EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

December 1, 2019 - Volume 11, Issue 23

Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Apple, Inc.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) today announced a $466,912 settlement with Apple, Inc. ("Apple"). Apple, a corporation based in Cupertino, California, has agreed to settle its potential civil liability for apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. part 598 (FNKSR). Apple appears to have violated § 598.203 of the FNKSR by dealing in the property or interests in property of SIS, d.o.o. ("SIS"), a Slovenian software company previously identified on OFAC's List of Specially Designated Nationals and Blocked Persons as a significant foreign narcotics trafficker. Specifically, from on or about February 24, 2015 to on or about May 9, 2017, Apple hosted, sold, and facilitated the transfer of SIS's software applications and associated content. OFAC determined that Apple voluntarily disclosed the apparent violations, and that the apparent violations constitute a non-egregious case.

NEWSLETTER NOTES

It Took Twitter a Whole Year to Shut Down This Russian Intel Account

A fake freelance reporter named Sophia Mangal was exposed as a GRU front years ago but her Twitter account was allowed to operate until this week.

Kevin Poulsen

Sr. National Security Correspondent

Published 11.14.19 4:52AM ET

U.S. orders family members of government employees to leave Bolivia

U.S. orders family members of government employees to leave Bolivia
WASHINGTON (Reuters) - The United States on Tuesday ordered family members of U.S. government employees to leave Bolivia due to civil unrest in the South American country, the State Department said in a statement.

The department also warned American citizens against traveling to Bolivia and said the U.S. government had limited ability to provide emergency services after a disputed election sparked protests that led Evo Morales to resign as president and flee the country.

Former Senior Alstom Executive Convicted at Trial of Violating the Foreign Corrupt Practices Act, Money Laundering and Conspriacy

Department of Justice
U.S. Attorney's Office
District of Connecticut
FOR IMMEDIATE RELEASE
Friday, November 8, 2019

WASHINGTON – A former senior executive with Alstom S.A. (Alstom), a French power and transportation company, was found guilty today for his role in a multi-year, multimillion-dollar foreign bribery scheme and a related money laundering scheme.

*(*Continued On The Following Column)*

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney John H. Durham of the District of Connecticut and Assistant Director in Charge Timothy R. Slater of the FBI's Washington Field Office made the announcement.

After a two-week trial, Lawrence Hoskins, 69, of the United Kingdom, was convicted of six counts of violating the Foreign Corrupt Practices Act (FCPA), three counts of money laundering and two counts of conspiracy. Sentencing has been scheduled for Jan. 31, 2020, before U.S. District Judge Janet Bond Arterton of the District of Connecticut.

According to the evidence presented at trial, Hoskins was a senior vice president for Alstom's International Network, who engaged in a conspiracy to pay bribes to officials in Indonesia – including a high-ranking member of the Indonesian Parliament and the President of Perusahaan Listrik Negara (PLN), the state-owned and state-controlled electricity company in Indonesia – in exchange for assistance in securing a $118 million contract, known as the Tarahan project, for Alstom Power Inc. of Connecticut and its consortium partner, Marubeni Corporation, to provide power-related services for the citizens of Indonesia. To conceal the bribes, Hoskins and his co-conspirators retained two consultants purportedly to provide legitimate consulting services on behalf of Alstom Power Inc., in connection with the Tarahan project. The primary purpose of hiring the consultants was to conceal the bribes to Indonesian officials, the evidence showed.

The first consultant retained by Hoskins and other members of the conspiracy received hundreds of thousands of dollars in his Maryland bank account to be used to bribe the member of Parliament, the evidence showed. The consultant then transferred the bribe money to a bank account in Indonesia for the benefit of the official. According to emails admitted at trial, Hoskins and other co-conspirators discussed in detail the use of the first consultant to funnel bribes to the member of Parliament and the influence that the member of Parliament could exert over the Tarahan project, including referring to him as a "cashier."

The trial evidence further showed that, in the fall of 2003, Hoskins and his co-conspirators determined that the first consultant was not effectively bribing key officials at PLN, who expressed concerns that the first consultant was just going to give them "pocket money" and "disappear" after Alstom Power Inc. won the project. As a result, the co-conspirators retained a second consultant to more effectively bribe PLN officials. Evidence revealed that Hoskins and his co-conspirators pressed Alstom Power Inc. to front-load the second consultant's terms of payment in order to "get the right influence" due to upcoming elections. Hoskins and his co-conspirators were successful in securing the Tarahan project and subsequently made payments to the consultants for the purpose of bribing the Indonesian officials.

