You've been hacked

By Melissa Cogavin, Managing Editor, SCTE

Ransomware attacks more than triple as criminals exploit distractions and loopholes caused by the pandemic.

"Opportunities are like sunrises. If you wait too long, you miss them"

-William Arthur Ward

This is probably how ransomware got started. Al Capone's criminal empire a century ago ruthlessly exploited the near total absence of enforcement of Prohibition in the US in the 1920s, supplying a thirsty nation with whisky from Canada. It gunned down rival gangs and caused shock, mayhem and hysterical column inches for seven eventful years. The American government at the time genuinely thought the influence of the Temperance Movement to be a powerful enough deterrent nationwide that everybody would just voluntarily stop drinking. That assumption made a lot of people very rich indeed.

Fast forward 100 years and history appears to be repeating itself. Gangsters, hackers, geeks and governments the world over saw an opportunity emerging as the digital revolution took hold in the mid-2000s and ran with it. Assumptions starting with "it'll never happen to me" up to "Don't worry, we have a firewall", as well as an almost total lack of enforcement has again caused shock, mayhem and hysterical column inches, and last year cost the USA $350m in ransom payments alone.*

A curious set of social, technical and political conditions occurred in the case of Prohibition and ransomware - that made exploitation irresistible to those who knew what they were doing and were sharp enough to spot a sunrise worth getting up early for.

Over the last few years a few notable cyberattacks have resulted in sensational headlines and humiliated CEOs worldwide – Solar Winds, Kaseya, Sony and Colonial Pipeline are recent high profile examples – but they are all very different in nature and are just the tip of the iceberg. It can happen to anyone, and it does.

T Mobile has just been hacked, with the personal information of 50m customers worldwide released publicly. Accenture has suffered a humiliating 6Tb data leak in August and bestselling FIFA 21 game has been released online after EA Games refused to pay the ransom. Attacks are taking place constantly. It is difficult to keep up.

Kevin Markwick runs an independent cinema in Uckfield, West Sussex and when his ticketing system was hacked his business went into freefall. "We had thousands of tickets sold up to a year in advance, but we had no idea who to. We had £20,000 worth of vouchers just out there with no idea who owned them or what their expiry dates were. It paralysed everything. It took a good couple of years to recover from it and even now we call it The Event. I wouldn't wish this on my worst enemy."

As technology improves, so does the nature of the crime, and it is bewildering to those unfamiliar with the fast-moving language and technicalities. Ben Rapp, Founder and Principal, Securys, a data privacy delivery consultancy told *Broadband Journal*:

"In 2014 most cyberattacks came via a virus sent as an attachment in an email, which were unwittingly opened and immediately disabled the operator's computer, or perhaps the whole company. We all know someone that has happened to.

"By 2021 cyberattacks are far more sophisticated and threat actors are now routinely exploiting vulnerabilities in firewalls, VPN passwords and so on. They are entering a company's servers via what seems to be an innocuous software update from a trusted supplier."

They are appearing on our phones too. This newer style attack is phishing, which, according to Mark Mulready, Vice President, Cyber Services at digital platform security firm Irdeto, has "extended the attack surface for most companies and increased the risk significantly. Hackers are phishing humans in SMS, web, social, gaming, collaboration apps, search and email."

Phishing as a Service (PaaS) is now big business, which is why over the last few months you will have seen what appears to be official correspondence from the Royal Mail from a random UK mobile number, asking you for £2 to settle outstanding postage via your mobile phone. This number is owned by someone paid to infiltrate databases. Awareness is as important as enforcement, especially where vulnerable people are concerned, and the UK government has launched a campaign to this end on national TV and radio.

