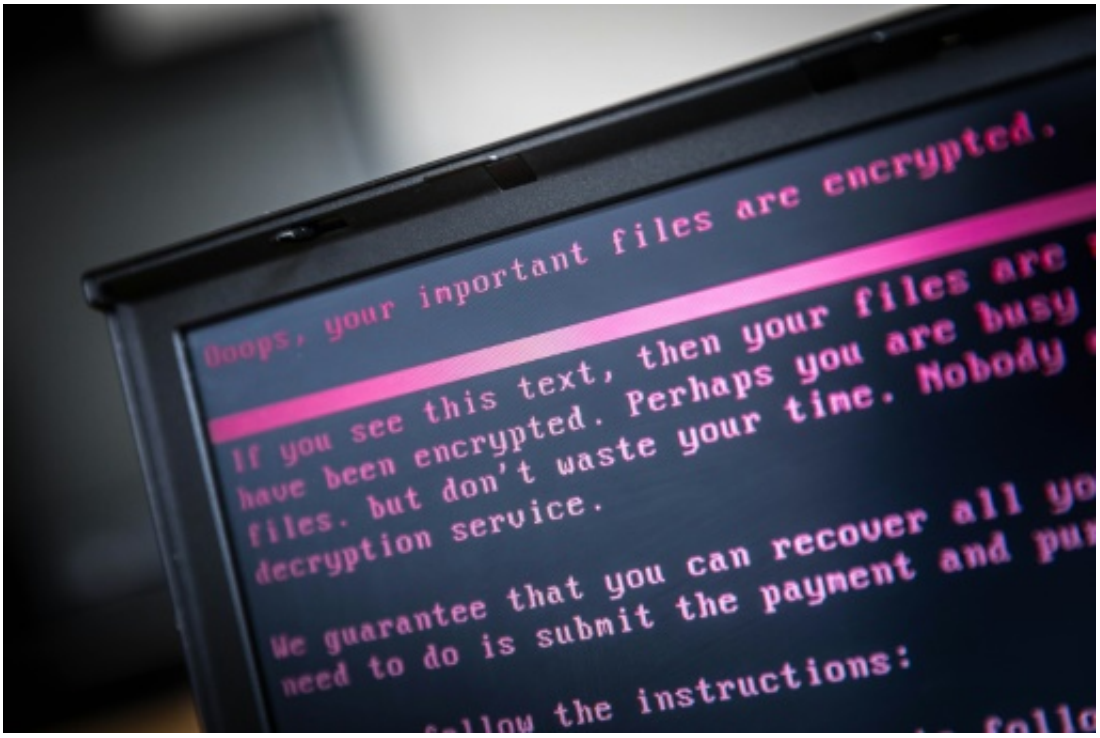
Firms scramble to recover from wave of cyberattacks

June 28 2017, by Dmytro Gorshkov With Max Delany In Moscow And Afp Bureaus



A laptop displays a message demanding payment for unlocking files encrypted by the ransomware attack that spread from Ukraine and Russia

Thousands of computer users across the globe scrambled on Wednesday to reboot after a wave of ransomware cyberattacks spread from Ukraine and Russia across Europe to the United States.

The virus, which locked up files at companies and government agencies including the Chernobyl nuclear site and demanded a payment worth $300, appeared similar to the WannaCry ransomware that swept the world last month, hitting more than 200,000 users in more than 150 countries.

But the new attack appeared much smaller in scale, with global cybersecurity firm Kaspersky Lab estimating the number of victims at 2,000. There was no immediate indication of who was responsible.

Some IT specialists identified the newcomer as "Petrwrap", a modified version of ransomware called Petya which circulated last year. But Kaspersky described it as a new form of ransomware.

In Ukraine, which first reported issues and appeared most heavily hit, companies and critical infrastructure operators were still struggling to cope with the virus.

Employees at the Chernobyl nuclear site were continuing to use hand-held Geiger counters to measure the levels of radiation after the monitoring system was shut down by the hack.

Online arrivals and departures information for Kiev's main Boryspil airport remained down, but its director said the hub was otherwise operating as normal.

Meanwhile, delivery service Nova Poshta said it was still facing problems with accepting payments by card and the Kyivenergo energy supplier said customers were having issues accessing accounts.

Global spread

The attacks started Tuesday at around 2:00 pm Kiev time (1100 GMT)

and quickly spread to 80 companies in Ukraine and Russia, said cybersecurity company Group IB.

In Russia, major companies including the oil giant Rosneft said that they had suffered cyberattacks at roughly the same time.

Later, multinationals in Western Europe and the United States reported that they too had been hit by the virus.

Among the companies reporting problems were global shipping firm Maersk, British advertising giant WPP, French industrial group Saint-Gobain and US pharmaceutical group Merck.

India's government on Wednesday said operations at a terminal at the country's largest container port in Mumbai, run by Maersk, were disrupted.

Windows vulnerability

Security specialists said the cyberattacks on Tuesday exploited an already patched vulnerability in Windows software and appeared to have focused on Ukraine as a primary target.

The malware that, once in a computer, locked away data from users who were then told to pay, bore resemblances to the recent WannaCry attack. US software titan Microsoft also called the latest virus ransomware.

"Our initial analysis found that the ransomware uses multiple techniques to spread, including one which was addressed by a security update previously provided for all platforms from Windows XP to Windows 10 (MS17-010)," a Microsoft spokesperson told AFP.

After the WannaCry scourge in May, Microsoft urged users to protect

machines with the MS17-010 patch.

The flaw—and the means to exploit it—had previously been disclosed in pirated documents about cyberweapons at the US National Security Agency.

So far there was no clear indication of who was behind the attack.

Some experts said it looked likely to be a criminal scam, while Ukraine suggested that its archrival Russia could have been behind the attack.