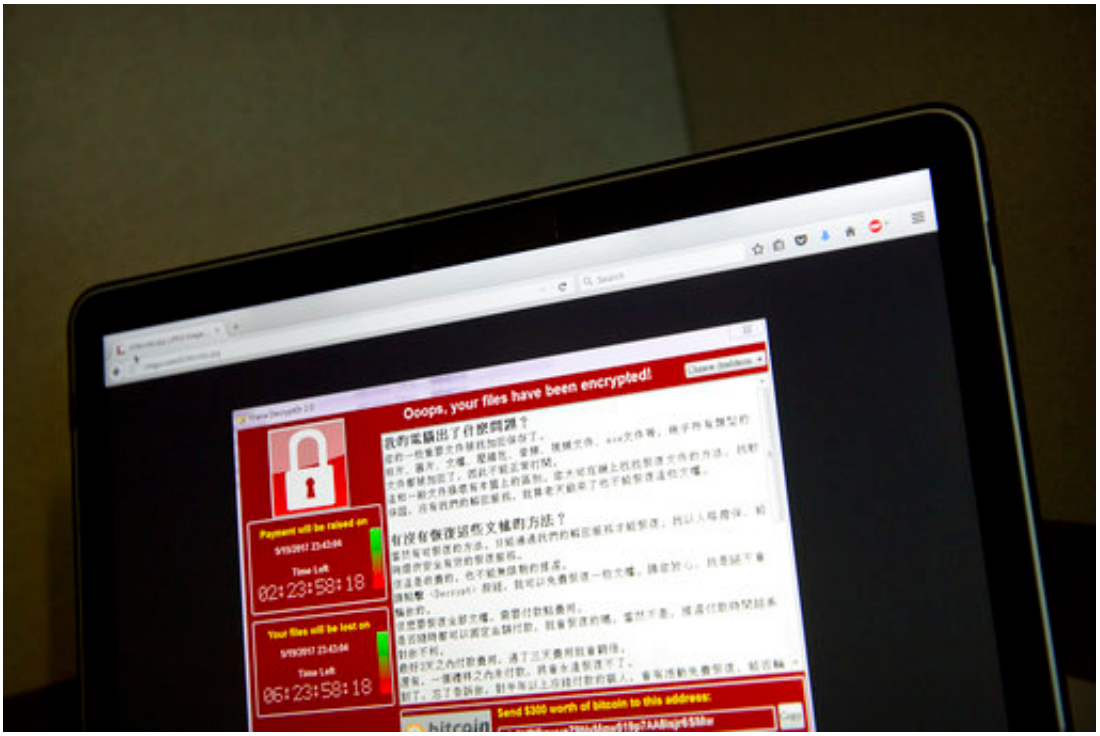
Cyberattack wave ebbs, but experts see risk of more

May 15 2017, by Jill Lawless And Danica Kirka



In this May 13, 2017 file photo, a screenshot of the warning screen from a purported ransomware attack, as captured by a computer user in Taiwan, is seen on laptop in Beijing. Global cyber chaos is spreading Monday, May 14, as companies boot up computers at work following the weekend's worldwide "ransomware" cyberattack. The extortion scheme has created chaos in 150 countries and could wreak even greater havoc as more malicious variations appear. The initial attack, known as "WannaCry," paralyzed computers running Britain's hospital network, Germany's national railway and scores of other companies and government agencies around the world. (AP Photo/Mark Schiefelbein, File)

The "ransomware" cyberattack that has hit companies and governments around the world ebbed in intensity on Monday, though experts warned that new versions of the virus could emerge.

Thousands more infections were reported Monday, largely in Asia, which had been closed for business when the malware first struck Friday. The cases were more contained, however, than the systemic outbreak that last week paralyzed computers running factories, banks, government agencies and transport systems around the world.

Many of the 200,000 victims in more than 150 countries were still struggling to recover from the first attack of the so-called "WannaCry" virus.

Carmaker Renault said one of its French plants, which employs 3,500 people, wasn't reopening Monday as a "preventative step."

Britain's National Health Service said about a fifth of NHS trusts—the regional bodies that run hospitals and clinics—were hit by the attack on Friday, leading to thousands of canceled appointments and operations. Seven of the 47 affected trusts were still having IT problems Monday.

As cybersecurity firms worked around the clock to monitor the situation and install a software patch, new variants of the rapidly replicating malware were discovered Sunday. One did not include the so-called kill switch that allowed researchers to interrupt the malware's spread Friday by diverting it to a dead end on the internet.

A patient takes a nap on her wheelchair as she waits with others at the registration desk at Dharmais Cancer Hospital in Jakarta, Indonesia, Monday, May 15, 2017 as the hospital's information system is in trouble by cyberattack. Global cyber chaos was spreading Monday as companies booted up computers at work following the weekend's worldwide "ransomware" cyberattack. The extortion scheme created chaos in 150 countries and could wreak even greater havoc as more malicious variations appear. (AP Photo/Dita Alangkara)

Ryan Kalember, senior vice president at Proofpoint Inc., which helped stop its spread, said the version without a kill switch could spread. It was benign because it contained a flaw that prevented it from taking over computers and demanding ransom to unlock files but other more malicious ones will likely pop up.

