2] https://twitter.com/360TIC/status/1107505406744514561

[3] https://www.virustotal.com/#/file/551541d5a9e2418b382e331382ce1e34ddbd92f11772a5d39a4aeb36f89b315e/detection

Winnti Malware challenges gamers to a game of Infestation – Why would companies be concerned about gamers? Well, many gamers use work systems to keep their gaming interests active. This would not be the first time a corporate network was infected via gaming. Researchers are aware of information released last week detailing malware that is being delivered via the supply chain of a gaming platform. From tactics and target regions, this malware appears to resemble a malware named "Winnti" which was documented in 2013.

This malware was discovered to be embedded into a game that was distributed by a gaming company in Thailand. The packed malicious payload is launched almost immediately when the program is run. The malware will make an attempt to avoid detection by the malware containing a list of software programs commonly used by security researchers and admins and will stop security execution, if any of those programs are running. The malware may then drop a malicious DLL file that can communicate with a C2 server.

This malware can trigger an infected machine to download other programs, run programs, and uninstall itself from the system. The malware has code specifically written so it will not target systems that are using Russian or Chinese languages (which is interesting). Delivering malware through supply-chain attacks is not unknown. Researcher see this to be an effective method for malicious actors to bypass detections because of the implied “trust” towards these programs. This shows that users should continue to be cautious while keeping AV databases on their systems - up to date.

Signatures: W64/Winnti.BN!tr W32/Winnti.AG!tr W32/Winnti.A!tr

Indicator(s):
xigncodeservice[.]com
gxxservice[.]com
infestexe[.]com

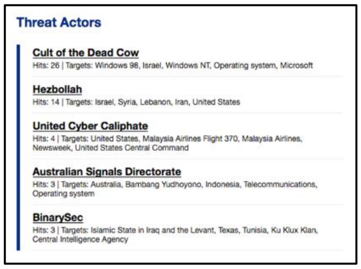
737 Max Aircraft Spam Campaign - Researchers have observed a spam campaign that is trying to take advantage of the two recent crashes of the Boeing 737 Max aircraft. The threat actors behind this campaign are distributing emails with the account “info@isgec[.]com” with the subject line “Fwd: Airlines plane crash Boeing 737 Max 8.” The emails are reported to have been written by a private investigator named “Joshua Berlinger” and is attempting to lure users into opening an attached JAR file. Researchers identified that the objective of this campaign is to drop the “H-WORM” Remote Access Trojan (RAT) onto the recipient’s machine via the malicious JAR file attachment.[4]

Gearbest, a Chinese e-commerce company, exposed over 1.5 million customers’ information and orders due to an unsecured Elasticsearch server. Researchers discovered their server was not password-protected and was open to public accessibility.

Information that was publicly visible include personally identifiable information (PII): account passwords, address, DOB, email addresses, IP address, name, national ID and passport information, order number, payment information, payment type,

[4] https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/spam-campaign-uses-recent-boeing-737-max-crashes-to-push-malware/

phone number, postcode, and products purchased.[5] This is yet another clear example of companies not taking basic steps to secure their networks by changing or creating solid passwords. Gearbest is owned by Shenzhen-based conglomerate Globalegrow and sells a wide variety of products and ships them all over the world. It has a considerable European presence (including warehouses).



Threat Actors

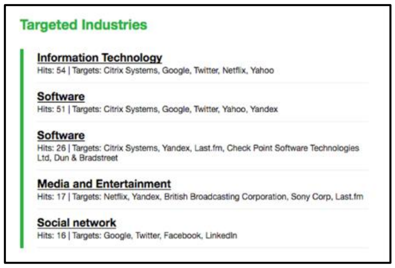
Cult of the Dead Cow
Hits: 26 | Targets: Windows 98, Israel, Windows NT, Operating system, Microsoft

