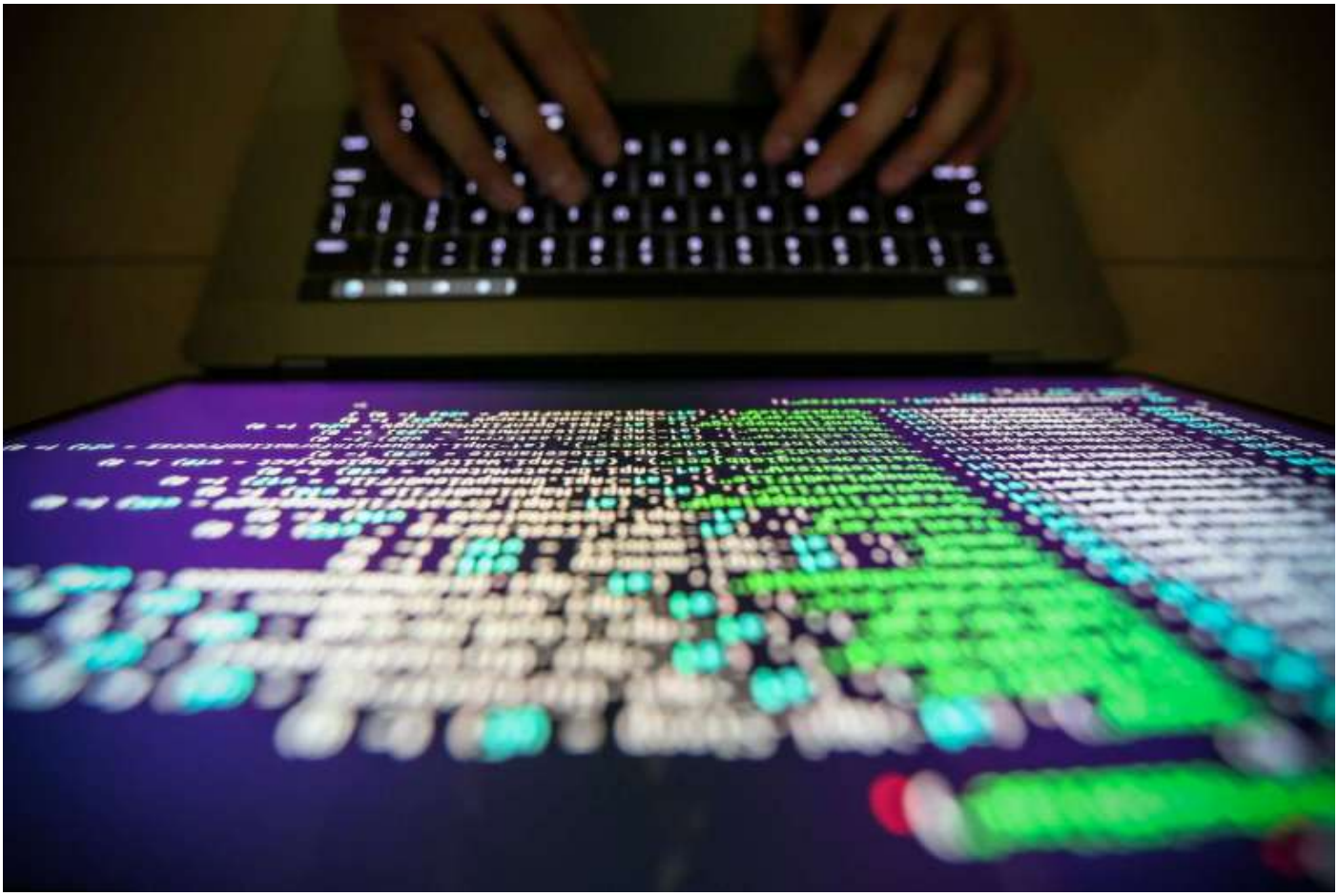
THE STRAITS TIMES

'Unprecedented' cyber attack hits 100 countries



A programer shows a sample of decrypting source code. PHOTO: EPA

PUBLISHED MAY 14, 2017, 5:00 AM SGT

Experts warn of more assaults as firms grapple with worm's impact

FRANKFURT • It may not be over yet, warned security experts, after a devastating cyber attack described as unprecedented in scale caused disruptions in nearly 100 countries from Europe to Asia.

