The computer virus that blackmails you

Out of media player. Press enter to return or tab to continue.

Media captionWhat is ransomware?

Ransomware is the fastest growing form of computer malware, experts warn.

It's a malicious virus that locks the user out of their computer and demands a fee to return their files.

A report published by the Australian government claims 72% of businesses surveyed experienced ransomware incidents in 2015.

The figure was just 17% in 2013 .

It's also a growing threat for mobile devices as it can be hidden in an app, says Gert-Jan Schenk, vice-president at internet security company Lookout.

"For the most part, we've seen ransomware delivered through drive-by downloads – it pretends to be a popular app, increasing the chances that you'll click on it," he explains.

"To avoid these threats, users should be very careful about what apps they install, and where they come from – read the reviews on Google Play, and avoid side-loading from untrusted sources."

How does it work?

Like most computer viruses, ransomware often arrives in the form of a phishing email, or spam, or a fake software update – and the recipient clicks a link or opens an attachment.

The virus then sets to work encrypting the user's files.

Once the computer is effectively locked down, it demands a fee – often in bitcoins because it is less easy to trace – for the return of the files.

The fee is generally one or two bitcoins – the equivalent of about $500 (£330).

It is less common now, but in the earlier days of the malware – about five years ago – the ransom note could take the form of a law enforcement notice.

The user was directed to a web page that appeared to be from, for example, the FBI, falsely claiming illegal images of children had been been found on the machine and a fine was payable.

There is generally a time limit to comply, after which the ransom increases.

Is there any way to get round it?

Sometimes it is just a threat, but mostly the virus really does encrypt files.

The only way to retrieve your files without paying the ransom is to go to a backed-up version.

Neil Douglas, from Edinburgh-based IT company Network Roi, has just helped a small business client whose server was hit by ransomware.

“We had to recover everything from back-up. We’d had a back-up two minutes before the infection, so the timing couldn’t have been any better – but it did result in quite a bit of downtime,” he says.

“You could risk paying them – but it’s a bit like paying a blackmailer. We would only recommend it as a last resort.

“You don’t know whether they’ll come back for more, you don’t know that they’ll clear the infection.”

Cybersecurity expert Prof Alan Woodward says paying also leaves you vulnerable to further cybercrime.

“As soon as you pay up, you get on a suckers’ list and you’ll probably get contacted again,” he says.

“It’s low-hanging fruit for the criminals.”

Do many people pay?

While all the expert advice is, of course, not to pay, plenty of people do – even those you would least expect to.

Tewksbury Police, in the US, admitted they had paid up when their main server had been attacked and locked down at the end of last year.

“Nobody wants to negotiate with terrorists. Nobody wants to pay terrorists,” Police Chief Timothy Sheehan told the town’s local paper.

“We did everything we possibly could.

“It was an eye-opening experience, I can tell you right now. It made you feel that you lost control of everything.

“Paying the bitcoin ransom was the last resort.”

Ransomware is lucrative for criminals because so many victims pay rather than face the shame of false accusations – or like the police department, they just desperately need their files.

“Some companies have set up bitcoin accounts in case it happens to them,” says Prof Woodward.

“I would recommend that nobody ever pays up.

“The only way to deal with it is to be sure you have a virus checker and back up.”

Who is behind it?

“It tends to be organised crime,” says Prof Woodward.

“They do make millions out of it. It’s opportunistic… they just try it on everybody. You keep third parties out of it – the bank isn’t involved.”

Recent research by Palo Alto Networks and industry partners suggested one family of ransomware known as Crypto Wall had generated about $325m (£215m) for the gang behind it.

“In the volume cybercrime space, ransomware is one of the most prolific problems we face,” Greg Day, chief security officer for Europe at Palo Alto Networks, told the BBC last month.

“Credit card theft is getting to the point where the value of each card is very low. As a result, ransomware has stepped into that gap and gives a higher value for each victim.”

News Source