Hezbollah
Hits: 14 | Targets: Israel, Syria, Lebanon, Iran, United States

United Cyber Caliphate
Hits: 4 | Targets: United States, Malaysia Airlines Flight 370, Malaysia Airlines, Newsweek, United States Central Command

Australian Signals Directorate
Hits: 3 | Targets: Australia, Bambang Yudhoyono, Indonesia, Telecommunications, Operating system

BinarySec
Hits: 3 | Targets: Islamic State in Iraq and the Levant, Texas, Tunisia, Ku Klux Klan, Central Intelligence Agency



Targeted Industries

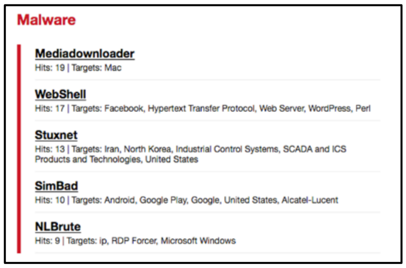
Information Technology
Hits: 54 | Targets: Citrix Systems, Google, Twitter, Netflix, Yahoo

Software
Hits: 51 | Targets: Citrix Systems, Google, Twitter, Yahoo, Yandex

Software
Hits: 26 | Targets: Citrix Systems, Yandex, Last.fm, Check Point Software Technologies Ltd, Dun & Bradstreet

Media and Entertainment
Hits: 17 | Targets: Netflix, Yandex, British Broadcasting Corporation, Sony Corp, Last.fm

Social network
Hits: 16 | Targets: Google, Twitter, Facebook, LinkedIn



Malware

Mediadownloader
Hits: 19 | Targets: Mac

WebShell
Hits: 17 | Targets: Facebook, Hypertext Transfer Protocol, Web Server, WordPress, Perl

Stuxnet
Hits: 13 | Targets: Iran, North Korea, Industrial Control Systems, SCADA and ICS Products and Technologies, United States

SimBad
Hits: 10 | Targets: Android, Google Play, Google, United States, Alcatel-Lucent

NLBrute
Hits: 9 | Targets: ip, RDP Forcer, Microsoft Windows

Cyber news over the last 7 days (above): Ransomware removal and protection; Updates on a Dutch hacker who DDoSed the BBC and Yahoo, and DLL hijacking attacks. Top threat actors are: Cult of the Dead Cow - computer hacker and DIY media organization founded in 1984 in Texas; Hezbollah is a Shi'a Islamist political party and militant group based in Lebanon; United Cyber Caliphate – also known as Islamic State Hacking Division, refers to any number of group self-identifying as the digital army for Islamic State. Targeted industries are IT, Software, Media and Entertainment, and Social networks. Malware: Mediadownloader, which targets MacOS operating systems; Webshells, which are script that can be uploaded to a web server to enable remote administration of the machine.

[5] https://www.helpnetsecurity.com/2019/03/15/gearbest-data-exposure/

22 MARCH 2019 TOP INDICATORS OF COMPROMISE:

Droppers Detected

- Application.JSEMiner.A - Generic JSE coin mining application
- Other:Malware-gen [Trj] - Generic Malware
- HEUR:Exploit.MSOffice.Generic - This is a generic malware designed to generally download and install other malware, Send information about PC, including usernames and browsing history, to a remote malicious hacker
- Trojan-Downloader.VBA.Agent - Generic VBA Trojan
- VB:Trojan.Agent.DROO - generic detection name for Trojans

Top Malicious Email Senders

- Everettfamily@iinet.net.au - sending Trojan:Win32/Spursint.P!cl to recipients at dfw.wa.gov ,
- noreplay.INFRASTRUTTURAPEC@eq.it - sending HEUR:Trojan-Downloader.Script.SLoad.gen to recipients at equitaliaonline.it, agenziariscossione.gov.it and eq.it
- office@fic.org.rs - Trojan-Downloader.O97M.Donoff - Only Ikarus Detection

