TIGHTENING THE NET

The last few years have seen an explosion in cybercrime. So where is the threat coming from? What will the future hold? And how can business fight back? **Matt Burgess** reports

"Oops, your files have been encrypted!" said the message at the top of the red box. On the left of the screen, a countdown timer showed the ever decreasing seconds, minutes, hours and days until the files you'd worked on for weeks would be erased forever. At the bottom of the popup was a note asking for $300 in bitcoin – and if you didn't pay in three days the ransom would be doubled. It seemed like a no-win situation.

This message appeared on 400,000 computers around the world in May, in the largest ransomware attack in history. WannaCry, as the attack was called, caused disruption and panic and even put lives in danger as it rapidly spread around the world infecting the medical profession, governments and train services. More than 40 hospitals and their governing organisations were infected in the UK's National Health Service as chaos ensued: doctors were forced to turn patients away and even cancel operations that relied on imaging technologies. Computer systems had not been upgraded or had the latest security updates applied, making them vulnerable.

If it hadn't been for 22-year-old security researcher Marcus Hutchins, WannaCry could have continued to spread to thousands more computers. When inspecting the ransomware, Hutchins spotted an unregistered URL address. After registering the domain, he inadvertently found it acted as a kill switch, stopping WannaCry's spread almost instantly.

WannaCry had propagated itself by harnessing a security exploit that can be used against the Windows operating system known as EternalBlue. Knowledge of how to exploit it had been posted online by a mysterious hacking group known only as the ShadowBrokers. They claimed that the exploit was stolen from the US National Security Agency (NSA) and they released it online only after they failed to sell EternalBlue and other hacking tools linked back to the NSA.

"An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen," Microsoft president Brad Smith wrote online, warning that a similar scenario could happen again. And he was right.

> "An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen"

The following month, NotPetya, a piece of malware based on EternalBlue, hit thousands of computers in Ukraine and other countries. The same attack had been repeated.

Until this year, giant cybersecurity incidents linked to ransomware were rare. Threats and cyberattacks at lower levels are more common and often have more success for their creators. These can encompass phishing scams, where legitimate-looking emails try to get users to reveal their details; keyloggers that record every press on a keyboard; and attempts to break encryption. More recently devices that are part of the Internet of Things have become a target. Connected DVRs, IP cameras and routers using weak passwords were all compromised by the Mirai malware in 2016. Once broken into, the devices were used as part of a giant botnet – said to have involved tens of millions of IP addresses – to overload the systems of web service provider Dyn in a Distributed Denial of Service (DDoS) attack. As a result of the disruption at Dyn, the websites of Netflix, Amazon, the BBC, PayPal, Reddit and more were taken either partially or completely offline.

GETTY

"There are longer term trends that pose a serious threat to business and infrastructure as well," says Tim Erlin, vice president at US security firm Tripwire, adding that the "most concerning" of these is an increase in attacks on industrial systems, including "utilities, manufacturing and critical infrastructure".

One of the first signs that hackers had started targeting infrastructure came from Ukraine in December 2015. Thousands of people in the Ivano-Frankivsk region of the country were left without electricity on 23 December after hackers gained access to internal systems. The attack is believed to be the first successful cyberattack on public utilities: officials in Ukraine, the US government and security companies have blamed outside influence for the blackout. But this hasn't been the only attack on infrastructure. Kiev's power grid was also targeted by sophisticated malware called Crash Override and other countries were impacted. Documents said to be leaked from the UK's spy agency GCHQ, and reported on by Vice Media's tech website Motherboard, say a "number of Industrial Control System engineering and services organisations" within the country are likely to have been compromised by hackers. The US government has also warned industrial firms that their systems and connected devices could leave them vulnerable to attack.

"As more technology is network connected, we'll see increasing attacks targeting the consumer and industrial Internet of Things," Erlin says. "Your connected home increases the risk of cyberattack. The same is true for connected businesses."

TRACKING DOWN THE HACKERS

Finding out who's responsible for any kind of attack is incredibly complex. Security company FireEye, using its iSIGHT intelligence tool, is tracking seven recognised groups linked to financial cybercrime and 60 cyber espionage groups – which have more than 600 clusters of activities. Some of these have been linked to their country's government. Hackers in China are said to have stolen US data on nuclear weapons and information from the FBI, while the USA has been linked to the Stuxnet worm, which infected Iran's Natanz nuclear power plant and stopped it making weapons. Meanwhile, Russian hacking groups have famously been blamed for interfering with the US 2016 presidential election.

