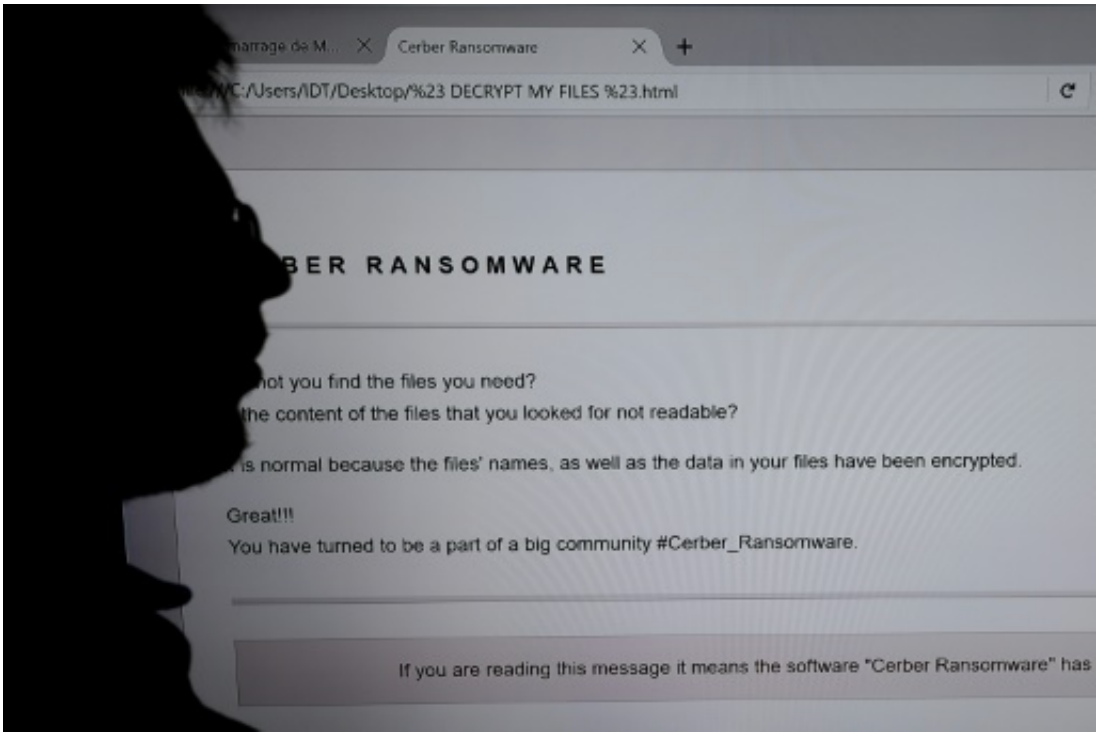
Ransomware, the weapon wielded in cyber attacks

June 27 2017, by Valentin Bontemps



Ransomware, which is a type of virus that locks computer files until the user pays a virtual fee to regain access to the data, has been used in the latest wave of international cyberattacks

Ransomware demands which hit a clutch of multinationals Tuesday are the latest in a wave of international cyberattacks in recent months.

In Europe, Danish sea transport company Maersk, British advertising

giant WPP and French industrial group Saint-Gobain all came under attack as did US pharmaceutical group Merck.

The attacking tool is believed to be ransomware of the so-called Petya malware type, which earlier affected firms in Russia including oil giant Rosneft and Ukraine.

The latest wave comes just six weeks after what the EU's law enforcement agency described as an "unprecedented" attack by WannaCry ransomware which hit more than 100 countries—notably Britain's National Health Service.

The repeated waves of attacks have raised questions on how companies can protect themselves effectively.

What is ransomware?

Ransomware is malicious software which locks computer files and forces users to pay the attackers a designated sum in the virtual Bitcoin currency to regain access to the files.

Ransomware is used on PCs as well as tablets and smartphones. It can affect "at the same time individuals, businesses and institutions," Amar Zendik, CEO security firm Mind Technologies, told AFP.

How does it work?

Cyberpirates generally take control of computers by exploiting flaws in the internet.

That could happen when a user logs onto a web site that has been previously infected or opens an email that invites the user to click on a link or download an attachment.

