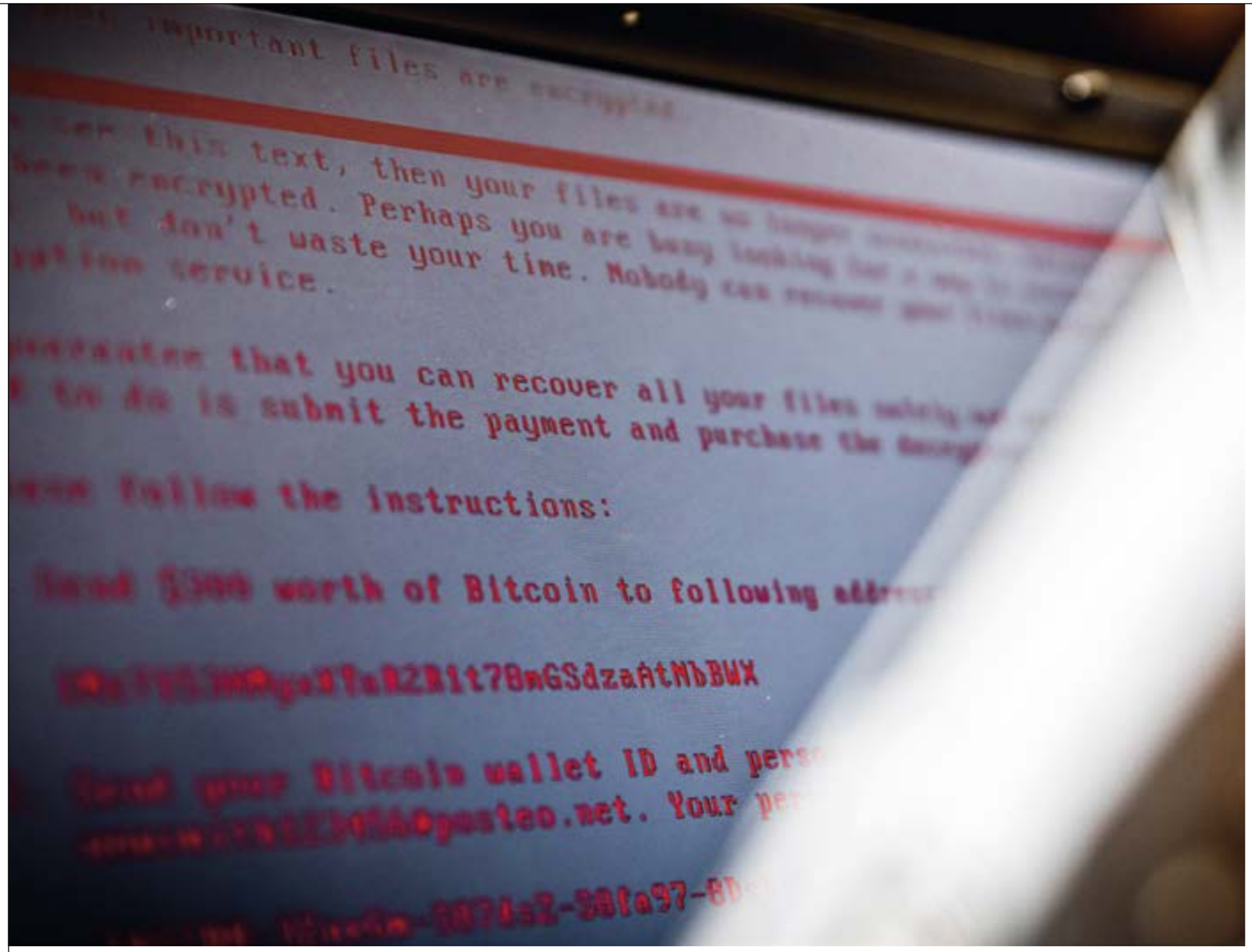

Picture credit: Getty

HELD TO RANSOM

Tony Rowan *uncovers the psychology behind hackers and ransomware*

While ransomware has been around for decades, in 2017 we've seen an unprecedented gear change in terms of the scale, severity and impact to businesses of these attacks. Organisations across the globe are continuing to count the cost of the fall out of May's WannaCry, the largest ransomware attack in history, which was closely followed by NotPetya in June. These consequences are significant with one recent estimate putting the average cost of a single ransomware incident at more than $713,000. It's not only the cost of a ransom payment that organisations can be faced with; the loss of data, extended downtime and disruption to normal business can all have a debilitating impact.

Perhaps more than any other form of cyber attack, there's also a psychological factor at play in ransomware attacks. These are not always the most technically advanced forms of attack, but they are designed, primarily, to elicit a response from victims. As those that have had their data taken hostage will know, receiving a ransom demand from an unseen, anonymous attacker can instil a sense of fear, anxiety, embarrassment or even guilt. All of which is designed to coerce them into paying up.

The WannaCry attack in May was the largest ransomware attack ever

EXAMINING TACTICS

However, while there are many insights into the technical mechanisms behind ransomware, there has been less exploration of these psychological aspects of an attack and the specific techniques that are being adopted to obtain payment. As such, SentinelOne, recently commissioned research to better understand the tactics used by attackers, from analysis of the digital ransom notes that they put forward. These are the first notifications that the victim is confronted with on the 'splash screen'. The findings uncovered the various differing levels of sophistication on the part of the attackers as well as some more surprising elements on how attackers are manipulating their victims.

Since the first ransomware attack back in the late eighties, attackers have recognised the lucrative potential of ransomware and that organisations will act on their payment demands. It's relatively difficult to uncover all the evidence on precisely how much cyber criminals are profiting from these crimes. However, the very fact that they are occurring more regularly indicates that they're achieving the aim of coercing victims into paying up to get their data