Victim Email Domain

- ebs-inkjet.pl - - Industrial ink-jet Printer Producer company out of Poland.
- gmail.com – Generic Mail
  agr.wa.gov - Washington State
- Department of Agriculture
  electroputere.ro - - One of the largest power company out of Romania
- dhl.com – Shipping Company

Email Subject line examples

- As instructed by our company\'s ceo - No connection to above lists
- AWS Notification - Subscription Confirmation – No connection to above lists
- ABB NEW ORDER - – No connection to above lists

International Sinkhole IP

- 14.170.89.181 - Vietnam Posts and Telecommunications Group
- 223.230.117.164 - Airtel Broadband, India
- 42.113.166.66 - FPT Telecom Company, Vietnam
- 223.230.24.84 - - Airtel Broadband, India
- 177.86.4.209 – Toledonet telecom Brazil

US Sinkhole IP

- 73.6.183.46 - COMCAST
- 198.38.92.138 - Mochahost.com - web page hosting company (Server Central Network
- 64.119.18.209 - Univision – Television Network out of NY
- 64.119.25.86 - - Univision – Television Network out of NY
- 64.119.20.169 - - Univision – Television Network out of NY

Top Pastebin Hits

- http://pastebin.com/KXdiKG0r - SOCKS4/SOCKS5 PROXY LIST
- http://pastebin.com/0iNs7egH - List of Unidentified IP addresses.
- http://pastebin.com/cGPmy5mv - List of Unidentified IP addresses.
- http://pastebin.com/gYYBqn0H - List of Unidentified IP addresses.
- http://pastebin.com/wDK4Vu6z - List of Unidentified IP addresses

GLOBAL TRENDS:

MENA – Israel / Iran

Israeli intelligence and security agency Shin Bet reportedly informed Benny Gantz, current Israeli leader Benjamin Netanyahu's political challenger, that his phone had been hacked by Iran around the time of his campaign announcement. Shin Bet reported that Iranian programmers retrieved personal details and text messages, revealing both personal and profession information.[6] Gantz denies any personal or blackmail information was

[6] https://www.i24news.tv/en/news/israel/197133-190315-gantz-on-gaza-border-israel-lost-its-deterrence

taken by the Iranians. This information grab was during the time of the recent Gaza rocket attacks into Israel and their airstrike retaliation.

This is a stark reminder to corporate cell phone users (especially C-Suite level professionals) that their phones are always susceptible to hacks for economic espionage or worse, terrorist purposes. Many cell phone antivirus tools are free[7] and should be utilized. If one is higher in an organization, other professional, paid antivirus tools may be required.

Algeria

The "Shaky Six" is an exclusive group of oil producers no one wants to join. Algeria is experiencing a current political crisis which is causing their future oil production to become tenuous (or "shaky) at best. As a results, Algeria is now the latest OPEC member to have become so vulnerable that it forms part of the "Shaky Six" group of nations suffering involuntary output cuts or is at risk of seeing their oil production fall. This adds yet another complication for the OPEC+ oil ministers as they gather in Baku, Azerbaijan this past week to assess the effectiveness of their latest output deal and what they all need to accomplish to rebalance the oil market. A drop in Algerian supply would add to the OPEC cuts already being implemented, but makes it more difficult for them to forecast when restrictions may ease.

Algeria's fate was sealed by 82-year-old President Abdelaziz Bouteflika's decision in February 2019 to seek a fifth term in office in elections that were due to take place on April 18. This triggered mass street protests, which did not dissipate after he withdrew his candidacy on 11 March 2019. Instead, the protests continued as the Bouteflika's decision to delay the polling until after a national conference on the country's political future was taken. Thiscitizens viewed as a disingenuous tactic to avoid real political and governmental reform.