(*Continued On The Following Page)

The FBI's Washington Field Office is investigating the case with assistance from the FBI's Meriden, Connecticut, Resident Agency. The Department appreciates the significant cooperation provided by its law enforcement colleagues in Indonesia, Switzerland's Office of the Attorney General and the United Kingdom, as well as authorities in France, Germany, Italy, Singapore and Taiwan.

Senior Deputy Chief Daniel S. Kahn and Assistant Chief Lorinda Laryea of the Criminal Division's Fraud Section and Assistant U.S. Attorney David E. Novick of the District of Connecticut are prosecuting the case.

The Fraud Section is responsible for investigating and prosecuting all FCPA matters. Additional information about the Justice Department's FCPA enforcement efforts can be found at www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

OFAC FINES COMPANY FOR AIRCRAFT ENGINE LEASE

Apollo Aviation Group, which is now part of Carlyle Aviation Partners Ltd., has agreed to pay a $210,600 civil penalty to settle 12 alleged violations of the Sudanese Sanctions Regulations, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) said.

The violations began on July 30, 2013, when Apollo leased two aircraft engines to a company in the United Arab Emirates, which in turn subleased the engines to a Ukrainian airline that installed them on an aircraft leased to Sudan Airways.

At the time of the violations, Sudan Air was listed on OFAC's Specially Designated Nationals and Blocked Persons (SDN) List for its ownership by the Sudanese government. U.S. persons and companies are generally prohibited from exporting to entities on the SDN List.

OFAC did not name the United Arab Emirates company or the Ukrainian airline in the settlement agreement.

Apollo's agreement with the company in the United Arab Emirates included a provision prohibiting the lessee from maintaining, operating, flying or transferring the engines to any countries that are subject to U.S. and UN sanctions. However, OFAC said Apollo "failed to monitor or otherwise verify the actual whereabouts of these aircraft engines during the life of its leases."

*(*Continued On The Following Column)*

Sudan Air used the two engines from November 2014 to February 2015, before they were returned to Apollo in March 2015.

Before it was discovered that the engines had been installed on the Sudan Air plane, Apollo in late May 2015 had already leased a third aircraft engine to the United Arab Emirates company, which followed the same pattern of subleasing it to the Ukrainian airline for an aircraft leased to Sudan Air. Apollo ordered the engine returned in September 2015.

OFAC said Apollo could have been assessed a maximum $3 million civil penalty for the sanction violations, but the company filed a voluntary self-disclosure with the agency and the violations were considered "non-egregious."

The agency also noted Apollo implemented internal measures, including the addition of compliance personnel, systems and company-wide training on U.S. export laws, to prevent further sanctions violations. In addition, OFAC praised Apollo for providing information related to the violations "in a clear, concise and well-organized manner."

OFAC said the Apollo enforcement action "highlights the importance of companies operating in high-risk industries to implement effective, thorough and ongoing, risk-based compliance measures, especially when engaging in transactions concerning the aviation industry."

In July, OFAC issued an advisory to the civil aviation industry to warn of deceptive practices used by Iran to get around U.S. and UN sanctions to support its aviation industry. Although the advisory focuses on Iranian aviation, the agency said participants in the civil aviation industry should be aware that others subject to U.S. sanctions may use similar deceptive practices. OFAC removed Sudan Air from the SDN List on Oct. 12, 2017.

The Carlyle Group (NASDAQ: CG) completed the acquisition of Apollo on Dec. 19, 2018. Apollo was established in 2002 by Bill Hoffman and Robert Korn and had about $5.6 billion in assets at the time of the acquisition.

Iran-related Designation

11/22/2019
OFFICE OF FOREIGN ASSETS CONTROL

Specially Designated Nationals List Update
The following individual has been added to OFAC's SDN List:

AZARI JAHROMI, Mohammad Javad, Iran; DOB 16 Sep 1981; POB Jahrom, Iran; Additional Sanctions Information - Subject to Secondary Sanctions; Gender Male (individual) [IRAN] [IRAN-TRA].

