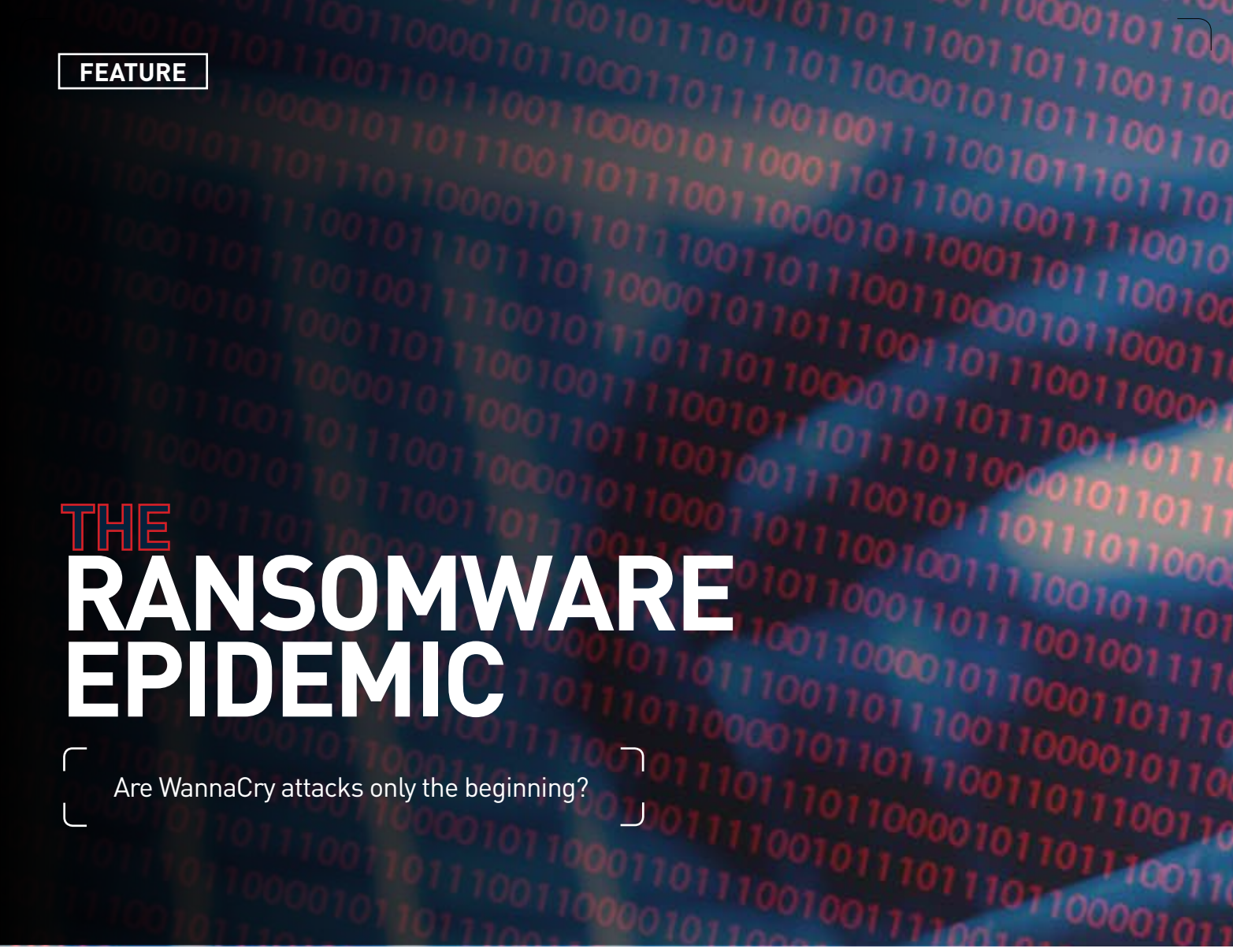

THE RANSOMWARE EPIDEMIC

Are WannaCry attacks only the beginning?

Thousands of organisations from around the world were caught off guard by the WannaCry ransomware attack launched last month. As this rapidly spreading threat evolves, more cybercriminals are likely to attempt to profit from this and similar vulnerabilities.

As a ransomware programme, WannaCry itself is not that special or sophisticated. In fact, an earlier version of the program was distributed in March and April and, judging by its implementation, its creators are not very skilled.

The difference between the earlier WannaCry attacks and the latest one is a worm-like component that infects other computers by exploiting a critical remote code execution vulnerability in the Windows implementation of the Server Message Block 1.0 (SMBv1) protocol.

Microsoft released a patch for this vulnerability in March and, on the heels of the attack on 12th May, even took the unusual step of releasing fixes for older versions of Windows that are no longer supported, such as Windows XP, Windows Server 2013, and Windows 8.

The WannaCry attackers didn't put in a lot of work to build the SMB-based infection component either, as they simply adapted an existing exploit leaked in April by a group called the Shadow Brokers. The exploit, codenamed EternalBlue, is alleged to have been part of the arsenal of the Equation, a cyberespionage group widely believed to be a team linked to the US National Security Agency.

The version of WannaCry that spread through EternalBlue had a quirk: It tried to contact an unregistered domain and halted its execution when it could reach it, stopping the infection. A researcher who uses the online alias MalwareTech quickly realised that this could be used as a kill switch and registered the domain himself to slow down the spread of the ransomware.

Since then researchers have discovered a couple more versions: one that tries to contact a different domain name, which researchers have also managed to register, and one that has no apparent kill switch. However, the latter version is non-functional and seems to have been a test by someone who manually patched the binary to remove the kill switch, rather than recompiling it from its original source code. This led

researchers to conclude that it's likely not the work of the original authors.

Separately, experts from the computer support forum BleepingComputer.com have seen four imitations so far. These other programmes are in various stages of development and try to masquerade as WannaCry, even though some of them are not even capable of encrypting files at this point.

This does indicate that attacks, both from the WannaCry authors and other cybercriminals, will likely continue and, despite patches being available, many systems will likely remain vulnerable for some time to come.

After all, security vendors are still seeing successful exploitation attempts today for MS08-067, the Windows vulnerability that allowed the Conficker computer worm to spread nine years ago.

FROM THE EXPERTS

The rapid spread of "WannaCry" Ransomware proved that absence of basic security hygiene can cripple companies. Strengthening systems by installing patches on a timely basis, email filtering, and network segmentation, etc. are some of the minimum security measures any organisations should be putting in place to protect it from both known and unknown attacks.

Sagheer Mufti, COO, ADIB

One of the reasons WannaCry happened to spread so quickly was that it depended less on phishing techniques but more on the Server Message Block (SMB) protocol vulnerability. So essentially, the delivery method was more akin to a worm infection. While patient-zero might have got the virus from a phishing mail, if (s)he was on a network with a widespread SMB vulnerability across systems, the worm took over the distribution of the ransomware. It was brilliant in its sophistication and integration of an exploit, a worm and finally the ransomware.

Yasser Zeineldin, CEO, eHosting DataFort.

Organisations should never conclude that the absence of a major cyber-attack means that they have effective cyber defences. WannaCry and Adylkuzz show how important security patches are in building and maintaining those effective defenses, and why regular patching plans to mitigate environment vulnerabilities need to become a higher priority.

Steve Grobman, CTO, McAfee

Even though the UAE is extremely well-prepared and equipped to deal with large scale attacks, we constantly observe that users are inadequately trained in cybersecurity awareness, which is the only way to protect the organisations against such cyber-attacks

Amir Kolahzadeh, CEO, ITSEC