To achieve this level of hacking success, the groups have to be organised and disciplined. FireEye analyst Kimberly Goody says cyber criminals deliberately work during the same timezone as those they are targeting, as an email received in business hours is more likely to look legitimate when compared to one that arrives in the middle of the night.

Goody's colleague, Cristiana Brafman Kittner, adds that those hacking for espionage purposes will often impersonate other groups to disguise their origins. "We assess that the group CyberCaliphate, which had previously conducted attacks as a pro-Islamic State hacktivist group, is actually a false front for activity conducted by Russian actors using infrastructure connected to [Russia-linked hacking group] APT28," Kittner says. The CyberCaliphate name was said to be behind a hack on French broadcaster TV5 Monde. The channels of the TV station were taken offline and false content was posted on its websites and social media channels.

"It's very easy for a skilled actor to create a

Angling for a win Team Shellphish watch their system perform at the DARPA Cyber Grand Challenge at DEF CON 24 in Las Vegas

ANN HERMES/THE CHRISTIAN SCIENCE MONITOR/GETTY

KEEPING YOUR BUSINESS SAFE

Brendan McKenna, CTO of Uni-Fi Global, which provides Sim-free global Wi-Fi devices with 4G data at local prices, has advice on how to keep your business safe from cyberattacks

1 Refrain from clicking on links contained within emails from sources that you do not know.

2 Check if a website is using Hypertext Transfer Protocol Secure (HTTPS), the green lock in web browsers, before sharing personal information.

3 Use a Virtual Private Network (VPN) to provide a 'secure tunnel' for data being sent from your device and from the internet.

4 Use unique and strong passwords (a combination of letters that don't make a word, characters and numbers) across all of your devices.

5 Every company should have a security policy and all members of staff should be trained, regardless of the size of a firm.

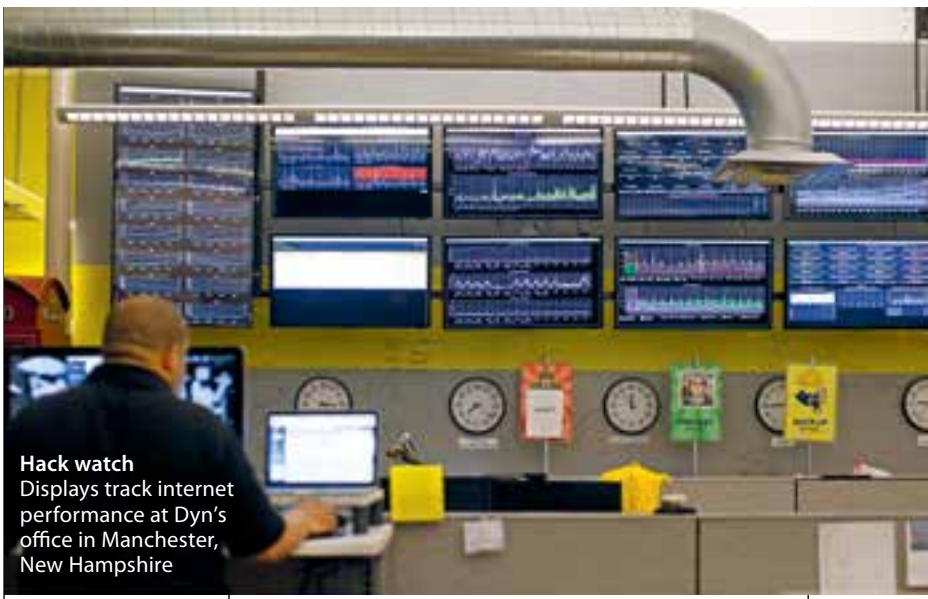
6 An in house or external IT support function is critical and should be alerted immediately if there are signs of malware, unauthorised access, corruption or intrusion.

7 When out of the office avoid connecting to unsecured Wi-Fi networks in cafés and hotels, and on public transport.

deception by altering artifacts – using similar domain-names, or infrastructure that has been used in previous cyberattacks," says Christiaan Beek, lead scientist and principal engineer at McAfee.