Temporary General License: Extension of Validity, effective November 18, 2019

On May 16, 2019, Huawei Technologies Co., Ltd. (Huawei) and sixty-eight of its non-U.S. affiliates were added to the Entity List. On August 19, 2019, the Bureau of Industry and Security (BIS) added forty-six additional non-U.S. affiliates of Huawei to the Entity List. The Huawei entities were added to the Entity List because they pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. Those additions to the Entity List imposed a licensing requirement under the Export Administration Regulations (EAR) regarding the export, reexport, or transfer (in-country) of any item subject to the EAR to any of the listed Huawei entities. The Entity List-based licensing requirement applied in addition to any other license requirement applicable under the EAR to the proposed transaction. On May 22, 2019, BIS published a temporary general license, effective May 20, 2019, that modified the effect of the listing in order to temporarily authorize engagement in certain transactions, involving the export, reexport, or transfer (in-country) of items subject to the EAR to the 69 listed Huawei entities. On August 21, 2019, BIS published an extension of the temporary general license, effective August 19, 2019, that extended the validity of the temporary general license through November 18, 2019, and made changes, including adding to the scope of the temporary general license forty-six additional non-U.S. affiliates of Huawei, effective August 19, 2019. At this time, the U.S. Government has decided to extend the temporary general license through February 16, 2020. In order to implement this decision, this final rule revises the temporary general license to remove the expiration date of November 18, 2019, and substitute the date of February 16, 2020.

U.S. Court of International Trade Confirms Limits to Section 232 Action

by Devin S. Sikes

In just one opinion, the landscape surrounding national security tariffs has undergone a dramatic shift. In Transpacific Steel LLC v. United States, an otherwise narrow dispute regarding steel imports from Turkey subject to national security tariffs, the U.S. Court of International Trade (CIT) wrote in broad terms that Congress has placed checks on the President's authority under Section 232 of the Trade Expansion Act of 1962. That statute authorizes the President to take action against imports that threaten to impair the national security.

*(*Continued On The Following Column)*

In advancing his trade policies, President Trump has relied heavily on Section 232, examining whether imports of aluminum, steel, uranium, autos and auto parts, and titanium sponge threaten to impair national security. Indeed, President Trump has used Section 232 more frequently than any of his predecessors. Transpacific may change the way that President Trump and his successors employ Section 232 to address imports that purportedly threaten to impair the nation's security.

Background

In March 2018, President Trump imposed a tariff of 25 percent on steel imports pursuant to Section 232. Those tariffs applied to steel imports from most countries, though the President negotiated agreements that exempted imports from some countries from the tariffs and placed quotas on imports from other countries.

Fast forward to August 2018. The political relationship between the leaders of the United States and Turkey had deteriorated significantly. President Trump increased the tariff on steel imports from Turkey from 25 to 50 percent, ostensibly due to the devaluation of the Turkish Lira.

Several months later, Transpacific Steel LLC (Transpacific), an importer of Turkish steel, filed suit at the CIT. Transpacific challenged the President's decision to double the tariff on steel imports from Turkey and advanced several claims, including that the President's action offends the Fifth Amendment's equal protection guarantees and failed to follow statutorily mandated procedures. Transpacific sought a refund equal to the difference in the tariff rates.

In the months that followed, CIT Chief Judge Stanceu assigned Transpacific's appeal to a three-judge panel consisting of Judges Kelly, Katzmann and Restani. The government moved to dismiss Transpacific's appeal, alleging that Transpacific failed to state a claim for which the CIT could grant relief.

The Decision

In an opinion authored by Judge Kelly and joined by Judge Restani, the CIT denied the government's motion to dismiss. The CIT held that Transpacific has advanced plausible claims based on equal protection and procedural violations, such that Transpacific may proceed with its refund claim against the government. In reaching that conclusion in this rather narrow dispute, the CIT included direct and firm statements on the limits of Section 232 that have the potential to broadly impact how this and future presidents administer Section 232.

