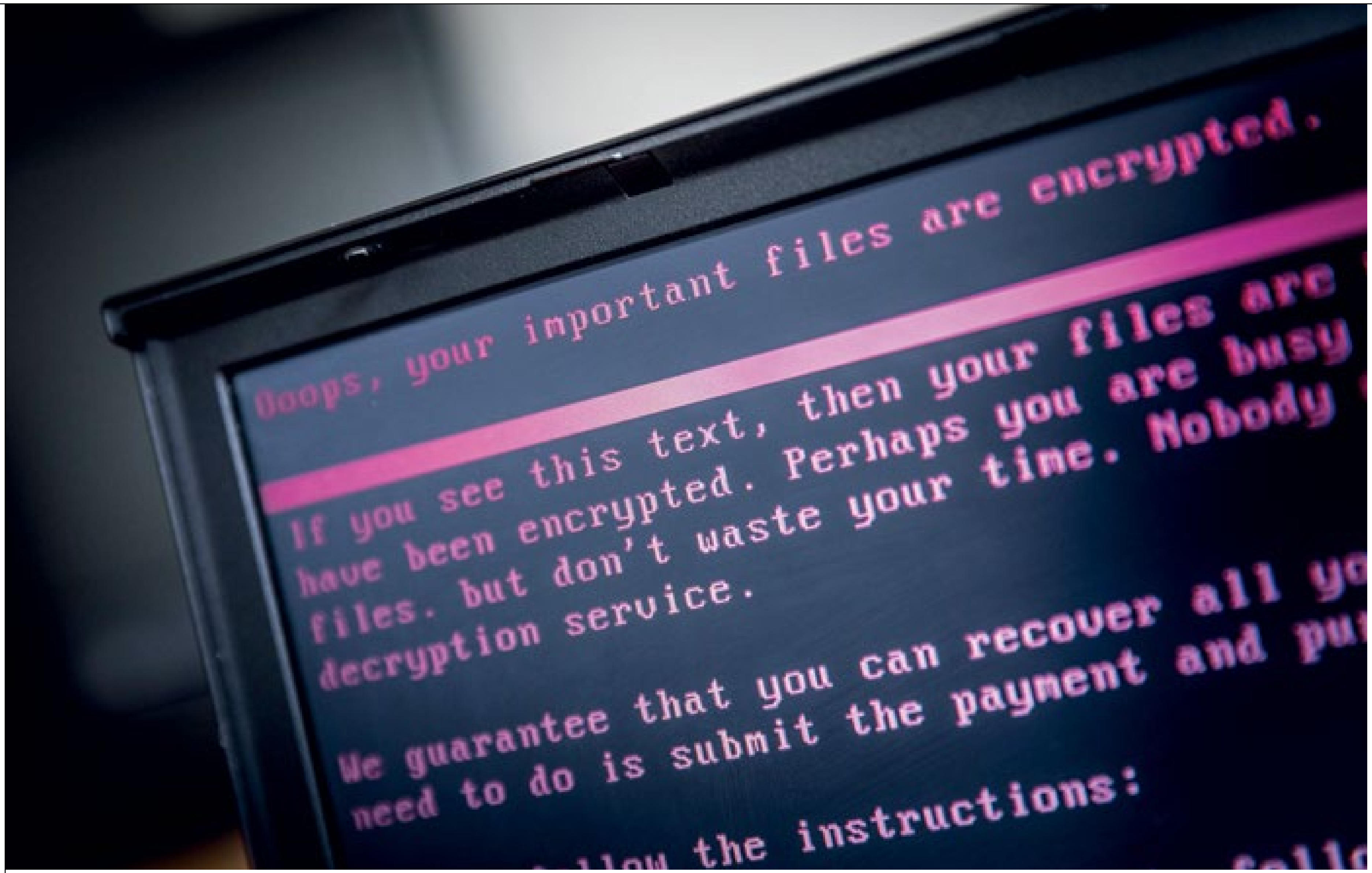


Ooops, your important files are encrypted.

