THE CONVERSATION
Academic rigour, journalistic flair

How WannaCry caused global panic but failed to turn much of a profit

May 18, 2017 10.11am BST

No money, no access. shutterstock.com

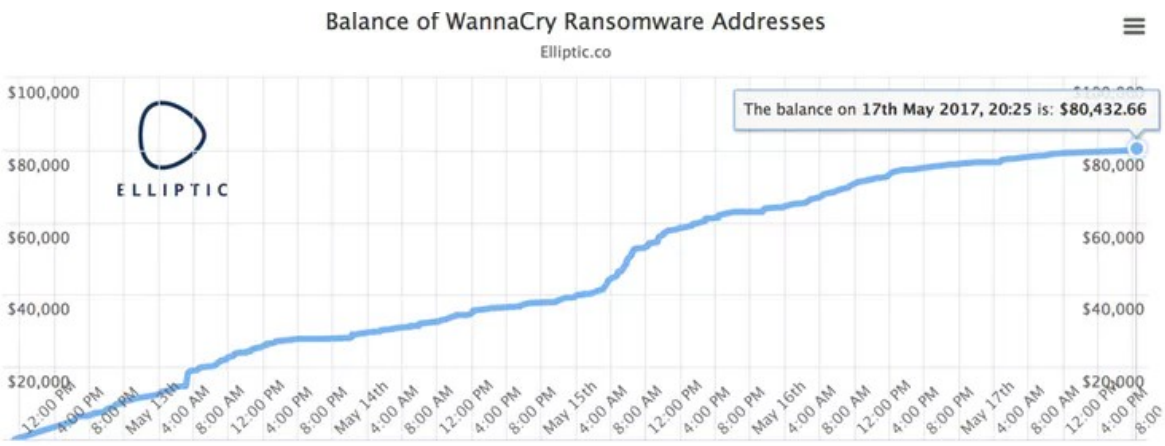
Author

Bill Buchanan
Head, The Cyber Academy, Edinburgh
Napier University

The WannaCry cyber-attack led to panic across the globe, showing just how important it is for organisations to have secure operating systems. This was not even the most sophisticated malware around. Numerous networks could easily cope with it and it largely hit legacy operating systems such as Windows XP.

In most corporate infrastructures, there would be no sign of Windows XP – and it seems unbelievable from a security perspective that the national health service of an advanced economy such as the UK would run its critical infrastructure on such an unsafe, antiquated system.

But perhaps the most striking aspect of this recent attack is how unsuccessful it has been in terms of generating a ransom. As well as the NHS in the UK, it hit French car manufacturer Renault, US delivery service FedEx, Russia's interior ministry and Spanish telecoms and gas companies. Yet ransom payments currently appear to total less than US$100,000.



The chart shows the current balance of the three Bitcoin addresses known to be associated with the WannaCry ransomware. Elliptic

This is minuscule when we compare it to other ransomware attacks. CryptoWall made its author US$325m with over 406,000 attempted infections.

The interesting thing about the WannaCry ransomware is that it mostly hit large organisations with legacy networks – and they will often not pay ransoms as they have backups or run their data from a central server. Thus, despite more than 200,000 infections worldwide, there have been fewer than 200 payments.

The weak impact is because this is a different type of ransomware. The most successful ones spread through spear phishing emails and target individuals and small businesses, which often do not have back-ups. This ransomware was different in that it spread of its own accord through unpatched systems (systems that had not followed recent warnings to protect against a virus and back-up their files) – as a worm. But it is humans that are generally the weakest link when it comes to information security.

The perfect crime?

Ransomware is almost the perfect IT crime. If an online criminal can trick you into installing malware, they can then lock your files and hold them ransom until you pay them a release fee. Only a secret encryption key, which they hold, can release the files.

It is simple, but highly effective. No virus scanner or law enforcement professional will be able to unlock your files unless they have the magic encryption key, and the longer the target takes to pay for it, the greater the risk there is to their business. As with any malware, though, there might be bugs in the software, so there's no guarantee that you'll get your files back, even if you do as the blackmailers say. And there's always the risk that they will just ask for more money once you pay them. Some malware increases its ransom demands over time, ultimately deleting all the files affected.

Nonetheless, it means that the success rate of the crime is incredibly high – at around 65%, as sensitive and important documents are often the target of the infection.

Success rate for ransomware. Trent Micro - New Research: Uncovering the Truth About Ransomware

Increasing infections

Computer security firm Trend Micro surveyed over 300 IT decision makers in the UK in September 2016 and found that 44% of businesses have been affected by ransomware over the last two years. The same survey found 79 new types of ransomware in the first nine months of that year. This compared to just 29 in the whole of 2015.

This is a great worry for many companies. The impact on those affected by the infection can be costly, with an average of 33 person hours taken to fix it.

In around 20% of the cases, £1,000 was requested, with an overall average of £540. Some large organisations faced demands of as much as £1m. But for many companies, this is the tip of the iceberg as it can be costly for a company in terms of reputation as customers could start seeing them as untrustworthy.

Perhaps the most frightening statistic that Trend Micro found was that in one in five cases, even when the company paid the ransom, they were unable to recover their important files – indicating that the ransomware service is not quite as robust as it should be.

If you ask many security professionals, the recent WannaCry ransomware was fairly easy to defend against, and was fairly unsophisticated. What it clearly shows is that there is still more success in tricking individuals than in spreading malware across large networks. The NHS does, though, need to make sure that not one unpatched computer ever goes near its network, and that employees understand that they shouldn't click on suspicious links.

Meanwhile, with law enforcement agencies focused on the three Bitcoin wallets associated with

WannaCry to try and find out who profits, there will be a whole lot more ransomware that goes unreported and unnoticed.

Cybersecurity **Digital economy** **Information technology** **NHS** **Ransomware** **WannaCry**