《勒索病毒发生变种 传播速度可能会更快》

勒索病毒发生变种 传播速度可能会更快

?????“????”???????????150????????????????????????????????Kill Switch????????????????????????????????????

LonDON - An unprecedented "ransomware" cyberattack that has already hit tens of thousands of victims in 150 countries could wreak greater havoc as more malicious variations appear and people return to their desks Monday and power up computers at the start of the workweek.

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 software — or to future versions that can't be stopped.

The cyberattack paralyzed computers that run Britain's hospital network, Germany's national railway and scores of other companies and government agencies worldwide.

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

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 Rob Wainwright, the head of Europol, Europe's policing agency.

"The numbers are still going up," Wainwright 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."

Researchers discovered at least two variants of the rapidly replicating worm Sunday and one did not include the so-called kill switch that allowed them to interrupt its spread Friday by diverting it to a dead end on the internet.

Ryan Kalember, senior vice-president at Proofpoint Inc, said the version with no kill switch was able to spread but it contained a flaw that wouldn't allow it to take over a computer and demand ransom to unlock files. However, he said it's only a matter of time before such a version exists.

"I still expect another to pop up and be fully operational," Kalember said. "We haven't fully dodged this bullet at all until we're patched against the vulnerability itself."

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 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 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 US and French carmaker Renault all reporting disruptions.

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.

Security officials urged 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."

The ransomware appeared to exploit a vulnerability in Microsoft Windows that was purportedly identified by the US 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.

"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, though he said they have a duty to citizens who "are living an online life."

"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."