If you see this text, then your files are
have been encrypted. Perhaps you are busy
files, but don't waste your time. Nobody
decryption service.

We guarantee that you can recover all yo
need to do is submit the payment and pu
llow the instructions:
follo

A laptop displays a message after being infected by ransomware

Picture credit: Getty

STAY ONE STEP AHEAD

Marie Clutterbuck *reveals why business is the new target for cyber criminals and explains what can be done to limit the threat*

Ransomware groups like Wannacry, Petya and SamSam dominated headlines back in 2017 as they plagued businesses and consumers alike. Two years later, hackers are now less bothered about developing tools to reach the masses instead focusing more targeted attacks, leading to the overall decrease in detection figures. In fact, according to recent reports, while the overall infection numbers have declined 26 percent, they have increased by 9 percent among businesses. While this is positive news for consumers, the same cannot be said for businesses who are being targeted more than ever by these criminal groups. Experts have further predicted new organisations will fall victim to ransomware every 14 seconds this year, with this trend expected to escalate to every 11 seconds by 2021 highlighting the need for businesses to start preparing for the worst.

While we are all worried about outsiders getting access to our personal data, many groups such as Ryuk explicitly target organisations rather than individuals. This is largely because cyber criminals know that businesses house data that is much more valuable than that of consumers, and that they cannot afford to have their business-critical systems taken offline. Hackers are therefore confident that businesses are likely to have the funds, as well as the pressing need, to pay the ransom and get operations back up and running as quickly as possible. In fact, a report from McAfee and Coveware this year revealed the Ryuk attackers have extorted more than 10 times the average malware ransom, making it the costliest exploit of its nature. This trend is particularly worrying for SMEs, who are the ones predominantly targeted by ransomware attacks yet have significantly fewer resources and systems in place to combat the threat. SMEs have reportedly been the chosen target in 67 percent of the ransomware attacks in 2018, highlighting the pressing need to put appropriate systems in place to protect them from potentially business-halting breaches.

GandCrab, the malware which first surfaced in early 2018 and which within only a year claimed the crown for one of the most destructive cyber infections in the world, appears to this year have stepped up its focus on businesses in particular, in search of bigger paydays. This is anything but surprising in today's climate, as new intelligent methods have led to greater confidence in hackers to get through initial safety walls with ease. It is no longer considered financially worthwhile to randomly scatter the virus around, as one big target can assure a bigger payoff than all of them combined. Out of all the malwares of this kind, GandCrab is seen as particularly dangerous as the technique they use is different from other attacks we've become accustomed to like Wannacry and Ryuk. Rather than demanding one lump sum payment as ransomware for hijacked data, GandCrab sets itself apart by demanding payments on a per-PC basis, which means a large company with hundreds or sometimes thousands of systems could end up costing millions when faced with a ransomware attack using the GandCrab method.

> 34% OF BUSINESSES HIT BY MALWARE TOOK A WEEK OR MORE TO REGAIN ACCESS TO THEIR DATA

Continuous technological advancements have led to the exponential increase in the number of vulnerabilities to IT systems. This coupled with increasingly sophisticated and diverse styles of attacks have made organisations with weak data protection systems extremely exposed to intrusions. Most businesses understandably concentrate on building strong defence systems to prevent cyber attacks from ever happening in the first place. This, however, is not plausible anymore as ransomware attacks targeting businesses are not only increasing in frequency, but are also becoming more sophisticated and better equipped to bypass organisational defences. Assuming that an attack taking place is more likely than not at some point in time, it is worth shifting focus towards building a strategy on how to recover from it – and do so quickly – because the truth is that it isn't really the attack itself that causes the gravest harm to the business, but rather the downtime of operations it leads to. According to recent statistics, 34 percent of businesses hit by malware took a week or more to regain access to their data, which is longer than most SMEs can survive.