(*Continued On The Following Page)

Equal Protection Violation

Transpacific alleges that the President's action offends equal protection guarantees in the Fifth Amendment because it singles out Turkish steel imports for a higher tariff rate. The CIT observed that, to survive an equal protection challenge, the government did "not have a high hurdle to clear" and would need only to "articulate any set of facts that rationally justify" the higher tariff rate assigned to Turkish steel imports. Slip Op. at 6. Nevertheless, the CIT reasoned that "it is difficult to imagine Presidential action in connection with {S}ection 232 where one would be at a loss to conjure a rational justification; yet, the reality of this case proves otherwise." Id. at 7. The CIT rejected every single reason that the government advanced to support the disparate tariff rate treatment. Those attempted justifications focused on a supposed general need to increase tariffs; allegedly high volumes of Turkish steel imports; and the allegedly high number of trade remedy orders against Turkish steel imports. Id. at 7–8. The CIT concluded that it "cannot sustain a classification for which there is no offered—or even possible—rational justification tethered to the statute." Id. at 8.

Procedural Violation

Transpacific alleges that, in doubling the tariff rate on Turkish steel imports some five months after initially imposing tariffs on steel imports generally, the President failed to follow the procedures set forth in Section 232. The government retorted that the President could continue or modify any Section 232 remedy at will, so long as the President concurred with the Secretary of Commerce at some earlier point in time that certain imports supposedly threaten to impair the national security, just as President Trump had done in March 2018 with respect to steel imports.

The CIT emphatically disagreed, holding that "{t}he President's expansive view of his power under {S}ection 232 is mistaken, and at odds with the language of the statute, its legislative history, and its purpose." Id. at 10. The CIT observed that Section 232's "clear and unambiguous steps—of investigation, consultation, report, consideration, and action—require timely action from the Secretary of Commerce and the President" because Section 232 requires the President to "eliminate" any national security threat posed by imports. Id. at 9, 10. Summarizing its conclusion in different words, the CIT held that Section 232 "cabins the President's power both substantively, by requiring the action to eliminate threats to national security caused by imports, and procedurally, by setting the time in which to act." Id. at 10–11. The CIT buttressed its conclusion by pointing to the fact that "Congress added specific time limits to {S}ection 232" in 1988, which "clarifies that Congress wanted the President to do all that he thought necessary as soon as possible." Id. at 11. The CIT concluded with unequivocal statements on the importance of these statutory procedural requirements:

(*Continued On The Following Column)

The procedural safeguards in {S}ection 232 do not merely roadmap action; they are constraints on power. . . . The time limits, in particular, compel the President to do all that he can do immediately, and tie presidential action to the investigative and consultative safeguards. If the President could act beyond the prescribed time limits, the investigative and consultative provisions would become mere formalities detached from Presidential action. However, Congress affirmatively linked the investigative and consultative safeguards to Presidential action, and Congress strengthened that link when it imposed time limits on the President's discretion to take action. Congress embedded these limits within its broad delegation of power to the President. . . . The broad discretion granted to the President and the limits on judicial review only reinforce the importance of the procedural safeguards Congress provided, and which the President appears to have ignored.

Id. at 12–13 (footnotes and citations omitted). Notably, the CIT distinguished the President's action to double the tariff rate on Turkish steel imports from scenarios in which "Congress envisioned ongoing action by the President"—namely, when negotiations to eliminate a national security threat fail or if the negotiated agreement does not eliminate the threat. Id. at 14 n. 15. The CIT did not address, however, whether "ongoing action" includes a President's ability to extend the negotiation period, a move that President Trump has considered to address imports of autos and auto parts.

Finally, Judge Katzmann concurred with the majority opinion, but he wrote separately to express his concerns that Section 232 offends the non-delegation doctrine because it "provides power to the President in international trade without meaningful limitation" and therefore "violate{s} the Constitution's separation of powers." Id. at 15. Earlier this year, Judge Katzmann raised these same concerns in a separate dubitante opinion in American Institute for International Steel, Inc. v. United States. In Judge Katzmann's view, Transpacific "may well yield further evidence of the infirmity of" Section 232. Id. at 16.

Transpacific represents the first judicial opinion to cast doubt on the lawfulness of action taken by President Trump under Section 232. To be sure, Transpacific addresses a unique situation specific to Turkish steel imports. Nevertheless, if not overturned on appeal, the direct and clear statements in Transpacific lay the groundwork for future challenges to the President's use of Section 232 to restrain U.S. imports.