For Algerian oil markets, the demonstrations that have continued included their Mediterranean ports of Arzew and Bejaia, which handle nearly 90 percent of the country's crude and oil condensate exports. This is not necessarily an immediate threat to oil production, as the country's oil and gas fields are situated further inland. But limited oil storage capacity means that any disruption to flows through export terminals from workers' strikes will very rapidly affect their output. If the protests continue to escalate, the attention of the Algerian security services may shift to quelling political unrest and away from protecting remote oil and gas fields. That could leave those facilities vulnerable to the types of attack that hit Algeria in January 2013, when Al-Qaeda terrorists overran the In-Amenas gas field and killed at least 38 hostages.

The recent experiences of some of the other members of the "Shaky Six," Angola, Iran, Libya, Nigeria and Venezuela; provide troubling precedents for the current state of Algeria's output. The closest comparable may be Libya, where civil unrest has seen repeated attacks on oil infrastructure. Storage tanks have been destroyed in battles to control export terminals, limiting the ability to keep pumping when storms close the ports. Production at Libya's largest oil field is now recovering, the field was then taken over last month (January 2019) by forces loyal to eastern militia leader Khalifa Haftar. If the current situation in Algeria continues to deteriorate, it could suffer some of the same types of disruption, although perhaps not on the same devastating scale.

EUROPE – France

[7] https://www.top10bestantivirus.com/best-free-antivirus

Figure 2. Paris Burns - Anarchist symbol

Rioters looted luxury stores and destroyed restaurants while lighting fires along Paris' Champs Elysees Avenue on 16 March 2019; marking the 16th straight week of Yellow Vest ("gilets jaunes") Protests. Shop owners boarded up smashed windows the next day after the worst unrest in central Paris since violence peaked before Christmas 2018 in a weekly series of protests. On 18 March 2019, the Macron government fired the Paris police chief and has banned any future Yellow Vest protests on the Champs Elysees if agitators are involved.

This movement began as a protest to the rise in diesel fuel tax increase and quickly spiraled into a broader movement against Macron, his pro-business reforms and elitism in general. Now this protest has evolved into mainly anarchists' actions against the French federal government. There seems to be a growing trend of anarchist infiltrating many European based social movements like the original Yellow Vest protest or various peaceful environmental groups and turn them into violent protest actions. The Extinction Rebellion, reported last week by Wapack Labs, is an example of infiltrated environmental groups and pushing potential violence protest tactics.

EURASIA – Russia

Venezuela proclaimed this past week that may re-route crude oil which was initially bound for the US to Russia and other countries. This stated by the Venezuela's Oil Minister and head of the state oil firm PDVSA.[8] Russia is the staunchest supporter and ally of Nicolas Maduro's regime in the political power struggle in the Latin American country who sit on top of the world's largest oil reserves. Russia has stood by Maduro for years and has poured billions of US dollars in Venezuela in the form of loans and oil investments. In another sign of the closer Maduro-Russia ties, the Venezuelan Oil Minister was in Baku, Azerbaijan and set to visit Moscow Russia in early April 2019 to open their PDVSA office. Maduro ordered the PDVSA headquarter moved from Lisbon Portugal to the Russian capital earlier this month.

ASIA – Vietnam

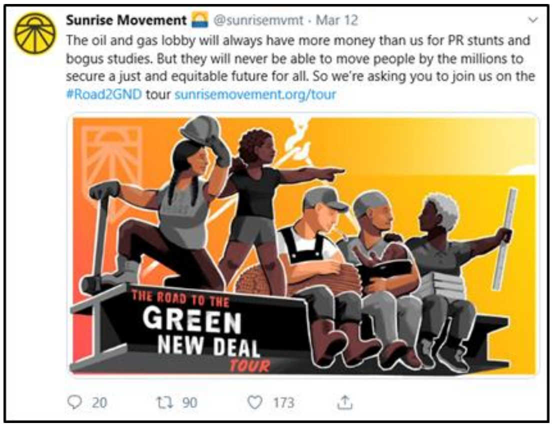
On 15 March 2019, Wapack Labs detected that hackers were able to install keylogger and steal passwords of a Vietnamese user for the Saigon Newport Corporation portal. Saigon Newport was established in 1989 by the Vietnamese government. They are the biggest container terminal operator in Vietnam with the sea -port operation services like: cargo handling, Logistics, Maritime services, salvage, pilot, real estate, office building, civil and military, construction. provides oil and gas logistics services and multi-modal transportation services.