BUSINESS CONTINUITY

Being aware of the threat is one thing; acting appropriately is another. Many actors who are both aware and extremely anxious about the looming danger often react the way most of us do – by panicking and blindly backing all available data up in a random order. While this may seem like a reasonable strategy, it is not the most practical one for business continuation. What many do not realise is that recovering files from backups is a laborious, time-consuming process. Seeing that the top priority for organisations following an attack is to recover data quickly to maintain business operations, a recovery strategy needs to be carefully planned, and it needs to be done before an attack has the chance to take place to have any effect.

If you take a moment to think about the vast amount of data your business holds, I'm sure you'll agree that not all of it is equally important for business continuation. To recover from an attack most efficiently, it is essential to firstly know exactly what data is available and what it does. Once the IT infrastructure is understood and the most valuable business critical data has been recognised, a system based on a previously decided upon priority of restoration can be put in place. This system allows for the most critical data to be recovered as a priority as quickly as in minutes if needed, allowing 'the show to go on' while fixing the breach yet still benefitting from the cost efficiencies of slower recovery times for less critical information. This ranking of data is important as, should all defences fail at once, IT security teams will know exactly what data is essential for business operations to continue and, therefore, needs to be restored first.

PLANNING AHEAD

For a recovery system to work, however, it needs to be thoroughly planned, developed and tested ahead of an attack taking place. Which workloads are most important for your business to stay operational? How fast do you need them back? What data can you survive without for a slightly longer period of time? Having the answers to these questions is vital and will effectively be a deciding factor in what will happen to your business in case of a ransomware attack. If a well-planned recovery plan is in place, IT security teams will be able to bring back data within minutes with minimal disruption to operations.

A zero-day recovery architecture is a service that enables administrators to quickly bring back data into operation in the event of an IT outage or cyber attack, without having to worry about whether the workload is still compromised. An evolution of the 3-2-1 backup rule, where three copies of data are stored on two different media and one backup which is kept offsite, zero day recovery enables IT departments to partner with the cyber teams and create a set of policies which define the architecture for what they want to do with data backups being stored offsite, normally in the cloud. This policy assigns an appropriate storage cost and, therefore, recovery time to each workload according to its strategic value to the business. It could, for example, mean that a particular workload needs to be brought back into the system within 20 minutes while another workload can wait a couple of days.

