Experts: Cyberattack havoc could grow as work week begins

May 14 2017, by Sylvia Hui And Sara Burnett

In this May 12, 2017 photo, a display panel with an error can be seen at the main railway station in Chemnitz, Germany. Germany's national railway says that it was among the organizations affected by the global cyberattack but there was no impact on train services. Deutsche Bahn said early Saturday that departure and arrival display screens at its stations were hit Friday night by the attack. (P. Goezelt/dpa via AP)

An unprecedented "ransomware" cyberattack that has already hit tens of thousands of victims in 150 countries could wreak even more havoc Monday as people return to their desks and power up their computers at the start of the work week.

Officials and experts on Sunday urged organizations and companies to update their operating systems immediately to ensure they aren't vulnerable to a second, more powerful version of the malicious software. The cyberattack paralyzed computers that run Britain's hospital network, Germany's national railway and scores of other companies and government agencies worldwide.

The attack, already believed to be the biggest online extortion scheme ever recorded, is an "escalating threat" after hitting 200,000 victims across the world since Friday, according to the head of Europol, Europe's policing agency.

"The numbers are still going up," he said. "We've seen that the slowdown of the infection rate over Friday night, after a temporary fix around it, has now been overcome by a second variation the criminals have released."

His concerns were echoed by James Clapper, former director of national intelligence under President Barack Obama. In an interview on ABC's "This Week," Clapper said the worry was "this ransomware attack will be even larger" as people return to their desks after the weekend.

People walk past a Megafon mobile phones shop in Moscow, Russia, Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

The 200,000 victims included more than 100,000 organizations, Europol spokesman Jan Op Gen Oorth told The Associated Press. He said it was too early to say who was behind the onslaught and what their motivation was, aside from the obvious demand for money. So far, he said, not many people have paid the ransom demanded by the malware.

The attack held users hostage by freezing their computers, encrypting their data and demanding money through online bitcoin payment—$300 at first, rising to $600 before it destroys files hours later.

The effects were felt across the globe, with Britain's National Health Service, Russia's Interior Ministry and companies including Spain's

Telefonica, FedEx Corp. in the U.S. and French carmaker Renault all reporting disruptions.

Chinese media reported Sunday that students at several universities were hit, blocking access to their thesis papers and dissertation presentations.

An exterior view shows the main entrance of St Bartholomew's Hospital, in London, one of the hospitals whose computer systems were affected by a cyberattack, Friday, May 12, 2017. A large cyberattack crippled computer systems at hospitals across England on Friday, with appointments canceled, phone lines down and patients turned away. (AP Photo/Matt Dunham)

Had it not been for a young British cybersecurity researcher's accidental discovery of a so-called "kill switch," the malicious software likely would have spread much farther and faster.

The 22-year-old researcher known as "MalwareTech," who wanted to

remain anonymous, said he spotted a hidden web address in the "WannaCry" code and made it official by registering its domain name. That move, which cost just $10.69, redirected the attacks to the server of Kryptos Logic, the security company where he works. The server operates as a "sinkhole" to collect information about malware—and in Friday's case kept the malware from escaping.

While that quick thinking may have slowed the outbreak, MalwareTech said he was now looking into a possible second wave of attacks.

"It's quite an easy change to make, to bypass the way we stopped it," he told the AP.

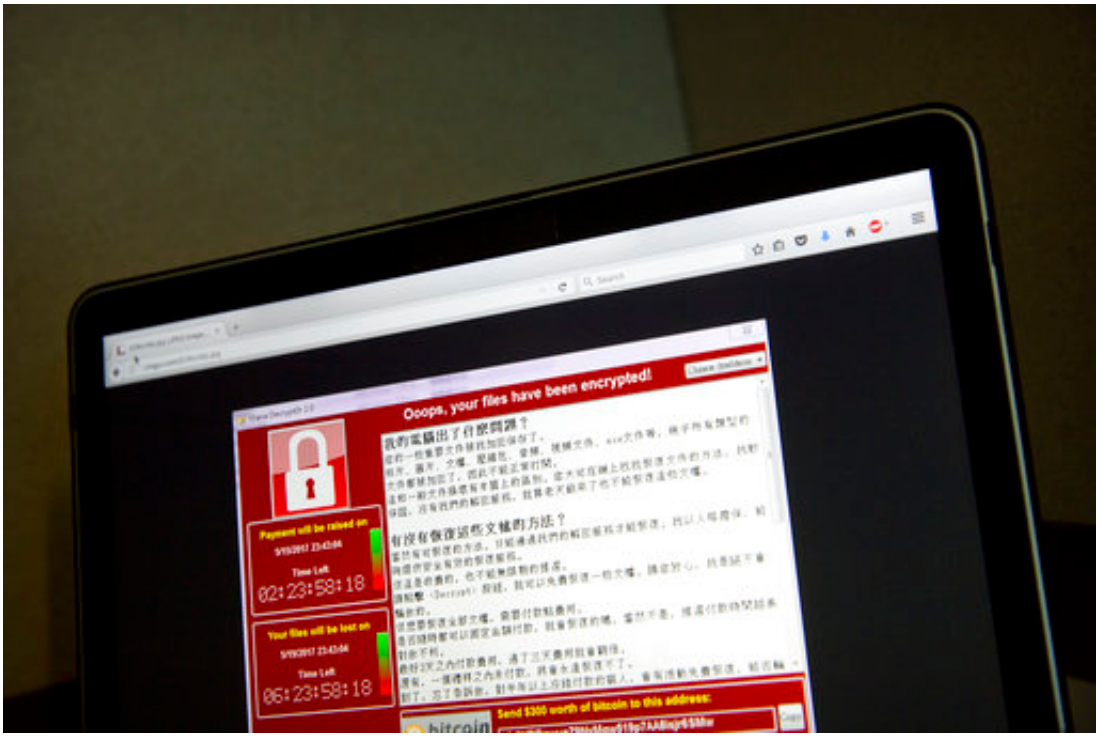
A security guard stands outside the Telefonica headquarters in Madrid, Spain, Friday, May 12, 2017. The Spanish government said several companies including Telefonica had been targeted in ransomware cyberattack that affected the Windows operating system of employees' computers. (AP Photo/Paul White)

