NotPetya is something a little different. EPA/ROB ENGELAAR

The WannaCry ransomware was barely out of the headlines when another cyberattack took down computer systems around the world.

This time, a piece of malware dubbed “NotPetya” is to blame. And unlike WannaCry, it has no clear “ kill switch ” as it spreads across infected networks.

NotPetya has reportedly hit several global organisations so far, including the American pharmaceutical company Merck and, in Australia, Cadbury .

The attack was initially classed as ransomware: malicious software that holds a user to ransom by encrypting their files and blocking access without a “key”. It was a reasonable assumption given the threatening message displayed to victims – but the picture is more complicated.

NotPetya is distinct from WannaCry in a number of important ways – particularly, money doesn’t seem to be its end goal.

1. It’s about disruption not profit

Unlike other ransomware incidents, NotPetya seems to be aimed at disruption rather than criminal profiteering (or perhaps just bad design).

First, the amount requested by the ransomers is relatively small – only US$300. This seems to place a low value on the loss of access that the malware causes.

Secondly, infected machines direct the user to make payment to one Bitcoin account. Users are

also referred to a single email address to obtain the keys necessary to decrypt their data. Unfortunately, many users have now discovered that the email account has been closed by Posteo, the email provider.

This means that, even having made payment for the ransom, end users are unable to recover their data. Locking yourself out from your victims with a fixed address in this manner just doesn't make good business sense.

This points either to amateurish implementation, or to the fact that NotPetya may have another purpose.

Some reports suggest the ransom demands may be a media lure to maximise public attention, while other researchers question whether recovery of encrypted data was ever possible .

In some circles, this attack has been classified as a "wiper" (in which data or even entire disks are deleted or modified beyond repair), but this is still to be firmly determined.

Whatever the case, if the perpetrators wanted to make money they have gone about it all wrong.

2. Ukraine seems to be the centre of the damage

Unlike WannaCry, which made headlines after it shut down the computer systems of British hospitals among other organisations, the largest number of NotPetya incidents have been reported in Ukraine.

The malware uses an "exploit" – a tool that can take advantage of a specific vulnerability on a computer – to remotely execute code on vulnerable Windows operating systems. This vulnerability, called MS17-010 , was patched by Microsoft in March. The instances of compromised systems suggests that many organisations and individuals have failed to install the patch.

One possible explanation for high levels of non-patched systems could be the prevalence of pirated software in Ukraine.

Another distribution mechanism used by the malware appears to be a software updater linked to the Ukrainian tax accounting software, M.E.Doc.

While there is no clear evidence pointing to the perpetrators of this attack, its motivations could be political. Unlike WannaCry, NotPetya is seriously disrupting businesses rather than making money, or else is masking its other intentions.

3. It may not even be ransomware

While NotPetya uses an edited version of the same EternalBlue software exploit as the WannaCry ransomware to remotely run code on the victim's Windows computer, it differs in many key ways.

Whereas WannaCry only encrypted certain files (typically users' most important data), NotPetya also prevents access to the entire operating system. It does this by writing over key parts of the hard disk as well as encrypting users’ files .

Traditional encryption ransomware typically has a key available to recover your files. With NotPetya, there is no key to facilitate recovery (despite the promises shown on screen). There is evidence that the allegedly unique ID shown to the victim is actually random data that could never result in a decryption key being provided.

While it is still too early to provide a definitive analysis of this cyberattack, it is clear this is a new twist in online warfare.

The code has been carefully designed to take advantage of vulnerable systems while the user

is duped into believing that it's possible to recover their files. The ransomware distraction may have been a careful misdirection to hide the true intentions of the mayhem.

We can expect this trend to continue and that organisations (and individuals) need to be more proactive in keeping their operating systems up to date and their data backed up.

Paul Haskell-Dowland is affiliated with the International Federation for Information Processing (IFIP) Technical Committee 11 and is a member of the ACS and BCS.

Authors: Paul Haskell-Dowland, Associate Dean (Computing and Security), Edith Cowan University

Read more http://theconversation.com/three-ways-the-notpetya-cyberattack-is-more-complex-than-wannacry-80266