Of course, Transpacific resolves only the opening salvo in this dispute. The CIT's decision merely authorizes Transpacific to proceed with its refund claim against the government. The CIT ordered the parties to submit a briefing schedule in early December. From there, the parties will address the issues on the merits. Unless the government pursues an interlocutory appeal to the U.S. Court of Appeals for the Federal Circuit or stipulates to judgement so that it may appeal Transpacific, a decision on the merits is likely months away.

The United States once again kicks the Huawei can down the road

By Clare Duffy, CNN Business
Updated 2:33 PM ET, Mon Novemember 18, 2019

New York (CNN Business)The Department of Commerce has again extended the temporary general license allowing American companies to sell to Huawei, the embattled Chinese tech company. The existing temporary license was set to expire Monday.

The announcement is good news for Huawei and for American tech companies who rely on it as a key customer. The Commerce Department also said the extension is largely designed to help the rural US wireless providers who use Huawei's inexpensive equipment in their networks. But it also represents continued isolation of Huawei, which has been working to become less reliant on American components in the face of US pressure, resulting in an increasingly independent Chinese tech giant.

"The Department will continue to rigorously monitor sensitive technology exports to ensure that our innovations are not harnessed by those who would threaten our national security," Commerce Secretary Wilbur Ross said in a statement Monday.

The Trump administration says Huawei's networking equipment carries risks to US national security because its telecommunications gear could be used for spying by Beijing. The US government has also accused Huawei of skirting sanctions and stealing intellectual property from American companies, all claims that Huawei staunchly denies.

In May, the Commerce Department put Huawei on the "Entity List," a trade blacklist that makes it illegal for American companies to do business with it without a license. But the move posed a serious threat to its American suppliers — Huawei is the largest telecom company in the world, the second largest smartphone maker and it buys tens of billions of dollars in products from US companies every year. The action has also weighed on Huawei's smartphone sales.

Soon after the Entity List action was announced, the Commerce Department granted the temporary general license. It allows American companies to sell certain products that don't pose a security risk to Huawei, such as software updates and microchips used for older wireless equipment. It was first extended in August. Monday's announcement is the third 90-day iteration of the license, which is now set to expire in February.

*(*Continued On The Following Column)*

Earlier this month, Ross told Bloomberg TV that more permanent licenses for individual companies to sell to Huawei would be coming "shortly." He said the Commerce Department had received 260 applications for such licenses. The Commerce Department did not immediately respond to a request for comment on the current status of those individual licenses. Also counting on the ability to do business with Huawei is a group of about 40 small wireless carriers in the rural US that have built their networks using the Chinese company's equipment. Those carriers say it could cost billions and take months to rip out the Huawei equipment and replace it. The temporary general license pushes out the timeline for them to have to do that, and could be a way of buying time until Congress could pass legislation proposed in September that would provide $1 billion to those carriers to help them replace Chinese equipment.

"The Temporary General License extension will allow carriers to continue to service customers in some of the most remote areas of the United States who would otherwise be left in the dark," Ross said in the Monday statement.

The news also comes as a breakthrough in the US-China trade deal, in which Huawei has been implicated, remains just out of reach. President Donald Trump and Chinese leader Xi Jinping have been expected to sign a partial trade deal for about a month, though negotiations over the final text of the deal hit yet another snaglast week.

In the meantime, Huawei has been working to become less reliant on American components for its products in case pressure from the US government does not let up. The company in August announced its own operating system, a backup plan to replace Google's Android. It has also developed its own smartphone chipsets.

All that could make Huawei into an international tech player that competes even more directly with American companies, rather than relying on their technology for its success. Some worry that could threaten American dominance of the tech industry.

"If somebody from the government believes that Windows on a laptop sold by Huawei would create a national security risk to the United States, then of course that's something that we want to talk about ... but we don't think that is the case," Microsoft President Brad Smith told CNN's Poppy Harlow last month. Microsoft has applied for an individual license to sell to Huawei.

"Right now, there is not a Chinese competitor for in the PC operating system space," Smith said. "Is it really in the United States' economic interest to create not only an incentive, but the necessity to go create a Chinese operating system? Because once it's created, it will compete with us around the world."

(*Continued On The Following Page)

For its part, Huawei says extending the temporary general license will have little affect on its business and argues that it shouldn't have been placed on the Entity List to begin with.