The compromised accounts had special access to pages allowing tracking vessel information hxxps://eport.saigonnewport[.]com[.]vn/Pages/Common/Ships_new (screenshot) and container information hxxps://eport.saigonnewport[.]com[.]vn/Pages/Common/Containers_new. The hacker used the Hawkeye keylogger and dan.max89@yandex.com for the account. Special attention should be placed with this email (Blacklist).

[8] https://oilprice.com/Latest-Energy-News/World-News/Venezuela-Says-It-May-Send-US-Bound-Oil-To-Russia.html

NORTH AMERICA – US

The Sunrise Movement, @sunrisemvmt, continues to attract new members to mobilize against the oil and gas industry in the US and internationally. The Sunrise Movement states that, “We are building an army of young people to stop climate change and create millions of good jobs in the process. This dark time in America must come to an end.” The movement is actively targeting and becoming successful with very young, non-traditional protest types.



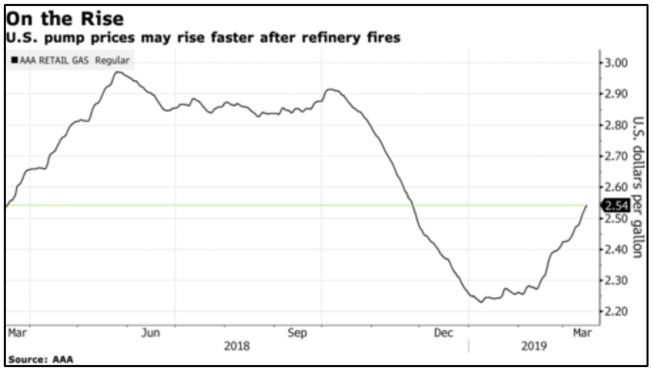
Sunrise Movement @sunrisemvmt · Mar 12

The oil and gas lobby will always have more money than us for PR stunts and bogus studies. But they will never be able to move people by the millions to secure a just and equitable future for all. So we're asking you to join us on the #Road2GND tour sunrisemovement.org/tour

On 15 March 2019, young school aged teens near Central Park in New York City were seen walking out of their schools and calling for more action on solving the climate crisis. The Youth #ClimateStrike was started by 16-year-old activist Greta Thunberg in Sweden and now being mimicked across the US. Greta Thunberg is a 16-year-old Swedish political activist who is seeking to stop global warming and climate change.

In August 2018, she became a prominent figure for starting the first school strike for climate, outside a Swedish parliament building. She is being nominated for a Nobel Peace Prize for climate activism. NY US Congressional Representative Alexandria Ocasio-Cortez tweeted @AOC, “I am so proud of NYC youth taking their future into their own hands today with a #ClimateStrike. Young people around the world are beginning to launch climate walkouts to pressure their governments into acting on a real climate change plan for their lifetimes, now.” It is of interest these anti-oil and gas programs are being promoted in elementary and secondary schools in the US. Wapack Labs will continue to monitor anti-oil environmental activism.

Intercontinental Terminals Company (ITC) plant, a petrochemical facility in Deer Park, TX, burst into flames on 17 March 2019 at approximately 10:30AM.[9] There were 30 employees at the facility when the fire started. The cause remains unknown. The ITC terminal is the second to catch fire over the weekend. On Saturday 16 March 2019, there was a fire at an ExxonMobil plant in Baytown, TX. On 15 March 2019, there was a fire at a Phillips 66 oil facility. All fires are under investigation. With supplies in the US on the lower supply side, analysts are predicting a rise in US gasoline process.