Capitalising on spying tools believed to have been developed by the US National Security Agency (NSA), hackers launched the cyber assault on Friday that infected tens of thousands of computers, with Britain's health system suffering the worst.

Cyber extortionists, using a malicious software called WannaCry, tricked victims into opening attachments to spam e-mails that seemed to contain invoices, job offers, security warnings and other legitimate files. The so-called ransomware encrypted data on infected computers, demanding payments of US$300 to US$600

(S$420 to S$840) to restore access.

Once inside the targeted network, the ransomware made use of recently leaked spy tools to silently infect other out-of-date machines.

This, security experts said, marked a risk of attacks spreading in the coming days and weeks.

Yesterday, finance chiefs from the Group of Seven nations meeting in Bari, Italy, vowed to join forces to fight the growing threat of international cyber attacks.

The ministers said in a statement that cyber incidents represent a growing threat to their economies and that tackling them should be a priority.

In Singapore, the Cyber Security Agency (CSA) yesterday said no government agencies or critical information infrastructure had been affected. The attack took place on the same day that the CSA said hackers had tried to steal data from the networks of the National University of Singapore and Nanyang Technological University.

Europol's European Cybercrime Centre said it was working closely with country investigators and private security firms to combat the threat and help victims. "The recent attack is at an unprecedented level and will require a complex international investigation to identify the culprits," it said.

Researchers with security software maker Avast said they had observed 126,534 ransomware infections in 99 places, with Russia, Ukraine and Taiwan the top targets.

Among those affected were French automotive giant Renault, which was forced to halt production at sites in France and its factories in Slovenia and Romania as part of measures to stop the spread of the virus.

Germany's Deutsche Bahn national railway operator's information screens and ticket machines were hit. Travellers tweeted pictures of hijacked departure boards showing the ransom demand instead of train times. But the company insisted that trains were running as normal.

Several medical facilities in Britain were forced to cancel or delay treatment for patients, but Interior Minister Amber Rudd said the system has almost fully recovered from the disruption as of yesterday.

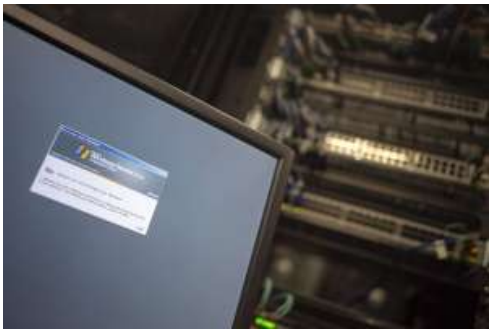
Despite the scale of the attack, experts working with investigators told The Guardian that the hackers appear to have raised just US$20,000.

The hackers, who have not come forward to claim responsibility or been identified, took advantage of a worm, or self-spreading malware, by exploiting a piece of NSA spy code known as "Eternal Blue" that was released last month by a group known as the Shadow Brokers, according to researchers with several private cyber security firms.

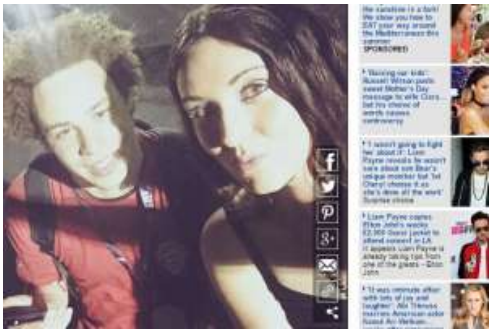
Researchers said the worm deployed in the latest attack, or a similar tool released by Shadow Brokers, is likely to be used for fresh assaults not just with ransomware but other malware to break into firms, seize control of networks and steal data.

REUTERS, AGENCE FRANCE-PRESSE

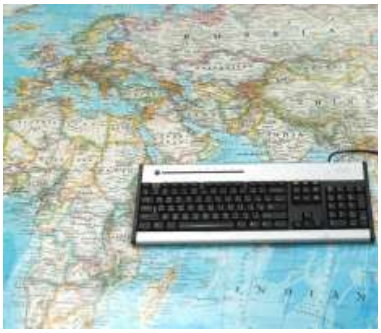
RELATED STORIES:



Cyber attack hits 200,000 in at least 150 countries: Europol chief



Self-taught accidental hero halts global ransomware attack but warns 'this is not over'



Businesses brace for Monday as ransomware threat lingers