This obfuscation can make the attribution of cyberattacks incredibly difficult for those analysing them. It isn't always the case, though. Kittner says there are similar "hallmarks" used by some hacking groups: these include the inclusion of the same malware in different cyberattacks and phrases or colloquialisms that pinpoint a certain geographical area. Some hackers also want to be found and leave clues to their presence. "When the mission is complete, operators may simply exit the network, leaving any tools, backdoors or other evidence in place," Kittner says. "Other operators may attempt to 'clean up' before departing, uninstalling backdoors, overwriting files and purging log data to minimise any evidence of their activity".

For Beek, one of the key ways to help identify the perpetrators of a cyberattack is deep analysis. "Look more broadly at an attack and ask yourself questions around who would benefit from this attack," he says. "Was there a political conflict going on? Does the data match with historical evidence and is it in line with behaviour we have seen before?"



Hack watch
Displays track internet performance at Dyn's office in Manchester, New Hampshire

AI COMES TO CYBERSECURITY

Almost all industries are being disrupted by AI and machine learning. And cybersecurity is no exception. In August 2016, some of the world's top security researchers and hackers descended on Las Vegas to take part in the world's first hacking contest in which bots were pitted against each other. The event, the final of the Defense Advanced Research Projects Agency (Darpa) Cyber Grand Challenge, saw the computers of seven teams launch cyberattacks against each other, while also trying to defend their own systems.

> "With the lack of regulation and oversight, malicious actors are able to advance their AI developments quite rapidly"

The contest showed how automated systems can be developed by hackers. Ankur Modi, the founder and CEO of cybersecurity startup StatusToday, says he always assumes "the enemy" is as smart, if not smarter, than those they targeting. "With the lack of regulation and oversight, malicious actors are able to advance their AI developments quite rapidly," he says. "AI is not good or bad, the actors who use it are."

There are a number of ways AI and machine learning could be used to launch attacks. The most imminent, says Dave Palmer, director of technology at Darktrace, utilises similar technology to the tech giants' increasingly ubiquitous AI assistants. "We're getting so good at understanding the meaning of text – whether that's in simple things like Twitter bots or advanced things like Alexa and Google Assistant – we're getting to the point where spam and spear-phishing could get supercharged," he says.

He imagines a malicious system that is able to learn how people communicate – messages to bosses may be more formal than conversations with friends – and imitate them. "The aim being you can spread from victim to victim very quickly and far more successfully than the really basic spam we've been thinking about in the last few years," he says. This could be used for messages trying to extort money as part of financial cybercrime or to convince a victim to open an email attachment that contains ransomware.

A more extreme example outlined by Palmer is using AI to "fool a business into making the wrong decision" by hacking its processes and editing its underlying data. This could involve strategic decision-making, such as manipulating an oil company into building a drilling rig in the wrong location by editing the information it has collected before it is analysed and reaches decision makers. AI researchers, including Elon Musk's OpenAI, the Massachusetts Institute of Technology (MIT), and Google's DeepMind have made progress on systems that can write their own software or code – there's no reason why hackers couldn't develop similar techniques.

However, both Modi and Palmer believe AI systems can have just as much of an impact in protecting businesses and individuals from cyberattacks. "I am amazed at the speed with which the machines responded to the use of bugs in software they had never seen before and fielded patches in response," Mike Walker, the DARPA program manager behind the Cyber Grand Challenge said at the time of its completion.

Modi says that AI has the potential to provide early warning systems and signal compromises in a firm's security by monitoring and looking for changes. To prove the point, technology developed at MIT's Computer Science and Artificial Intelligence Lab created an AI system that predicted 85 per cent of cyberattacks included in 3.6 billion lines of computer code, generated by system users over a period of three months.

"Responding on a human timescale to an attack that might be very rapid, particularly in this era of ransomware, is often not enough, and a lot of harm could be done when you're operating at internet and cloud speeds," Palmer says. As a result, Darktrace is focusing on an autonomous response to attacks.

In the future, it seems, cyber wars may be fought without human intervention. May the best bot win… ■

NEW YORK TIMES/REDUX/EYEVINE