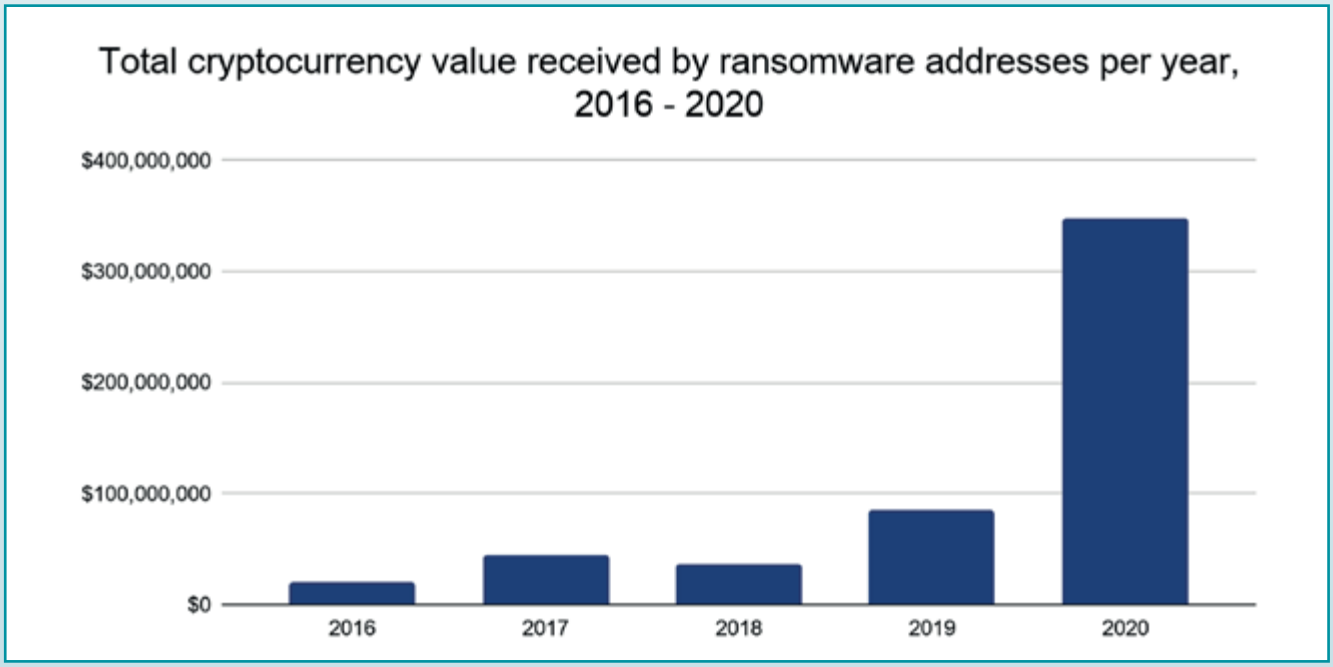
Even Irdeto itself has been subject to some audacious recent attacks. "A Whatsapp message was even sent to a staff member with a deepfake voice message purporting to be the CEO. The voice was pretty realistic representation. Fortunately, the staff member was suspicious and notified the IT security team before it went anywhere."

In the last few weeks, the news about the Pegasus cyberattack has also hit headlines; spyware (for surveillance, not ransom) has been launched on 50,000 Android and iOS mobile devices belonging to heads of state, politicians, royalty and journalists worldwide, the work of an Israeli software developer, licensed by – well, it might be libellous to say in *Broadband Journal* as the story continues to unfold. It has always been assumed that iPhones in particular were impenetrable, but once again, assumptions have got people into awful trouble.

"There are two elements at work in a ransomware attack," said Ben. "There is a base layer; software factories in Eastern Europe produce toolkits that licence them to invidious third parties that gain access to a client and these factories take a percentage.

This is called Ransomware as a Service (RaaS). That was going on before but has expanded and is more formalised now.

He went on. "Then there is another layer that involves organised crime groups perpetrating attacks directly. There is a lot of rumour that these are state sponsored, and Russia is alleged to be behind many attacks. There is a lot of supposition that these activities are tacitly enforced by the State." That is not just one state – governments worldwide are rumoured to be



Source: https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest

actively harnessing this technology, which may explain why they have been so slow to act on regulation and enforcement. "The choice of targets in these later cases tends to be strategic rather than purely commercial," he concluded.

In 2010 an attack took place on an Iranian nuclear power plant, causing the centrifuges to actually tear themselves apart. Fingers were pointed at the US and Israeli governments at the time, though they remain allegations even now. This attack, known as Stuxnet, was ground-breaking at the time in that it directly affected the hardware, rather than the infrastructure around it, and hasn't been replicated since (though it is entirely feasible).

Attackers of Colonial Pipeline meanwhile, which supplies gas to the entire Eastern Seaboard of the United States, had focused for the administrative side of the business, forcing Colonial Pipeline to shut down the business entirely. This was the choice of the company rather than the attackers. Colonial chose to shut it down as they were haemorrhaging money while the attack went on because their administration, their ability to charge for gas, had been compromised.

Ben agreed. "This leads to Interesting moral and ethical questions - if the delivery infrastructure isn't affected, should the business really be shut down? Hospitals are a good example of this. Do you stop providing healthcare if you can't keep charging for it?"

Mark elaborated on the relative subtleties of the ramsomware landscape. "State-sponsored cyberattacks and cybercrime should be seen as two separate fields (although they are inter-twined to some extent). State sponsored cyber capacities can be compared to the nuclear arms race of the last few decades. If major nation states both have the same capabilities it will work as a deterrent and no one will use it to 'take down an entire nation' (although this is already theoretically possible).