On the Rise

U.S. pump prices may rise faster after refinery fires

Source: AAA

Lawmakers in several US states are introducing bills that would increase criminal penalties for people who trespass "critical infrastructure" facilities, such as oil and gas pipelines, power plants, and petrochemical refineries. According to many legislators, these bills are a reaction to widespread protests of oil and gas infrastructure. Some of the protests grew to national and international attention. Protest examples include the indigenous-led protests at Standing Rock in North Dakota and in Iowa against the Dakota Access Pipeline, who are opposing the Keystone

[9] https://www.chron.com/news/houston-texas/article/Deer-Park-tells-city-to-shelter-in-place-as-plant-13695162.php

XL pipeline from Nebraska to Texas; protests of the Bayou Bridge pipeline in Louisiana, and opposition to several pipeline projects in Pennsylvania.

Five states have enacted some form of these bills into law: North Dakota, South Dakota, Oklahoma, Iowa, and Louisiana.[10] Many of these bills are virtually identical and some speculate are being driven by oil companies. Several companies and lobbying organizations used groups like the American Legislative Exchange Council (ALEC) and the Council of State Governments (CSG) to put these policies into the hands of legislators. These model "critical infrastructure" anti-protest bills adopted by ALEC and by CSG would allow prosecutors to impose large fines and felonies, not only on individuals who are arrested, but organizations that are deemed to be supporting those individuals.

SOUTH AMERICA – Venezuela

Venezuela's key oil export terminal Jose is now back in operation, after days of electrical grid shuts downs and massive blackouts. These shuts downs stopped operations in Jose. Meanwhile, more than 6 million barrels of Venezuelan crude oil on 11 tankers, initially bound for the US are sitting stranded in the Atlantic due to the US sanctions. PDVSA is now asking for prepayment for oil shipments, but the US firms are not allowed to pay PDVSA because of the sanctions; instead they are directed to deposit the payments in escrow accounts.

This situation has resulted in US refiners Valero Energy and Citgo, the US unit of PDVSA, proposing to return crude oil loaded before the sanctions were imposed, while Chevron has unsuccessfully tried to legally pay for oil it had contracted to buy, citing an internal document of the Venezuelan state oil firm it had seen. This is causing PDVSA to seek other buys of their oil.[11] See EURASIA section.

Venezuelan crude exports are now down to 350,000 barrels a day, according to latest oil collection data. Crude oil from Venezuela has been tracked to Gibraltar for ship-to-ship transfer to other merchant tankers. This is a new development which further complicates the final oil destination from Venezuela, since the January 2019 US sanctions.[12] Two tankers this past week have been tracked transferring Venezuelan oil in waters off Gibraltar, according to vessel tracking data. These are the first ship to ship (STS) transfers seen in the Mediterranean for Venezuelan crude. Suezmax vessel M/T Matala (owned by TMS Tankers), transferred its 1m-barrel crude cargo to another Suezmax tanker, the M/T Marlin Savannah on 15 March 2019 in waters off of Gibraltar.