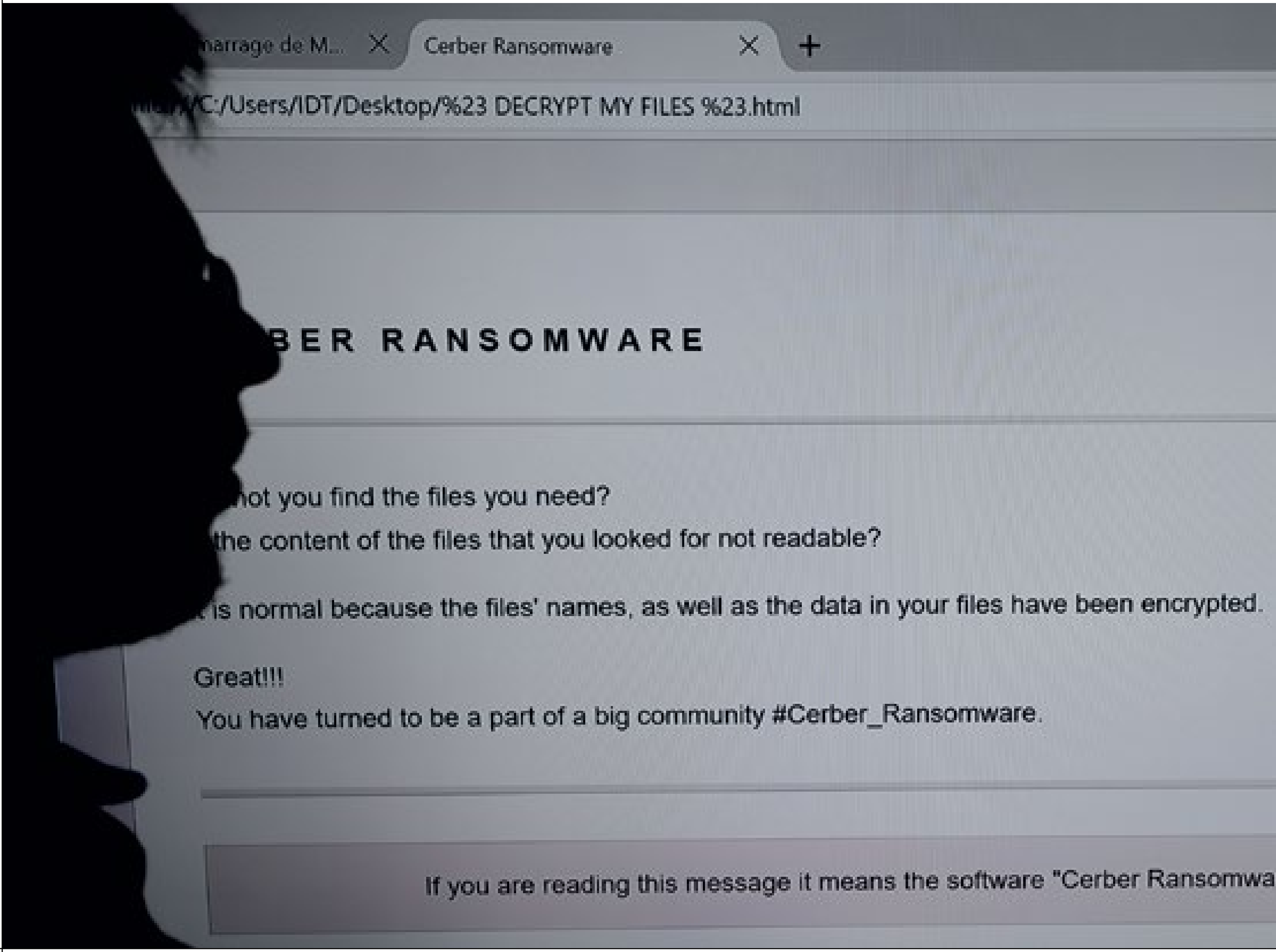
ORGANISING DATA

This system can further optimise storage usage by organising data according to relevance. This cost-effective, automated system will keep the most relevant and recent data at hand as green data for 30 days or so, to then be moved to a lower amber level of the storage system after 45 days and finally archive any files which have been untouched for over 60 days onto tapes or an object file system. Being completely automated, this process saves engineers massive amounts of time and effort, allowing them to direct their efforts elsewhere while being fully confident their data is resting safe and sound on the system. A simple and clear cataloguing scheme will further ensure this data remains accessible at all times, as it will show exactly where specific data is being held and moved to at all times. Categorising in this way also allows IT teams to go back to the owner of a particular workload and let them know exactly how much it costs to run their workload and how much it will cost per month to place that workload as a priority in the restoration process, therefore giving it high survivability. This process could even help save money on storage, ultimately meaning the process pays for itself.

With hackers shifting their focus away from random individual targets towards bigger payoffs offered by corporations, the risk of both financial and operational losses caused by ransomware attacks is bigger than ever. A rapid data restoration system is the difference between a minor inconvenience and complete business paralysis, yet is often overlooked by business managers. By investing in an advanced recovery system, systems and data will be significantly less affected in case of an attack allowing the continuation of business operations with minimal disruption. With zero day recovery, data can be recovered quickly, minimising or even eliminating the damage that a destructive cyber attack would have caused the business ●

> RYUK ATTACKERS HAVE EXTORTED MORE THAN 10 TIMES THE AVERAGE MALWARE RANSOM

Marie Clutterbuck is the CMO of data protection and recovery expert Tectrade, with nearly 20 years of experience in technology and cyber security across both government and commercial organisations.



not you find the files you need?

the content of the files that you looked for not readable?

is normal because the files' names, as well as the data in your files have been encrypted.

Great!!!

You have turned to be a part of a big community #Cerber_Ransomware.

If you are reading this message it means the software "Cerber Ransomwa

An IT researcher stands next to a computer that's been infected by ransomware

Picture credit: Getty