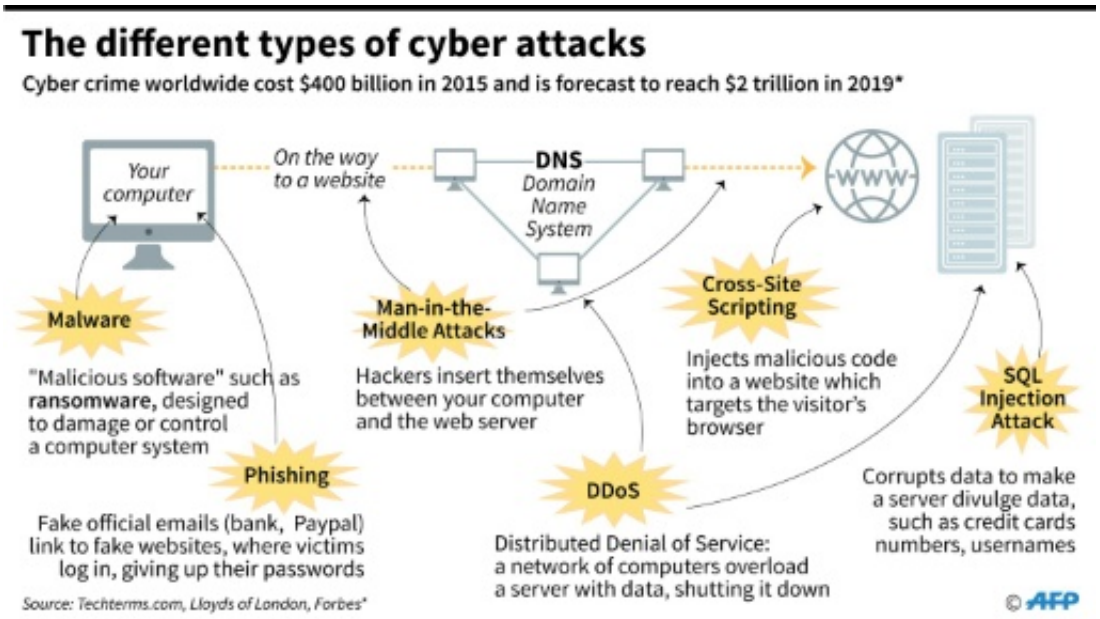
In a few seconds, the malware can be implanted. And when it's installed, "it can't be detected," Laurent Marechal, a cyber security expert at McAfee, told AFP.

It's only afterwards that it "downloads the 'payload', that is the viral charge," he said.

From then on the computer work station is blocked. "Most often the user has to send an SMS"—and pay up—"in order to get the unblocking code," says Marechal, adding that in certain complex cases, the virus can spread "without any human intervention".

Is it used frequently?

Yes. And ransomware continues to multiply. According to security software Kapersky Lab, 62 new types of ransomware were identified last year.



The different types of cyberattacks that could take place

And the US computer security software company McAfee said the number of "samples" detected increased by 88 percent in 2016, totalling some four million.

"Often the pirates ask for small sums of money. But accumulated, these small amounts add up to big money," says cyber security expert Zendik.

"This is a bit like a flu epidemic in winter," said Nicolas Duvinage, head of the French military's digital crime unit, on Tuesday.

"We will get many of these viral attack waves in coming months," he told AFP.

System flaw

The culprits behind the cyberattacks in May apparently took advantage of a flaw in the Windows operating system, divulged in documents leaked from the US National Security Agency (NSA), according to initial findings.

Zendik said the attack was based on a previously unknown Windows flaw.

"We're not talking about classic 'ransomware' which generally targets individuals and small businesses," he said.

"Here the hackers attacked big institutions, not likely to be susceptible to paying, especially given the publicity about the operation."

He added that "in theory, the authors of the attack did not want to make money, but rather to achieve a (cyber) coup."

How to protect oneself

Several simple rules can be followed to reduce the risks of a ransomware attack.

Among them are regularly updating security software which can correct any flaws exploited by the virus.

In case of a cyberattack, the authorities advise disconnecting the infected equipment immediately from the network.

In the case of a virus affecting a business or an institution, the IT experts should be alerted right away.

Authorities also recommend not paying the hackers the ransom demanded—because it's no guarantee that access to the data will be restored.