"This has done significant economic harm to the American companies with which Huawei does business, and has already disrupted collaboration and undermined the mutual trust on which the global supply chain depends," Huawei said in a statement. "We call on the US government to put an end to this unjust treatment and remove Huawei from the Entity List."

CNN's Brian Fung contributed to this report.

FBI warns of major ransomware attacks as criminals go “big-game hunting”

Threat data firms see spike in sophisticated criminal ransomware operations.

SEAN GALLAGHER - 10/7/2019, 4:26 PM

The FBI has issued a public service announcement entitled "High Impact Ransomware Attacks Threaten US Businesses and Organizations." While the announcement doesn't provide any details of specific attacks, the Bureau warns in the announcement:

Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 [the Internet Crime Complaint Center] and FBI case information

This pronouncement will come as no surprise to anyone who's followed the wide-ranging ransomware attacks against cities, counties, state agencies, and school districts over the course of 2019. While some of the most publicized attacks—such as the Baltimore City "RobbinHood" attack in May—have appeared to be opportunistic, many more have been more sophisticated and targeted. And these attacks are but the most visible part of an upsurge in digital crime seen by commercial information security firms thus far in 2019. In fact, sophisticated criminal attacks have nearly fully eclipsed state actors' activity—despite there not being any reduction in state-sponsored attacks.

*(*Continued On The Following Column)*

Data from CrowdStrike has shown a rise in what the firm refers to as "big-game hunting" over the past 18 months. These attacks focus on high-value data or assets within organizations that are especially sensitive to downtime—so the motivation to pay a ransom is consequently very high.

"Big-game hunters are essentially targeting people within an organization for the sole purpose of identifying critical assets for the purpose of deploying their ransomware," said Jen Ayers, CrowdStrike's Vice President in charge of the Falcon OverWatch threat-hunting service in an interview with Ars. "[Hitting] one financial transaction server, you can charge a lot more for that than you could for a thousand consumers with ransomware—you're going to make a lot more money a lot faster."

While CrowdStrike saw a significant uptick in this sort of attack in the second half of 2018, Ayers explained, "we've seen quite a bit of that happening in the beginning half of the year, to the point where it's actually dominating our world right now in terms of just a lot of activity happening."

The industries targeted by these sorts of attacks have included healthcare, manufacturing, managed services, and media. But since May, attacks increasingly targeted state and local governments, library systems, and school districts. Since many government agencies are short on budget and security resources but have a strong need to stay up and running to provide services, they have naturally become an attractive target to these sorts of attacks.

Ayers acknowledged:It has been interesting in the targeting of these what you would typically think of as small entities... But there is wide-scale impact when you look at destructive campaigns like this. I mean, everybody kind of more thinks of—forgets about the local and town government and their day-to-day operations, but that's no marriage certificate. That's no building permit. That's no vehicle-excise tax payments. That's no local, state tax payments depending on where you live.

The fact that attackers are specifically targeting these sorts of organizations speaks to them knowing how well their security is done, is pretty big. In terms of having that kind of understanding—to know to hit these entities and how to hit these entities—that is very interesting.

That understanding comes down to having done reconnaissance on organizations' key calendar dates. A series of ransomware attacks against schools last month appeared to be timed to have ransoms expire just before the first day of school—putting districts in the position of having to either delay opening or pay up.

*(*Continued On The Following Page)*

Breaking and entering

The FBI IC3 notice cited three primary ways ransomware operators are getting into networks for these targeted attacks: email phishing campaigns, exploitation of Remote Desktop Protocol (RDP), and known vulnerabilities in software.

The phishing attacks the FBI has investigated in connection with ransomware recently "have been more targeted" than past opportunistic attacks. The phishing is often focused initially on compromising the victim's email account so that an internal email account can be used to spread malware and evade spam filtering.

Email credentials may also be used in remote desktop-based attacks. But in general, the RDP attacks—common in gaining access to hospitals and other organizations that leave RDP accessible for third-party service providers to perform product support—have generally relied on one of two things. They either use brute-force "credential stuffing" attacks against logins, or they have used credentials stolen by others that are sold on underground online marketplaces.

"Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems," the FBI warned.

