Explainer: What is ransomware?

May 13 2017, by Michael Balsamo

A security camera stands outside the main Telefonica headquarters in Madrid, Spain, Friday, May 12, 2017. The Spanish government said several companies including Telefonica had been targeted in ransomware cyberattack that affected the Windows operating system of employees' computers. It said the attacks were carried out with a version of WannaCry ransomware that encrypted files and prompted a demand for money transfers to free up the system. (AP Photo/Paul White)

Computers across the world were locked up Friday and users' files held for ransom when dozens of countries were hit in a cyber-extortion attack

that targeted hospitals, companies and government agencies.

Here's a look at how malware and ransomware work and what people can do if they fall victim to attacks.

WHAT IS MALWARE AND RANSOMWARE?

Malware is a general term that refers to software that's harmful to your computer, said John Villasenor, a professor at the University of California, Los Angeles. Ransomware is a type of malware that essentially takes over a computer and prevents users from accessing data on the computer until a ransom is paid, he said.

HOW DOES YOUR COMPUTER BECOME INFECTED WITH RANSOMWARE?

In most cases, the software infects computers through links or attachments in malicious messages known as phishing emails.

"The age-old advice is to never click on a link in an email," said Jerome Segura, a senior malware intelligence researcher at Malwarebytes, a San Jose-based company that has released anti-ransomware software. "The idea is to try to trick the victim into running a malicious piece of code."

The software is usually hidden within links or attachments in emails. Once the user clicks on the link or opens the document, their computer is infected and the software takes over.

BUT HOW DOES IT WORK?

"Ransomware, like the name suggests, is when your files are held for ransom," said Peter Reiher, an adjunct professor at UCLA who specializes in computer science and cybersecurity. "It finds all of your

files and encrypts them and then leaves you a message. If you want to decrypt them, you have to pay."

A security guard stands outside the Telefonica headquarters in Madrid, Spain, Friday, May 12, 2017. The Spanish government said several companies including Telefonica had been targeted in ransomware cyberattack that affected the Windows operating system of employees' computers. (AP Photo/Paul White)

The ransomware encrypts data on the computer using an encryption key that only the attacker knows. If the ransom isn't paid, the data is often lost forever.

When the ransomware takes over a computer, the attackers are pretty explicit in their demands, Segura said. In most cases, they change the wallpaper of the computer and give specific instructions telling the user

how to pay to recover their files. Most attackers demand between $300 and $500 to remove the malicious ransomware; the price can double if the amount isn't paid within 24 hours.

Law enforcement officials have discouraged people from paying these ransoms.

HOW CAN PEOPLE PREVENT ATTACKS LIKE THIS?

The first step is being cautious, experts say. But Villasenor said there is "no perfect solution" to the problem.

Users should regularly back up their data and ensure that security updates are installed on your computer as soon as they are released. Up-to-date backups make it possible to restore files without paying a ransom.

Friday's attack exploited vulnerabilities in some versions of Microsoft Windows. Microsoft has released software patches for the security holes, although not everyone has installed those updates.

"If your software is not patched, you can exploit that user. Anyone who applied the patch that Microsoft released likely wasn't affected by this," Reiher said.

Users should also look for malicious email messages that often masquerade as emails from companies or people you regularly interact with online. It's important to avoid clicking on links or opening attachments in those messages, since they could unleash malware, Villasenor said.