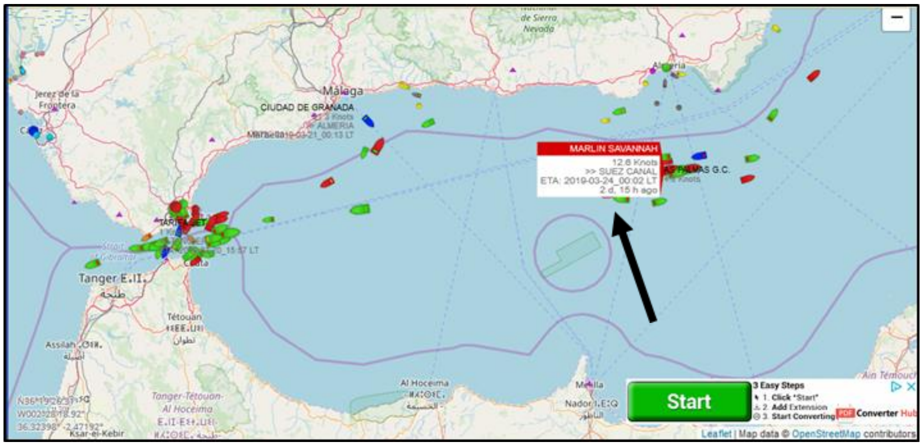


Figure 3. M/T Marlin Savannah track on 20 MAR 2019

The M/T Marlin Savannah is now sailing in the Mediterranean off Algeria and signaling its next destination as the Suez Canal. Their likely destination in somewhere in Asia. Another TMS

[10] https://www.prwatch.org/news/2019/03/13456/state-bills-criminalize-peaceful-protest-oil-gas-critical-infrastructure
[11] https://oilprice.com/Latest-Energy-News/World-News/Venezuela-Says-It-May-Send-US-Bound-Oil-To-Russia.html
[12] https://lloydslist.maritimeintelligence.informa.com/LL1126697/Shiptoship-transfers-obscure-Venezuelan-oil-trades

Tanker-owned vessel, M/T Karekare, was alongside Cosco Shipping's VLCC Xin Mao Yang on 19 March 2019, in Gibraltar's STS zone, suggesting a second STS was under way. Both tankers loaded 1m-barrel cargoes in Puerto La Cruz, on 28 February and 2 March 2019 respectively.

Exports of oil from Venezuela are now the lowest on record, going back to 2004. Some 10.9m barrels have been loaded on tankers for export from 1-5 March 2019, bringing the monthly pace so far to 350,000 bpd. That is just over one third of the 1m bpd tracked oil exported in February 2019, and below the 1.5m bpd averaged in 2019. India is currently the biggest buyer of Venezuelan crude, importing more than 300,000 bpd in 2019, followed by China at 230,000 bpd. In addition to the Matala, TMS Tankers currently has four tankers laden with Venezuelan crude on the water: the M/Ts Alicante, Shiraga, and Fontana - all heading east for Asia. Another two tankers, Vilamoura and Mindoro are currently at anchor in Venezuelan waters waiting to load. Neither shipping companies would respond to media requests.

Maritime insurers and their attorneys are warning owners that US/Venezuelan sanctions prevent financial transactions in US dollars involving Venezuela oil exchanges. Additionally, vessels that have made port calls to Venezuela, will likely subject to greater inspection if they arrive in a US port. PDSVA has defaulted on charter payments for tankers and ended a 25-year association with a German ship management company, Bernhard Schulte Shipmanagement (BSM). BSM is in the process of handing back 15 ships it has managed on behalf of the Venezuelan national oil company.

The fate of four Greek shipper Dynacom tankers, who are engaged in a long-term charter to PDSVA, remains uncertain. All vessels are said to be in the process of being returned to PDSVA. M/Ts Morning Glory, Felicity, and Pericles are currently at anchor in Venezuelan waters, while the fourth vessel, M/T Ice Energy, has switched off its AIS transponder. On 22 March 2019, the M/T Pericles was moored off the coast of Punto Fijo, Venezuela. A legal source is reporting that PDVSA's fleet is now in danger of being arrested beyond Venezuelan waters due to unpaid fees to various service providers.[13]

Standard & Poor's (S&P) rating agency is expected to remove PDVSA from its coverage amid growing financial constraints and a lack of transparency. In the past, S&P put PDVSA on "selective default," just below full default. PDVSA owns 18 tankers, 15 of which are idled in and around Venezuela.

AFRICA – Nigeria

Nigerian is planning to restructure their Nigeria National Petroleum Corporation (NNPC) joint operating agreements with international oil and gas companies. This could help raise substantial financial gains to support the country's national budget and also create an opening for more international oil companies to invest in shares that traditionally would be surrendered by the national oil agency.

