For daily analysis and debate on science and technology, visit
Economist.com/science

Cyber-crime

Electronic bandits

Malware attacks are not new. But the spread of WannaCry might tip the balance towards treating them seriously

IN 1933 Britain's parliament was considering the Banditry bill—the government's response to a crime wave. The problem was that criminals were using a newfangled invention, the motor car, to carry out robberies faster than the police could respond. The bill's proposed answer to these "smash-and-grab" raids was to create new powers to search cars and to construct road blocks.

In the end, the Banditry bill was not enacted. Its powers were too controversial. But the problem did not go away; what the bill proposed was eventually permitted, and now seems normal. Since then, the technology of theft has not stood still. Indeed, just as in the 1930s, it remains one step ahead of the authorities.

On May 12th, for instance, security companies noticed that a piece of malicious software known as WannaCry was spreading across the internet, first in Britain and Spain, and then around the world. It would reach 230,000 computers in 48 hours, an unprecedented scale of infection according to Europol, Europe's international police agency. WannaCry rendered useless some of the computers that help run Britain's National Health Service (NHS), causing ambulances to be diverted and shutting down non-emergency services. It also nabbed machines at Telefónica, Spain's biggest telecommunications company; at Hainan, a Chinese airline; and even in Russia's interior ministry.

Malicious software ("malware", for short) is designed to infect and damage computers. Sometimes, especially if the creators are youngsters flexing their programming muscles, it is written for the sheer hell of it. Sometimes, it is the work of governments, designed to harm the interests of rivals or enemies. Usually, though, it is written for profit. This seems to have been the case for WannaCry, the modus operandi of which is to encrypt a victim's files and demand payment to reverse that encryption—a common technique, known as ransomware. What makes the WannaCry attack special is its scale and the high-profile nature of its victims. That public profile has led to the asking of questions similar to those which resulted in the Banditry bill.

Bugging out

WannaCry is a combination of two kinds of malware. One, known as a worm, is designed to spread from computer to computer. The other, delivered by the worm, is the encrypting ransomware itself. It is this combination that has made WannaCry so threatening. Ransomware is usually delivered one user at a time, via spoof e-mails which tempt the recipient to click on a link or attachment that then downloads and activates the software. In this case, a single click was able to infect an entire network.

The outbreak was terminated not by official action but by vigilantism. The malware had its head lopped off by a security consultant who goes by the pseudonym "MalwareTech"—for not everyone in the complex ecosystem of computer hacking is a bad guy. MalwareTech discovered that every time a copy of WannaCry runs, it pings out onto the internet a request for a response from a non-existent web address. This behaviour is intended to check that the copy in question is truly out in the wild, and is not being examined in a "sandbox", a closed piece of software in which security researchers can dissect digital bugs to learn their secrets.

Sandboxes simulate access to the entire internet, to persuade the malware under examination to run at full capacity and reveal its secrets. That means responding to all pings in the way a real responder would. So, if a ping returns from the non-existent address, the program can deduce it is in a sandbox, shut itself down, and thus retain its secrets. MalwareTech worked out the web address in question, registered and activated it, and thus convinced every copy of WannaCry that it was in a sandbox and so should shut up shop.

All credit, then, to MalwareTech. But the simplicity of stifling WannaCry suggests the whole thing was a bit of a botched job—as does the apparent business model of its creators. Professional ransomware operations come with fully operational call centres in which real people answer calls from distressed owners of infected machines in order to walk them through the process of getting their files back (and paying the ransom, of course).

WannaCry has none of these. It simply asked for payment, into a particular account, of a sum in bitcoin, an electronic currency. Moreover, Check Point, a com- ▸▸

puter-security consultancy in Israel, has shown that WannaCry's encryption software is so badly assembled that decrypting a user's data after payment has been made is practically impossible. Properly organised ransomware criminals, alive to the advantages of repeat business, usually do unencrypt the hostage data once the money has been paid.

"This is not a serious organised crime gang," Ross Anderson, professor of computer security at Cambridge University, says of the entity behind WannaCry. "It's some kid in a basement in São Paulo or Bucharest or Aberystwyth. If he has any sense, he will smash his hard drive and burn the shards in a bonfire, and never cash in the bitcoin he's been sent, because there are about 30 nation states that would like a chat with him."

