《近百国遭黑客攻击 奇虎360称可部分恢复被勒索病毒加密的文件》

近百国遭黑客攻击 奇虎360称可部分恢复被勒索病毒加密的文件

??????????????100????????????360????????——????????????????????360??

Colleges and gas stations in China among the hardest hit, expert says

The unprecedented spread of ransomware that has swept across more than 100 countries since Friday has been cracked by a Chinese tech company?at least in part.

Qihoo 360, a major internet security company in China, issued a software patch at 3 am on Sunday that can recover the data encrypted by the unidentified attackers. The software can operate without internet access, and customers do not need to pay for it.

Zheng Wenbin, the company's chief security engineer, said the recovery kit was built around a flaw his team found in the malware.

"Some ransomware developers directly encrypt the original files. That would be hard to crack. Lucky for us, the attackers only encrypted the copy and deleted the originals. So all we need to do is find ways to recover the deleted ones," Zheng explained. "Sometimes a simple idea is the most effective."

Zheng said that in an experimental run, his software's recovery rate reached 100 percent. However, in reality, the longer a user waits before using the tool, the higher the chance is of permanently losing some data, because the more changes a user makes to existing files, the harder it becomes to recover deleted data. This is because deleted data is not immediately erased, but the memory space it occupies is considered free and the computer will use it to store other data.

For now, the recovery kit is in Chinese only. Zheng said he does not know if the company will provide the service in English or other languages, though he admitted that changing the user language would be "fairly easy".

By 360's estimation, at least 200,000 computers had been breached by the malware as of 7 pm on Saturday. The number was going up quickly across the globe.

Schools, especially colleges where a lot of students live on campus with their personal computers and laptops, have been hit hard. According to 360's report, the intranets within education networks were especially vulnerable to the ransomware, as a particular virtual gate that is easily penetrated remains largely open on college networks.

Also severely hit were gas stations. China National Petroleum Corp, one of China's largest gas suppliers, said on its website that the payment system in many of its gas stations could not function due to the virus. Luckily, by noon

on Sunday, 80 percent of its stations had been reconnected to the company's central network, while credit cards, prepaid gas cards and online payment channels were being fixed.

Ransomware is a type of malware that deliberately encrypts a user's data through a virus or hack, then asks for a payment in exchange for unlocking the data.

This time, the attackers used a piece of malicious software called WannaCry, which takes advantage of a vulnerability in the Windows operation system used by most PCs around the globe, and demanded $300 in cryptocurrency Bitcoin.

The technology was reportedly stolen from the United States' National Security Agency.

Microsoft released a software update that could fix the weakness back in March, but not every user installs the latest patches on a regular basis.

Plus, Microsoft has stopped providing updates for older versions of Windows, including Windows XP, a classic product still widely used by many Chinese.

Microsoft issued later on Friday security updates for the outdated platforms including Windows XP, Windows 8 and Windows Server 2003. Phillip Misner, the company's principal security group manager, warned that customers should "use vigilance when opening documents from untrusted or unknown sources".