Darien Huss, a 28-year-old research engineer who helped MalwareTech, agreed the threat was far from over.

"We could potentially see copycats mimic the delivery or exploit method they used," he said.

Both joined security officials in urging organizations to protect themselves by installing security fixes right away, running antivirus software and backing up data elsewhere.

"Just patch their systems as soon as possible," MalwareTech said. "It won't be too late as long as they're not infected. It should just be a case of making sure installing updates is enabled, installing the updates, and reboot."



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, Saturday, May 13, 2017. Dozens of countries were hit with a huge cyberextortion attack

Friday that locked up computers and held users' files for ransom at a multitude of hospitals, companies and government agencies. (AP Photo/Mark Schiefelbein)

The ransomware appeared to exploit a vulnerability in Microsoft Windows that was purportedly identified by the U.S. National Security Agency for its own intelligence-gathering purposes. The NSA tools were stolen by hackers and dumped on the internet.

Experts say this vulnerability has been understood among experts for months, yet too many groups failed to take it seriously. Microsoft had "patched," or fixed it, in updates of recent versions of Windows since March, but many users did not apply the software fix.

Worse, the malware was able to create so much chaos because it was designed to self-replicate like a virus, spreading quickly once inside university, business and government networks.

Microsoft was quick to change its policy, announcing free security patches to fix this vulnerability in the older Windows systems still used by millions of individuals and smaller businesses. Before Friday's attack, Microsoft had made fixes for older systems, such as 2001's Windows XP, available only to those who paid extra for extended technical support.

People outside a Megafon mobile phone shop in Moscow, Russia, on Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

"The problem is the larger organizations are still running on old, no longer supported operating systems," said Lawrence Abrams, a New York-based blogger who runs BleepingComputer.com. "So they no longer get the security updates they should be."

Short of paying, options for those already infected are usually limited to recovering data files from a backup, if available, or living without them.

British cybersecurity expert Graham Cluley doesn't want to blame the NSA for the attack.

"There are other criminals who've launched this attack, and they are ultimately responsible for this," he said. "But there's clearly some culpability on the part of the U.S. intelligence services. Because they could have done something ages ago to get this problem fixed, and they didn't do it."

This April 12, 2016 file photo shows the Microsoft logo in Issy-les-Moulineaux, outside Paris, France. The cyberextortion attack hitting dozens of countries was a "perfect storm" of sorts. It combined a known and highly dangerous security hole in Microsoft Windows, tardy users who didn't apply Microsoft's March software fix, and a software design that allowed the malware to spread quickly once inside university, business and government networks. (AP Photo/Michel Euler, File)

He said most people "are living an online life," and these agencies have a duty to protect their countries' citizens in that realm as well.

"Obviously, they want those tools in order to spy on people of interest, on other countries, to conduct surveillance," Cluley said. "It's a handy thing to have, but it's a dangerous thing to have. Because they can be used against you. And that's what's happening right now."

People inside a Megafon mobile phones shop in Moscow, Russia, Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

A view of the logo of a Megafon mobile phone shop, in Moscow, Russia, on Saturday, May 13, 2017. A top Russian mobile operator said Friday it had come under cyberattacks that appeared similar to those that have crippled some U.K. hospitals. Pyotr Lidov, a spokesman for Megafon, said Friday's attacks froze computers in company's offices across Russia. (AP Photo/Ivan Sekretarev)

People are reflected in a glass sign of a Telefonica building in Madrid, Spain, Saturday, May 13, 2017. The Spanish government said several companies including Telefonica had been targeted in ransomware cyberattack that affected the Windows operating system of employees' computers. A cybersecurity expert Ori Eisen of Trusona says the biggest cyberextortion attack in history is going to be dwarfed by the next big ransomware attack that could be done to crucial infrastructure, like nuclear power plants, dams or railway systems. (AP Photo/Paul White)