Cyber-security

The exploits of bug hunters

Trading in software flaws is a booming business

TO HELP shield their products from ransomware like the recent worldwide WannaCry attack, most big software-makers pay "bug bounties" to those who report vulnerabilities in their products that need to be patched. Payouts of up to $20,000 are common. Google's bounties reach $200,000, says Billy Rios, a former member of that firm's award panel. This may sound like good money for finding a programming oversight, but it is actually "ridiculously low" according to Chaouki Bekrar, boss of Zerodium, a firm in Washington, DC, that is a dealer in "exploits", as programs which take advantage of vulnerabilities are known.

Last September Zerodium's payment rates for exploits that hack iPhones tripled, from $500,000 to $1.5m. Yuriy Gurkin, the boss of Gleg, an exploit-broker in Moscow, tells a similar story. Mundane exploits for web browsers, which might, a few years ago, have fetched $5,000 or so, are now, he says, worth "several dozen thousand". Unsurprisingly, Zerodium and Gleg are not alone in the market. Philippe Langlois, head of P1 Security, a Parisian firm, reckons there are more than 200 exploit brokers in the world.

Such brokers buy exploits from freelance hackers, who make a profitable hobby out of searching for vulnerabilities. They then sell them to those who can use them. Some, Zerodium and Gleg among them, are perfectly respectable, and choosy about whom they deal with (Zerodium says it declines more sales than it makes). Government agencies in America and western Europe, in particular, are eager customers. Others are less scrupulous. For example, e-mails posted to WikiLeaks in 2015 show that Hacking Team, a Milanese broker, sold exploits to Bahrain, Egypt, Morocco, Russia, Saudi Arabia, Sudan and the United Arab Emirates, none of which has a sparkling record of democracy and freedom.

Exploits are also sold in shadowy online markets, where customers are often out-and-out criminals. At some point, no doubt, WannaCry changed hands this way. Nor is that lack of doubt rhetorical, for monitoring activity in the nether parts of the web can, and in this case did, offer omens of trouble to come.

Just as someone will sell you an exploit, so someone else will sell you a warning. One such is CYR3CON, in Phoenix, Arizona. This firm produces reports of possible threats, based on the results of its software sifting automatically through the online writings, in 15 languages, of hackers involved in the field.

On April 15th, a month before WannaCry began freezing data on Windows-based computers, CYR3CON's software picked up chatter about exploits designed for just that task. Eleven days later, it highlighted exchanges about one such exploit that had been installed but not yet activated on more than 62,000 computers. Many were in medical facilities that had previously paid up "without unnecessary conversations". Forewarned, those who had been using CYR3CON's services could take precautions. Others were not so fortunate.

In contrast to its encryption software, however, WannaCry's worm, which spread it so fast, is a sophisticated piece of coding. That is because it reuses software stolen several months ago from America's National Security Agency (NSA), and released online by a hacking group known as the "Shadow Brokers". The stolen software exploits a vulnerability that the NSA discovered in a piece of Microsoft's Windows operating system known as the Server Message Block, which handles networking between computers. This bug, which first appeared in Windows XP, in 2001, has stuck around in all subsequent versions. How long the NSA had known about it, and kept it secret, is unclear.

Computers manage their connections to one another through a series of ports, normally 1,024 of them. Each is assigned a specific sort of task, and can be opened and closed as needed. Port 25, for instance, is designated for sending e-mail. The vulnerability discovered by the NSA lets WannaCry spread from machine to machine, as long as those machines have port 445 left open. On home computers' internet connections, and on astutely managed institutional networks, port 445 is usually kept firmly shut. Exactly how many left it open, and fell victim to WannaCry, has yet to be determined.

Software underbelly

Despite the flurry of headlines, WannaCry is not the worst malware infection the world has seen. Other worms—Conficker, MyDoom, ILOVEYOU—caused billions of dollars of damage in the 2000s. But Bruce Schneier, a noted independent security expert, points out that people seem to have a fundamental disregard for security. They frequently prefer to risk the long-term costs of ignoring it rather than pay actual cash for it in the present.

Here, perhaps, the headlines around WannaCry may do some good. Managers in organisations like the NHS know that there will be no second chances for them in this area. If there is another successful attack, heads will roll. WannaCry's fame has also drawn attention to criminals' normal business of attacking targets that can be relied on to pay up quickly and quietly. Often, these are indeed hospitals. But not the hospitals of an entire country. This is not publicity those criminals will welcome.

That said, the activities of malware criminals do indeed resemble those of Britain's 1930s smash-and-grab gangsters in that they take advantage of getaway speeds offered by new technology—speeds with which the authorities have not yet caught up. Criminals can, in effect, retreat at the velocity of light, to a safe jurisdiction that is near-impossible to discover anyway. If they are to be stopped, someone will have to devise modern-day electronic equivalents of road blocks and search warrants. ■

Solar power

Does light equal enlightenment?