Many see the motivating force behind the planned reduction of NNPC share in joint ventures to 40 percent, is to raise additional financing to support President Buhari's $24.4 billion national budget for next year. It could also signify NNPC's multinational partners would either increase their share in any joint ventures, with possibilities of more oil and gas companies entering Nigeria's lucrative offshore space.[14]

Current joint ventures in Nigeria's offshore oil fields include Chevron Nigeria Ltd in which NNPC holds 60 percent while Chevron owns 40 percent. Under the proposed restructuring there is likely to be 20 percent shareholding

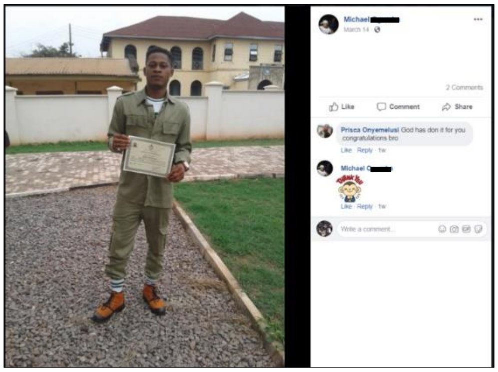
[13] https://lloydslist.maritimeintelligence.informa.com/LL1126550/PDVSAs-woes-deepen

[14] https://www.oedigital.com/news/464288-nigeria-aims-to-cut-national-oil-company-shareholding

that is become viable to Chevron. Chevron was one time the second leading oil producer in Nigeria. Mobil Producing Nigeria Unlimited is another joint venture that could be restructured under the government proposal. NNPC has also partnered with Elf in both on and offshore fields with the national oil company holding with the same 60/40 percentage split. The Texaco Overseas Petroleum Company of Nigeria Unlimited (TOPCON) venture, NNPC also has 60 percent ownership leaving Texaco and Chevron with 20 percent share apiece. Udoma oil company has not provided details of their relationship with NNPC.

Nigeria is known for making broad policy pronouncements which often end up on the drawing room floor. Many are dubious the restructuring of NNPC for joint venture in oil assets will ever be fully realized.

Of note: Wapack Labs was tracking a hacking group in Port Harcourt Nigeria. During the past presidential and state elections and currently, this group has gone dark. This could represent a government crackdown on hacking activities to help entice international investments. This group as involved in invoice fraud and traditional Nigerian 419 phishing type attacks.



Michael [redacted]
March 14

2 Comments

Prisca Onyemelusi God has don it for you congratulations bro
Like · Reply · 1w

Michael [redacted]
Like · Reply · 1w

Figure 4. Port Harcourt member

On 18 March 2019, it is alleged that Muslim terrorists Boko Haram kill hundreds of Christians in Nigeria. Muslim terrorists continued to descend on Nigeria's Middle Belt region, killing more than 140 people in predominantly Christian localities since February while much of the world was focused on the isolated murder spree by a deranged shooter at a New Zealand mosque on March 15. "Scores" are believed to have been killed last Monday in Michika, a small town in Nigeria's eastern Adamawa State and a predominantly Christian area.

Fleeing residents have blamed Boko Haram.[15] Added to attacks by Muslim Fulani herders elsewhere in Nigeria, the death toll among Christians at the hands of Muslim extremists may have surpassed 100 since the beginning of March 2019. Community leaders in Michika, Adamawa, are appealing to Nigerian Army for more security and to deploy more troops and armored tanks.[16]

Figure 5. Union Bank bombed by Boko Haram

[15] https://www.lifesitenews.com/news/world-remains-silent-as-muslim-terrorists-kill-hundreds-of-christians-in-nigeria
[16] https://guardian.ng/news/boko-haram-we-need-more-troops-armoured-tanks-elders-in-michika-beg-nigerian-army/