Scanning for vulnerabilities was a primary means of initial compromise for attacks such as the SamSam ransomware that hit several hospitals in Maryland in 2016. But targeted attacks are also leveraging vulnerabilities to gain a foothold to deploy their attacks. The FBI notice reported that "cyber criminals recently exploited vulnerabilities in two remote management tools used by managed service providers (MSPs) to deploy ransomware on the networks of customers of at least three MSPs." This statement is likely at least partially in reference to the over 20 Texas municipalities hit by ransomware this summer through an MSP's network.

Rent-a-hack

Two other areas of criminal hacking have spiked in the first half of this year, according to CrowdStrike's data—and one of them is tied closely to some of the ransomware attacks. Ayers said that there has been an uptick in criminal organizations essentially selling access to the networks of victims. The organizations are performing nearly nation-state style intrusions to provide other actors with a footprint for attacks.

"The higher-level organizations within the criminal realm are selling and outsourcing their distribution mechanisms to get a bigger, wider spread," Ayers said. "So we've seen a lot more players in sort of the big-game hunting than we had last year because it is now much more, much easier to do."

*(*Continued On The Following Column)*

Smaller organizations will rent capabilities to gain access to potential victims. Then they'll use that access to perform reconnaissance before eventually dropping ransomware.

The third group seen on the rise, Ayers said, is "really still focused on the data—on exfiltrating and taking information." But this group is using more advanced capabilities to hang around, with an uptick in what Ayers described as "hands-on keyboard types of activity"—using their access to manually explore victims' networks, much like state actors have in espionage operations.

"We haven't quite yet made an inference in terms of what the objectives are at this point," she said. "But it is certainly a third tier that we hadn't seen in the past."

NEW NAFTA NOT PROBABLE 2019

Pelosi calls new NAFTA the 'easiest trade deal we've ever done,' but doesn't rule out vote next year

Republicans growing increasingly worried that time is running out for a vote this year, and that it won't be possible to consider next year

House Speaker Nancy Pelosi said President Donald Trump's new NAFTA deal is the "easiest trade deal that we've ever done."

"We're on a path to yes, and I think every day brings us closer to agreement," Pelosi told a roundtable with Bloomberg reporters and editors on Friday. "I'd like to have it done as soon as it's ready. I wouldn't rule it out next year. Hopefully we can do it sooner, but I said when it's ready we'll do it."

Democratic negotiators and the Trump administration are close to finalizing fixes to the U.S.-Mexico-Canada Agreement, Pelosi said Friday, adding that she believes the deal could serve as a template for future trade agreements if they get it right.Her positive attitude on the trade deal comes after the House on Thursday voted to formalize its impeachment investigation of the president, marking the beginning of the public phase of the process.

Pelosi said that approving the trade agreement won't be influenced by the impeachment inquiry and the timeline will depend on when the deal is ready.

Earlier this year, Pelosi designated a group of Democrats to negotiate changes to the agreement with U.S. Trade Representative Robert Lighthizer, focusing in particular on strengthening the labour and enforcement provisions.

(*Continued On The Following Page)

House Ways and Means Chairman Richard Neal, who is leading the Democratic working group, said this week that the two sides made significant progress. He also called on AFL-CIO President Richard Trumka, Lighthizer and committee staff to meet soon to resolve outstanding differences.

Trumka this week met with progressive lawmakers and told them not to rush to a vote. At the same time, he indicated that the negotiators are getting close to the finish line.

So far, many labour groups have said the agreement isn't good enough, but it's not clear if they would pressure Democrats to kill the entire deal.

Republican lawmakers and Trump administration officials have become increasingly concerned that time is running out for a vote on the agreement this year and that it won't be possible to consider it next year, people familiar with the internal deliberations said.

Bloomberg News reported earlier this week that the administration and Congress are still negotiating and have major differences on the language of the legislation that lawmakers will vote on, indicating another uphill battle.

Samsung Heavy Industries to pay $75 million to resolve bribery case

Samsung Heavy has admitted to paying about $20 million to a Brazilian intermediary between 2007 and 2013 knowing that parts of it would be paid as bribes to officials

Samsung heavy industries Co Ltd has agreed to pay more than $75 million in criminal penalties to resolve a US investigation of a scheme to pay millions of dollars in bribes to officials in Brazil, the US Justice Department said on Friday.

Samsung Heavy has admitted to paying about $20 million to a Brazilian intermediary between 2007 and 2013 knowing that parts of it would be paid as bribes to officials in Brazil's state-run oil company Petrobras SA for a contract which facilitated the sale of a drillship by Samsung Heavy, the Justice Department said in a statement.