"We haven't fully dodged this bullet at all until we're patched against the vulnerability itself," Kalember said.

Lynne Owens, director-general of Britain's National Crime Agency, said there was no indication of a second surge of the cyberattack, "But that doesn't mean there won't be one."

Tim Stevens, a lecturer in global security at King's College London, said the incident should be a wakeup call to both the public and private sectors to incorporate security into computer systems from the ground up, rather than as an afterthought.

"This thing cannot be brushed under the carpet," he said. "It is so visible and so global. There is going to have to be change at levels where change can be made."

On Monday, Chinese state media said 29,372 institutions there had been infected along with hundreds of thousands of devices.

Patients wait at the registration desks at Dharmais Cancer Hospital in Jakarta,

Indonesia, Monday, May 15, 2017. Global cyber chaos was spreading Monday as companies booted up computers at work following the weekend's worldwide "ransomware" cyberattack. The extortion scheme created chaos in 150 countries and could wreak even greater havoc as more malicious variations appear. (AP Photo/Dita Alangkara)

Universities and other educational institutions in the country were among the hardest hit, possibly because schools tend to have old computers and be slow to update operating systems and security.

On social media, students complained about not being able to access their work, and people in various cities said they hadn't been able to take their driving tests because some local traffic police systems were down.

Railway stations, mail delivery, gas stations, hospitals, office buildings, shopping malls and government services also were reportedly affected.

In Japan, 2,000 computers at 600 locations were reported to have been affected. Companies including Hitachi and Nissan Motor Co. reported problems but said they had not seriously affected their operations. In Indonesia, the malware locked patient files on computers in two hospitals in the capital, Jakarta, causing delays.

In Britain, the government denied allegations that lax cybersecurity in the financially stretched, state-funded health service had helped the attack spread.

Prime Minister Theresa May said "warnings were given to hospital trusts" about the Microsoft vulnerability exploited by the attackers.

People walk in front of the headquarters building of Hitachi Ltd., center, in Tokyo, Monday, May 15, 2017. The global "ransomware" cyberattack hit computers at 600 locations in Japan, but appeared to cause no major problems as Japanese started their workday Monday even as the attack caused chaos elsewhere. Hitachi spokeswoman said emails were slow or not getting delivered, and files could not be opened. The company believes the problems are related to the ransomware attack, although no ransom appears to have been demanded so far. They were installing software to fix the problems. (AP Photo/Shizuo Kambayashi)

NHS Digital, which oversees U.K. hospital cybersecurity, said it sent alerts about the problem—and a patch to fix it—to health service staff and IT professionals last month.

Experts urged organizations and companies to immediately update older Microsoft operating systems, such as Windows XP, with a patch released

by Microsoft Corp. to limit vulnerability to a more powerful version of the malware—or to future versions that can't be stopped.

The attack held users hostage by freezing their computers, popping up a red screen with the words, "Oops, your files have been encrypted!" and demanding money through online bitcoin payment—$300 at first, rising to $600 before it destroys files hours later.

Microsoft distributed a patch two months ago that protected computers from such an attack, but in many organizations it was likely lost among the blizzard of updates and patches that large corporations and governments strain to manage.

The president of Microsoft laid some of the blame at the feet of the U.S. government. Brad Smith criticized U.S. intelligence agencies, including the CIA and National Security Agency, for "stockpiling" software code that can be used by hackers. Cybersecurity experts say the unknown hackers who launched the attacks used a vulnerability that was exposed in NSA documents leaked online.

Tom Bossert, a homeland security adviser to President Donald Trump, said "criminals" were responsible, not the U.S. government. Bossert said the U.S. hasn't ruled out involvement by a foreign government, but that the recent ransom demands suggest a criminal network.

In this May 11, 2017 file photo, the emblem of a Nissan car is seen at its showroom in Tokyo. Japan has fallen victim of a global "ransomware" cyberattack that has created chaos in 150 countries. Nissan Motor Co. confirmed Monday, May 15, 2017, some units had been targeted, but there was no major impact on its business. (AP Photo/Eugene Hoshiko, File)

Bossert told ABC's "Good Morning America" that the attack is something that "for right now, we've got under control" in the United States.

So far, not many people have paid the ransom demanded by the malware, Europol spokesman Jan Op Gen Oorth told The Associated Press.

Eiichi Moriya, a cybersecurity expert and professor at Meiji University, warned that paying the ransom would not guarantee a fix.

"You are dealing with a criminal," he said. "It's like after a robber enters your home. You can change the locks but what has happened cannot be undone."