back. It's the cyber equivalent of a human kidnap attack in which a family would be willing to pay whatever sum is demanded in order to release the victim. The major difference is that these 'kidnappings' can be done at scale. The FBI has warned that ransomware will soon be a billion dollar enterprise, and that, in just the first quarter of 2016, an estimated $209 million was paid out by victims – compared with $24 million across the whole of 2015. When your data has been taken hostage and your business is on the line, payment can seem like the only available option.

Through analysis of a range of splash screens, such as the visuals and the language that's adopted, we've been able to examine the tactics that attackers are using, to manipulate their victims, and attempt to elicit these payments. The techniques used to persuade and influence individuals exhibit some of the key aspects of social engineering including:

- **Scarcity:** scammers will take advantage of this by creating a sense of urgency, usually linked to a time-critical offer.
- **Authority:** the concept that individuals are more willing to respond to requests, or follow directions, from someone they view as being in authority.
- **Liking:** exerting influence by getting someone to like you so that they will comply with your requests.

While there are clear variations across the splash screens, what we discovered highlighted some common trends in the way that attackers attempt to prey on people's fears and emotions to elicit a response, using these techniques.

When ransomware hits, time is not on the victim's side: criminals want fast payment and one of the key aspects of ransomware is the 'ticking clock' countdown, giving the victim a specific time limit in which to pay. The research found that a deadline appeared in more than half the samples, to create a sense of urgency in the victim, and to force them into making a pressured decision quickly without careful consideration. Most attackers requested payment within a 72-hour period, although deadlines ranged from 10 hours to more than 96 hours. Most splash screens requested payments, in the form of hard-to-trace online currency Bitcoin (BTC) with payments ranging from 0.001 BTC (around $30) to a maximum of 13 BTC ($4,980).

There is often a consequence for not making a payment, such as the threats of publicly disclosing data. In several cases, the ransom amount increased as time between the onset of the attack and payment elapsed. Attackers would also threaten to delete a file each hour after the payment deadline.