Samsung Heavy will pay at least half of the total fine to the US government under a deferred prosecution agreement filed in the Eastern District of Virginia, it said.

President Trump Waffles On Hong Kong Democracy Bill Amid China Trade Talks

President Trump said Friday he supports pro-democracy demonstrators in Hong Kong. But he stopped short of saying he would sign legislation requiring sanctions against China for any crackdown on Hong Kong protesters.

"We have to stand with Hong Kong, but I'm also standing with President Xi," Trump said in an interview on the Fox News program Fox and Friends. "He's a friend of mine."

The U.S. House and Senate this week passed the Hong Kong Human Rights and Democracy Act with overwhelming, veto-proof support. The bill calls for stripping Hong Kong of its preferential trade status if China fails to maintain the freedoms guaranteed to the former British colony when Beijing took over more than two decades ago.

Now it heads to Trump's desk as the U.S. and China attempt to broker a mini trade deal that would boost China's purchases of American farm goods

The talks have stumbled over how much tariff relief the Trump administration is willing to grant China.

If no deal is reached by mid-December, the administration is preparing to impose new tariffs on another $160 billion worth of Chinese imports, including popular consumer items such as cellphones and laptops.

"The bottom line is we have a very good chance to make a deal," Trump said Friday, calling the Hong Kong protests a "complicating factor." China could withdraw from the talks if Trump signs the Hong Kong bill.

"I stand with Hong Kong. I stand with freedom," Trump said. "But we are also in the process of making the largest trade deal in history. And if we could do that, that would be great."

Hong Kong's pro-democracy parties sweeping pro-Beijing establishment aside in local elections, early results show

Figures compiled by the South China Morning Post newspaper show pro-democracy parties winning 108 seats and pro-Beijing parties just 12 out of a total of 452, with many swinging to the pro-democracy camp. The results appear to be an indictment of Hong Kong's political leaders and an endorsement of the protest movement.

Congress would override Trump if he vetoes Hong Kong support, says Republican leader

HALIFAX, Canada — Congress will override President Donald Trump if he vetoes bipartisan legislation meant to support pro-democracy protesters in Hong Kong, a Senate Republican leader said Saturday.

"There's overwhelming support for this — as you know, 100 [votes] in the United States Senate. I would imagine there would be an override of this. I would encourage the president to sign it," Senate Republican Conference Chairman John Barrasso, R-Wyo., told reporters. Barasso was responding to a question at the 2019 Halifax International Security Forum, where The John McCain Prize for Leadership in Public Service was presented to two residents of Hong Kong in support of their pro-democracy activism. Barasso shared the stage with a bipartisan congressional delegation and Cindy McCain, the widow of the late Senate Armed Services Committee chairman.

Trump's public wavering on the bill — in contrast with the resolve from key Republicans and Congress overall — marked another example for allies of a foreign policy divide in Washington. A key topic at the forum, which is focused on the shared democratic values that undergird America's alliances, was Trump's shift toward transactional geopolitics.

Barasso's sentiments echoed key proponents of the legislation from Trump's party, Sen. Ted Cruz, of Texas, and Senate Foreign Relations Committee Chairman Jim Risch, of Idaho, who have also urged Trump to sign the bill. Cruz emphasized in a statement Friday that the measures passed with veto-proof majorities

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)

"When we strive to become better than we are, everything around us becomes better too."

Fareed: While We're All Focused on Impeachment, Trump Is Upending US Foreign Policy

"While impeachment has been dominating the headlines, we are missing a set of stories about US foreign policy that might prove equally consequential," Fareed writes in his latest Washington Post column. "The Trump administration has been doubling down on a policy of unilateralism and isolationism—a combination that is furthering the abdication of American leadership and the creation of a much more unstable world."

That policy includes demands that South Korea and Japan pay more to house US troops, failed overtures to North Korea, outsourcing Middle East policy to strongmen, and undermining America's commitment to European NATO allies.

Russia and Iran are often blamed for undermining the global order, Fareed writes, but "the greatest threat to the liberal international order right now is surely the Trump administration, which is systematically weakening the alliances that have maintained peace and stability and rejecting the rules and norms that have helped set some standards in international life."