The benefits of cheap illumination in remote areas can be limited

FOR sunny places not connected to the electricity grid, the falling price of solar panels and LED lighting promises a bright future. No more smoky, lung-damaging kerosene lamps. Greater security and safety. More ways to connect with the world—even if that involves only something as simple as being able to charge a mobile phone. And, above all, the chance to work or study into the evening and thus improve both a family's immediate economic circumstances and its children's future prospects. It is a tale of hope. But as a study just published in *Science Advances*, by Michaël Aklin of the University of Pittsburgh and his colleagues, shows, these potentially glowing benefits can in some cases amount to not very much at all.

More than 1bn people around the world have no access to electricity. Providing them with off-grid solar power is something almost all development experts agree is A Good Thing. Yet the evidence for how beneficial it really is was largely observational. Off-grid solar has not been put through the rigours of a large, randomised, controlled trial, of the sort that scientific researchers like to use to test relationships between cause and effect. To fix this oversight, Dr Aklin set about organising just such an experiment.

He and his colleagues teamed up with Mera Gao Power (MGP), one of India's providers of solar-power systems. Their volunteers lived in small villages, all of which lacked electricity, in the Barabanki district of Uttar Pradesh, a state in northern India. Of the 81 villages in the study, 41 were left alone, to act as controls. In the other 40, MGP offered to install a basic, solar-powered minigrid service provided that at least ten households per village subscribed 100 rupees (about $1.70) each a month to be connected to it. That sum represents about 2% of a typical household's expenditure. Those that signed up then had their homes fitted with two bright LED lights and a mobile-phone charging-point.

Connection to a minigrid brought some advantages. Households using solar power in this way cut their consumption of unsubsidised kerosene by a fifth—though, because a limited supply of kerosene is subsidised by the government in this part of Uttar Pradesh, the actual sum saved amounted to about 48 rupees per month, only half of the cost of the (unsubsidised) grid connection. When it came to social benefits from the use of solar power, though, Dr Aklin and his colleagues found little or no evidence of their existence. People did not work longer hours, did not start new businesses and did not study more. Overall, in this case at least, the researchers concluded that solar power had few measurable effects.

This certainly was not what had been hoped for. Dr Aklin conjectures that the explanation may lie with the relatively paltry nature of what was offered, which amounted to an hour or two's extra lighting per day. That is a fair observation, but bigger, more complex systems that would make substantially larger amounts of solar power available would probably be too expensive for villagers in this area.

But will it help him learn?

What would make a big difference, says Dr Aklin, are better batteries that can garner more of the sun's bounty in the first place. "If batteries were cheaper and could store more power," he observes, "off-grid companies could offer larger systems that enable rural households to run appliances and machinery." That, rather than a bit of light in the evening, might really promote economic activity.

As it happens, the cost and performance of batteries is steadily improving, not least because of the development of electric cars. And even if new batteries remain too expensive for use in village solar systems, perhaps second-hand ones that are no longer up to the job of providing the oomph for vehicles will be able to help power villages instead. ■

Clean water

Parsing gas

A way to make water potable using carbon dioxide

THE world's thirst for clean drinking water is vast and growing. It is also unslaked, particularly in poor countries. The World Health Organisation estimates that more than 660m people rely on what it calls "unimproved" water sources. A quarter of this is untreated surface water. Moreover, even water that has undergone at least some treatment may not be potable. Across the planet, 1.8bn human beings drink water contaminated with faeces. All this polluted water spreads diseases such as cholera, dysentery and typhoid. Every year, more than half a million people die from waterborne diarrhoea alone. As they describe in a paper in *Nature Communications*, however, Howard Stone of Princeton University and his colleagues have an idea for a new and cheap way to clean water up by mixing it with a substance normally regarded as a pollutant in its own right—carbon dioxide.

There are many existing ways to make water safe to drink, but each has drawbacks. The first step is usually sedimentation: store the stuff in ponds and let as much of the muck as possible drop out under the influence of gravity. But that cannot cleanse water of minuscule, buoyant particles, including many bacteria and viruses, which will not settle. These have to be removed by a second process: filtration.

