Manhunt for hackers behind global cyberattack (Update)

May 13 2017

The huge cyberattack wiped out display screens at rail stations in Germany

International investigators hunted Saturday for those behind an unprecedented cyber-attack that affected systems in dozens of countries, including at banks, hospitals and government agencies, as security experts sought to contain the fallout.

The assault, which began Friday and was being described as the biggest-ever cyber ransom attack, struck state agencies and major companies

around the world—from Russian banks and British hospitals to FedEx and European car factories.

"The recent attack is at an unprecedented level and will require a complex international investigation to identify the culprits," said Europol, Europe's police agency.

Europol said a special task force at its European Cybercrime Centre was "specially designed to assist in such investigations and will play an important role in supporting the investigation".

The attacks used ransomware that apparently exploited a security flaw in Microsoft operating systems, locking users' files unless they pay the attackers a designated sum in the virtual currency Bitcoin.

Images appeared on victims' screens demanding payment of $300 (275 euros) in Bitcoin, saying: "Ooops, your files have been encrypted!"

Payment is demanded within three days or the price is doubled, and if none is received within seven days the files will be deleted, according to the screen message.

But experts and government alike warn against ceding to the hackers' demands.

"Paying the ransom does not guarantee the encrypted files will be released," the US Department of Homeland Security's computer emergency response team said.

"It only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information."

'Painful'

Experts and officials offered differing estimates of the scope of the attacks, but all agreed it was huge.

Mikko Hypponen, chief research officer at the Helsinki-based cyber security company F-Secure, told AFP it was the biggest ransomware outbreak in history, saying that 130,000 systems in more than 100 countries had been affected.

He said Russia and India were hit particularly hard, largely because Microsoft's Windows XP—one of the operating systems most at risk—was still widely used there.

French police said there were "more than 75,000 victims" around the globe, but cautioned that the number could increase "significantly".

The virus spread quickly because the culprits used a digital code believed to have been developed by the US National Security Agency—and subsequently leaked as part of a document dump, according to researchers at the Moscow-based computer security firm Kaspersky Lab.

Microsoft said the situation was "painful" and that it was taking "all possible actions to protect our customers".

It issued guidance for people to protect their systems, while taking the highly unusual step of reissuing security patches first made available in March for Windows XP and other older versions of its operating system.

Europe worst hit

US software firm Symantec said the majority of organisations affected were in Europe, and the attack was believed to be indiscriminate.

The companies and government agencies targeted were diverse.

In the United States, package delivery group FedEx said it was "implementing remediation steps as quickly as possible," while French carmaker Renault was forced to stop production at sites in France, Slovenia and Romania.

Russia's interior ministry said some of its computers had been hit by a "virus attack" and that efforts were underway to destroy it. The country's banking system was also attacked, although no problems were detected, as was the railway system.

Germany's rail operator Deutsche Bahn said its station display panels were affected. Universities in Greece and Italy also were hit.

China's network information safety working group sent a warning to universities about the cyber-attack and the National Internet Emergency Center suggested that users update Windows security patches.

Shanghai's Fudan University received reports that a large number of school computers were infected with the virus.

Accidental 'kill switch'

Kaspersky said it was "trying to determine whether it is possible to decrypt data locked in the attack—with the aim of developing a decryption tool as soon as possible."

On Saturday, a cyber security researcher told AFP he had accidentally discovered a "kill switch" that could prevent the spread of the ransomware.

The researcher, tweeting as @MalwareTechBlog, said registering a

domain name used by the malware stops it from spreading, though it cannot help computers already affected.

"If you have anything to patch, patch it," the researcher said in a blog post. "Now I should probably sleep."

A hacking group called Shadow Brokers released the malware in April claiming to have discovered the flaw from the NSA, Kaspersky said.

"Unlike most other attacks, this malware is spreading primarily by direct infection from machine to machine on local networks, rather than purely by email," said Lance Cottrell, chief scientist at the US technology group Ntrepid.

G7 finance ministers meeting in Italy vowed to unite against cyber crime, as it represented a growing threat to their economies and should be tackled as a priority. The danger will be discussed at the G7 leaders' summit next month.

In Britain, the attack disrupted care at National Health Service facilities, forcing ambulances to divert and hospitals to postpone operations.

"There will be lessons to learn from what appears to be the biggest criminal cyber-attack in history," Interior minister Amber Rudd said.

"But our immediate priority as a government is to disrupt the attack, restore affected services as soon as possible, and establish who was behind it so we can bring them to justice."

https://phys.org/news/2017-05-unprecedented-cyberattacks-wreak-global-havoc.html