

## SPACEWALKING ASTRONAUTS PREP STATION FOR NEW PARKING SPOT

**CAPE CANAVERAL, Fla:** Astronauts ventured out on a spacewalk Friday to prep the International Space Station for a new parking spot. NASA's Shane Kimbrough and France's Thomas Pesquet emerged early from the orbiting complex, then went their separate ways to accomplish as much as possible 250 miles up.

"We are ready to get to work," Mission Control informed them. Their main job involves disconnecting an old docking port. This port needs to be moved in order to make room for a docking device compatible with future commercial crew capsules, and provide more clearance. The new docking device - the second of two - will fly up late this year or early next and hook onto this port.

If all goes well, flight controllers in Houston will relocate the old docking port tomorrow, using the

station's robotic arm. Then next Thursday, the crew will conduct another spacewalk to secure the unit.

SpaceX and Boeing are developing capsules capable of flying astronauts to and from the space station. Until the SpaceX Crew Dragon and Boeing Starliner come on line - possibly next year - US astronauts will have to keep riding Russian rockets to orbit. Before working on the docking port, Kimbrough replaced a computer-relay box with an upgraded version. Pesquet, meanwhile, looked for signs of a small ammonia coolant leak in outdoor plumbing. He patted and tugged at hoses, but did not spot any frozen flakes of ammonia. A GoPro camera caught his every move for playback later.

"No flakes. All good," Pesquet reported. Also on the spacewalkers' to-do list Friday: replace a pair of

Japanese cameras and grease latching mechanisms on the end of the big robot arm.

NASA wants to cram in two and possibly three spacewalks before Kimbrough, the station's commander, returns to Earth on April 10. Before a third spacewalk can be conducted, however, Orbital ATK needs to launch a cargo ship to the space station with replacement parts. That shipment was supposed to be there by now, but repeatedly has been delayed because of rocket concerns. It's unclear when the Atlas V rocket will be ready to soar from Cape Canaveral, Florida.

NASA has been contracting out cargo deliveries since the end of the space shuttle program in 2011. The space agency is counting on private companies to do the same with astronauts. — AP



**SEOUL:** Shin Jong-kyun, president and co-chief executive officer of Samsung Electronics Co, left, and Yoon Boo-keun, attend the company's annual general meeting at the Seocho office building in Seoul yesterday. — AP

# SAMSUNG SHAREHOLDERS HAIL STOCK PRICE GAINS

## SOME LAMENT CORRUPTION SCANDALS

**SEOUL:** Shareholders of Samsung Electronics praised the company yesterday for big gains in its share price while lamenting its involvement in a massive corruption scandal that brought the arrest of the company's de facto leader.

Kwon Oh-hyun, Samsung's chief executive, told an annual shareholders meeting the scandal was regrettable, but the company did nothing illegal. Five Samsung executives, including its vice chairman and founding family heir apparent Lee Jae-yong, have been indicted on bribery and other charges.

The scandal resulted in the impeachment of President Park Geun-hye earlier this month.

Calls to reform Samsung and other conglomerates are gaining momentum after Samsung, Hyundai, SK, LG and other major businesses made big donations to foundations controlled by a friend of Park's who has been charged with meddling in state affairs. Some shareholders expressed concern over growing public hostility to Samsung, South Korea's biggest company.

The company's image has also taken a big hit from cases of overheating and sometimes exploding batteries of its flagship Galaxy Note 7 smart phones. Samsung ended up discontinuing the product just weeks after it was launched in August. Shin Jong-kyun, a Samsung president, promised shareholders the company will put "flawless" products through extensive safety checks. The precautions would be perfect, he said.

Samsung is due to unveil the Galaxy S8 smartphone next week, its first major smartphone launch since the battery fiasco. But the main focus of attention during yesterday's meeting was the scandal.

Some found fault with the company's apologies. One shareholder, who said he worked at the company for 26 years, demanded an explanation for how Samsung's board of auditors, which included a former national chief prosecutor, could have allowed corporate funds to be misused.

Kwon, the chief executive, denied

Samsung did anything unlawful in making the donations to Park's associate. "It was a donation that was traditional and customary," Kwon said. "The auditing committee found it was executed through normal procedures."

Samsung says it will require its board of directors to approve any donations of over 1 billion won (\$89 million) to prevent future scandals. A newly created committee to improve the company's governance structure will be appointed by next month, the company said. It is still searching for a global business leader to join its board. While shareholders were shaken by the scandal and resulting damage to the company's image, many praised the company for delivering strong results overall.

Samsung stock jumped more than 60 percent from a year ago thanks to strong performance of its semiconductor business, which offset the damage from the Note 7 battery troubles.

"I can't help rejoicing over how the value of my asset has gone up," said one shareholder surnamed Park. — AP

## WIKILEAKS: CIA HACKED APPLE DEVICES IN WAYS USERS CAN'T FIX

**NEW YORK:** New documents from WikiLeaks point to an apparent CIA program to hack Apple's iPhones and Mac computers using techniques that users couldn't disable by resetting their devices.

Security experts say the exploits are plausible, but suggest they pose little threat to typical users. They say that many of the tricks are older - the iPhone hack involves the 3G model from 2008, for instance. The techniques also typically require physical access to devices, something the CIA would use only for targeted individuals, not a broader population. "The most notable part of this latest WikiLeaks release is that it shows the CIA doing exactly what we pay them to - exploit specific targets with limited attacks to support our national interests," said Rich Mogull, CEO of the security research firm Securosis.

Apple didn't respond to a request for comment. The CIA has not commented on the authenticity of this and earlier WikiLeaks revelations, but has previously said it complies with a legal prohibition against electronic surveillance "targeting individuals here at home, including our fellow Americans." The agency declined further comment Thursday.

### Document dump

The leaks Thursday come about two weeks after WikiLeaks published thousands of alleged CIA documents describing hacking tools it said the government employed to break into computers, mobile phones and even smart TVs from companies like Apple, Google, Microsoft and Samsung.

The latest disclosures are much more focused and consist of just 12 documents, all involving Apple products. The documents describe techniques for rewriting devices' firmware in ways that would maintain a hacker's access even if a user resets a phone or computer to factory settings. Doing so wipes out all apps and the operating system and installs a clean version; it is an extreme measure sometimes used to deal with technical problems, but is also the sort of step that someone suspicious of surveillance might take when getting a brand new phone.

A December 2008 document describes "NightSkies," a tool apparently designed to target the iPhone 3G; the document claims it can retrieve files such as contact lists and call logs and execute other commands. WikiLeaks suggested in a press release that the "CIA has been infecting the iPhone supply chain of its targets since at least 2008."

However, the document describes only how to install the malware on a "factory fresh" version of the 3G - specifically, the iPhone 3G running the 2.1 version of Apple's operating system, both of which are now nine years old.

But infecting all phones somewhere in the manufacturing process would be extremely difficult, said Mogull, especially given multiple layers of inspections conducted by Apple and its contractors. At most, he said, the CIA might have shipped a rogue phone individually to a target. And while it's possible that the CIA developed similar techniques for later iPhone models, Mogull said iPhones from the past few years have much greater security, including digital security certificates that cannot be overwritten. A flag would be raised during the setup process if certificates do not match. Johannes Ullrich, director of the Internet Storm Center at the SANS Institute, said NightSkies might not even be a current project given that the document was last updated in 2008, while the leaks appear to have come in 2016. — AP