Filtering water may be done through porous membranes, but that requires pressure, and thus needs costly pumps. Also, the membranes foul quickly, so require frequent replacement. Filtration through beds of sand needs no membranes, but ▸▸

does need chemicals called flocculants to persuade pollutants to coagulate, so that they can be caught by the filter. An alternative, "slow sand" filtration, employs the layers of algae and bacteria that develop on wet sand grains to remove pollutants. It thus requires fewer chemicals. Slow-sand filters must, though, be refurbished regularly. And both sorts of sand filtration miss up to 10% of harmful bacteria.

Dr Stone's alternative is to abandon the idea of filtration altogether. Instead, he plans to apply a phenomenon called diffusiophoresis to the problem. When CO_2 and water meet at the liquid's surface they react to make carbonic acid. This is a solution of hydrogen ions, which are positively charged, and bicarbonate ions, which are negative. The newborn ions then diffuse away from the surface and into the main body of the water. That creates a gradient of ionic concentration perpendicular to the surface. Dr Stone's insight was that, because the gravity-resistant particles which need to be removed almost always have either positive or negative static-electric charges on their surfaces, their interaction with an ion gradient of this sort, which is itself composed of charged particles, could be used to move them around.

He and his colleagues therefore created an experimental apparatus through which a channel of water flowed in parallel with two channels of gas, one on either side of it, separated from the water channel by gas-permeable membranes. One of the gas channels carried CO_2. The other carried air. CO_2 thus dissolved into the water on one side of the stream, and out again on the other side, entering the airstream and keeping the gradient constant.

As the team hoped, this arrangement caused suspended particles with positive surface charges to concentrate towards the CO_2 side of the water stream, and those with negative surface charges to concentrate towards the air side, leaving the centre of the stream more or less particle-free. In a working system it would simply be a question of splitting the water stream into three as it left the processor, with the two outer branches being recycled and the inner one tapped and piped to consumers.

Dr Stone's apparatus removed all but 0.0005% of the target particles. And it used less than a thousandth as much energy to do so as membrane filtration would have required. A full-scale version would not need additional chemicals beyond the CO_2. And it should, Dr Stone thinks, be easy to maintain.

As to the necessary CO_2, he imagines this would come from power stations and other industrial processes, such as cement-making, that produce the gas in large quantities as exhaust. This would restrict diffusiophoretic water plants to industrial cities—but, since such cities are huge sources of demand, that is hardly a problem. ■

The value of old egg collections

Evolutionary warblings

Nest parasites help to create species-specific eggshell patterns

COLLECTING wild birds' eggs is a hobby, once popular, that is frowned on today. In some countries, it is illegal. That, though, makes past collections the more valuable. And one of them, assembled by the splendidly named John Colebrook-Robjent and bequeathed by him, in 2008, to the Natural History Museum's outpost at Tring, north-west of London, has recently been pressed into service. Its job was to answer questions about the arms races that go on between some birds and the nest parasites (cuckoos and so forth) that attempt to trick them into raising the parasites' young.

That this behaviour causes parasites' eggs to evolve to look like those of their hosts, and the hosts' eggs to evolve not to look like those of parasites, is well established. But Eleanor Caves of Cambridge University and her colleagues wondered if there was more to it. They noted that some nest parasites have sub-groups, known as races, which specialise on different hosts, even in places where these races overlap. One such place is Zambia, the land Colebrook-Robjent adopted after he had been seconded there from Britain, to serve in its army.

In this case, as they report in the *Proceedings of the Royal Society*, the researchers suspected that a second evolutionary pressure would be at work—to avoid laying eggs that look like those of a different host species, so as to evade the attentions of parasite races that specialise on that species. Employing Colebrook-Robjent's collection, they studied the eggs of Zambian warblers. Some of these were laid by species parasitised by birds called cuckoo finches and some by species not so parasitised. For each egg, they measured its precise spectral colour, and also five aspects of its patterning, such as the contrast between markings and background, and the proportion of its surface that was covered by markings.

Using a statistical technique called discriminant function analysis, they used these data to measure how closely eggs resembled one another. As predicted, the eggs of different parasitised species looked far more distinct than did those from different unparasitised species. They could more easily be seen as belonging to the species in question. This, in turn, would be expected to encourage the eggs of different cuckoo-finch races to resemble those of their hosts more closely—which examination of cuckoo-finch eggs in the collection confirmed was true.

Such an arrangement does, however, take time to emerge, as another part of the collection demonstrated. The eggs of a group of weaver-bird species parasitised by diederik cuckoos proved hard to tell apart—as did those of the cuckoos. These weaver birds are, however, closely related, and may be newly separated species. Come back in a few hundred thousand years, and their eggs could be as distinct as warblers'.

Unscrambled eggs