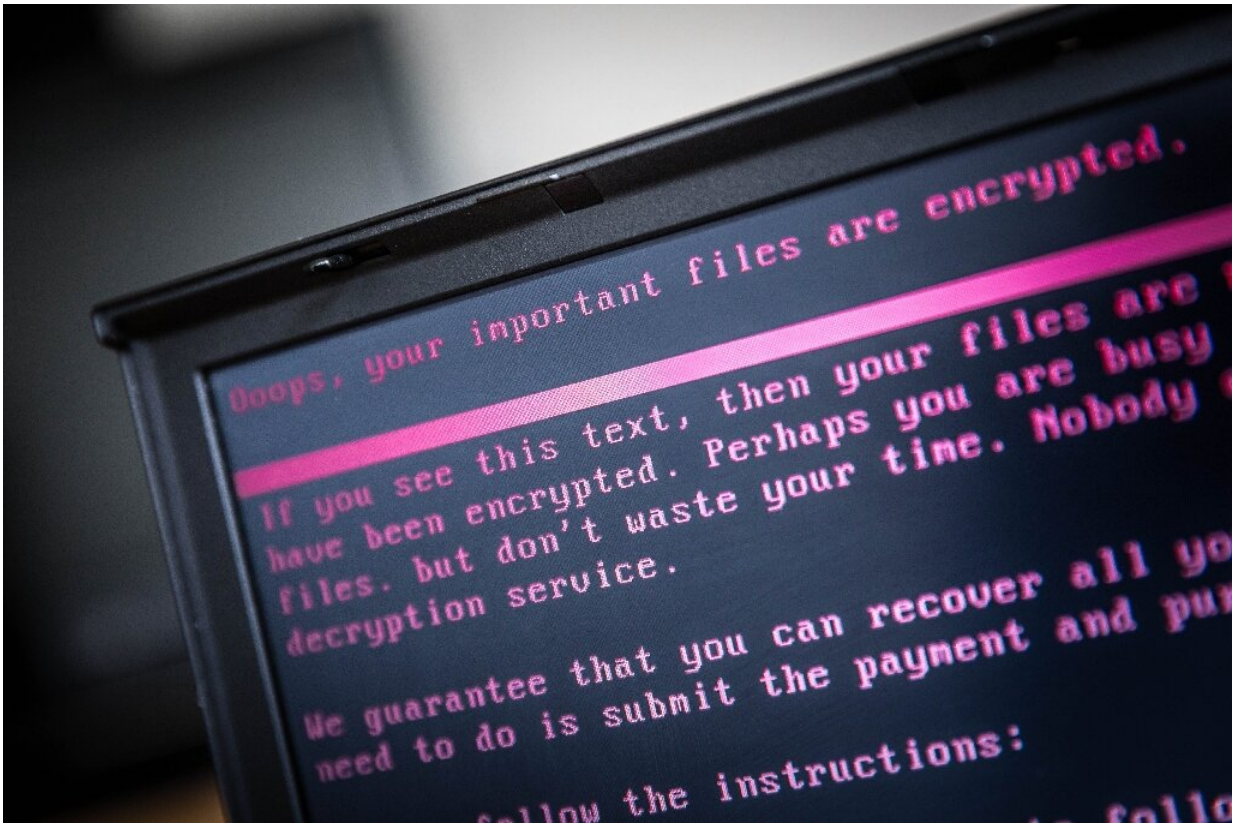
Ransomware attacks 'getting bolder': Europol

October 9 2019



Ransomware attacks have become more targeted, eaccording to Europol

Global ransomware attacks are on the decline, but such malicious cyber strikes are getting bolder and homing in on more profitable companies, with data encryption a key target, Europe's police agency said

Wednesday,.

Europol said it was also concerned by the rise of so-called "self-generated explicit material" produced by underaged children who then share sexual images and videos with peers through smartphones, making themselves vulnerable to sexual offenders.

Police and the private sector "confirm a diminishing number of ransomware attacks targeting individual citizens" but such attacks are "becoming more bold", the agency said as it released its latest annual report on internet organised crime.

Ransomware is a type of software, used by cybercriminals to extort money from internet users.

One of the most visible ransomware attacks happened in March last year when SamSam malware paralysed the southeastern US city of Atlanta for six days.

Although the attackers asked for a ransom of roughly $50,000 (45.000 euros) it cost the City of Atlanta more than $2.6 million to respond to the attack, according to science and technology publication Wired Magazine.

The US Justice Department later charged two Iranian hackers for deploying the ransomware into the systems of more than 200 institutions across the US and Canada, encrypting their operations and making them inaccessible until the owners paid ransoms in bitcoin.

"This only proved to be the tip of the iceberg," Europol said. "There are cases where a company's encrypted files have been ransomed for over one million euros," the agency said.

Globally losses from ransomware rose by 60 percent last year to $8 billion, according to data compiled by the Internet Society's Online Trust Alliance.

Ransomware "has become more targeted because it's like any business model," Interpol's cybercrime directorate chief Craig Jones said.

Criminals. like businessmen "look to see where they can make the most money, where the sweet spot is," Jones told AFP on the sidelines of a combined cybercrime conference organised by Europol and Interpol in The Hague.

Data destruction

Company data remains a key target, Europol said, not only for conventional ransomware attacks, but also sabotage.

These attacks which permanently erase or irreversibly damage company data doubled during the first six months of 2019 with half focusing on the manufacturing sector, Europol said.

This included a new strain of malware called GermanWiper "which rather than encrypting the victim's files, rewrites the content resulting in the permanent destruction of the victim's data."

The agency's Internet Organised Crime Threat Assessment report also highlighted online child sexual exploitation as an ongoing major concern—with children themselves contributing to the problem, helped by greater access to smartphones.

"Self-generated explicit material has been a growing concern for several years, as more-and-more young children share explicit material online," Europol said.

"Kids these days have access to smartphones and other devices that can take high-resolution images, they are present on different social media platforms, so it's easy," said Philipp Amann, strategic head at Europol's EC3 cybercrime centre.

"Looking at the law, for instance even if a 14-year-old receives a (explicit) picture of his 13-year-old girlfriend that could still legally be considered child abuse material," he told AFP.