TICKING TIMEBOMB

For businesses that hold particularly sensitive information, the fear of losing data, or of sensitive information being made public, could encourage them to make a payment. There's an added pressure on victims with the clock ticking away: weighing up the cost of making a Bitcoin ransom payment against the loss of valuable data may drive organisations and individuals to make decisions that they otherwise simply would not make. The decisions made in the first minutes following a ransomware warning are, therefore, critical and can make all the difference between containing and managing the threat, or of the attack spreading and causing even more widespread disruption.

> THE FBI HAS WARNED THAT RANSOMWARE WILL SOON BE A BILLION DOLLAR ENTERPRISE

They have been given the added pressure of ever increasing consequences if payments aren't made, which further ratchets up the stress. This is scarcity and urgency at work; the victims now believe that only a quick reaction will prevent sensitive files from being released and if you're desperate to get your data back and your business back up and running, you're more likely to pay. There are, however, no guarantees that the attackers will comply and that the data will be released once payment has been made.

It might seem at odds with the very notion of cyber crime that there should be an element of customer service involved, however, one of the key findings from the study has revealed ways in which the attackers appear to assist the victims, with a 'helpdesk' approach. These included screens with the use of instructions on how to make payments using Bitcoin, frequently asked questions and even the offer to speak with one of the team. A third of the splash screens actively provided instructions on how the victim could purchase Bitcoins to pay the ransom. We can't – perhaps – surmise that this is evidence of a social conscience, but it could fit the social engineering tactic of 'liking' and another ploy used by

the attackers to attempt to elicit prompt payment.

What was also notable from the screens is the use of visuals, associated with authority or taken from popular culture. In some cases, the FBI logo was used with the aim of creating authority. In other instances, menacing pop culture images used included 'Jigsaw' from the Saw horror movie series.

We're just starting to uncover the underlying mind games used by attackers, but exploring the techniques used is important in broadening our understanding of how we can educate and support end users. The range of ways that attackers are leveraging fear, piling on pressure and ratcheting up anxiety points to a worrying trend. While the examples we analysed show varying levels of sophistication, we do know that we'll most likely see more professional ransomware campaigns emerging and – as attackers continue to profit from the crimes – higher payment figures will more than likely be demanded as a result.

ESTIMATES PUT THE AVERAGE COST OF A RANSOMWARE INCIDENT AT MORE THAN $713,000

We're also seeing new ways of criminals attempting to extort money from organisations such as the recent attack on HBO, in which attackers broke into the network of the studio and reportedly stole over 1.5TB of information, including unreleased *Game Of Thrones* episodes, demanding a multi-million dollar ransom.

TACKLING THE PROBLEM

It's clear that we'll need new approaches to deal with these threats. Mechanisms for reporting crime that are clearly defined are important. Ransomware often goes unreported, however we need to have a clear and accurate picture of the scale of the problem in order to more effectively tackle the ransomware epidemic. Reporting these crimes will help government agencies and law enforcement to understand how and where to allocate the resources.

Organisations need to continue to be vigilant. Ensure that there are proper backups in place and isolate the attack quickly so that it cannot spread further. It's vital that staff are trained to act quickly – the first actions taken in the immediate aftermath of an attack are critical to minimising its impact. Our advice is also that organisations should not pay the ransom; this plays into the hands of the attackers and perpetuates the spread of this crime.

Ransomware is one of the fastest growing types of malicious software and as it continues to evolve, we need to deepen our knowledge of the tactics criminals are using to manipulate victims. This provides a route to more informed defence strategies, training, and awareness for users and security teams, which is based on the realities of the threats they are facing ●

Tony Rowan is SentinelOne's Chief Security Consultant. He has over 20 years' of experience in the security industry across multiple sectors, including the defence industry.

Criminals hacked HBO's network and threatened to leak episodes of *Game Of Thrones* if their demands weren't met

Picture credit: Getty