"What makes it more complex is that the nuances are different in cyberspace, attribution is a challenge and when does someone actually cross a line? Espionage has always been 'fair game' between nation states and was established well before the internet. It's just that the geo-political developments and technological advancements in recent years have brought new capabilities which have been enablers in this context."

Perfect timing

The current geo-political climate, the rise of nationalism, obsession with border control and the global pandemic have provided something of a petri dish for recent ransomware attacks. We are all distracted, anxious, unable to concentrate and worried about the future. Money worries have added to this - investing in a firewall will have been low down in a crisis environment where hand-washing and masks were considered life-or-death priorities over the last 18 months.

We are also working from home in isolation, hardly the most secure environment and for the IT department of a large multinational, the stuff of nightmares. "It's the perfect time for ransomware," one industry insider told me. "It's out of control. We are at war." Alarmed, I pushed for more detail. He laughed. "Is it state sponsored? Does it matter? What can we do about it if it is? Better to focus on what we can control."

Perhaps the biggest single issue facing our industry is pace. Technology is evolving faster than your average multinational can keep up with it, but the perpetrators are agile enough to exploit gaps in knowledge, technical bewilderment and lethargy at the highest level. They then turn it into a lucrative - and thanks to cryptocurrency also peaking round about now - virtually untraceable business.

Ben also pointed out that for cybercriminals, planting malware into systems and extracting ransoms is a full-time job, whereas cyber security for most of us is a drain on time, a reluctant purchase, a pain to install and something few of us understand in any real depth. We may also have a full-time job elsewhere to manage. There they have the advantage.

Online, forums are enraged at the glacial progress at national and international level; chatrooms are ablaze with 'I told you so' and 'we warned you on Twitter in 2017!' rhetoric, and they have a point. Agencies are hampered by slow legal processes that are years behind the technology they are attempting to legislate. However, things are starting to shift. This side of the Atlantic there is a well-constructed "No More Ransom" website produced by both Interpol and Europol, offering advice and a place to report attacks with a dark warning that "the general advice is not to pay the ransom. By sending your money to cybercriminals you'll only confirm that ransomware works, and there's no guarantee you'll get the decryption key you need in return." If you do pay, the likelihood is you will be targeted again of course.

The US government has also recently introduced a platform for American citizens to report ransomware attacks – StopRansomware.gov. Interpol hosted a forum this summer and a statement from Secretary General Stock confirmed that the approach must now "adopt the same international

> **As long as companies continue to pay the ransom and there is little to no risk of being subject to criminal sanctions, the criminal groups will continue to exploit and grow this ransomware plague.**

collaboration used to fight terrorism, human trafficking or mafia groups such as the 'Ndrangheta."

The creaky Five Eyes Alliance, a security agency set up at Bletchley Park between the US and UK in 1941 and now also includes Australia, New Zealand and Canada also monitors transnational cyber threats. It probably helps a bit, but given the outrageous frequency and gravity of security breaches emerging daily it clearly isn't anywhere near enough.

In April a consortium of big tech companies and the National Crime Agency in the UK approached the Biden administration with a set of recommendations about what needed to be done to curtail such rampant activity, especially concerned that the pandemic had opened the floodgates to ransomware attacks in small companies, public sector offices, schools, hospitals and universities. The Colonial Pipeline attack has served as a wake-up call and it appears federal agencies and business are on high alert and collaborating together for the first time. The same is starting to happen in the UK, but while encouraging, this is not legislation; to date there have been no arrests.

It is an arms race. Mark agrees. "For cybercriminals it's a race between regulation/enforcement and the opportunity to commit the crime. As long as companies continue to pay the ransom and there is little to no risk of being subject to criminal sanctions, the criminal groups will continue to exploit and grow this ransomware plague. They will use some of their ill-gotten gains to fund ever more sophisticated attacks by paying researchers and other criminal groups to develop or share new exploits. This will lead to continued significant disruptions in the coming years, unless there is a swift and strong regulatory and enforcement response on a global level, such as making it illegal to pay ransom."

Humans getting in the way

Culturally it would also appear that senior executives in large multinationals prone to hacking have not evolved at the same rate as the technology attacking their servers or their perpetrators. On 2 July this year Miami-based software company Kaseya was targeted by a Russian ransomware gang in a supply chain ransomware attack, which has since gone public and identified itself, asking for $70m in ransom. Kaseya ironically provides software 'to improve efficiency and security' for its customers but unfortunately for them, their own software was hacked by malware pretending to be a software update. This was not spotted by Kaseya itself and resulted in the infection of 1500 of their customers' infrastructure and, according to REvil, the gang behind the attack, 'more than a million systems' were affected overall. You can imagine the press reaction. Bloomberg reported a catalogue of security failures within the company from 2017-2020 further to interviews with exasperated junior employees, whose pleas to management were ignored repeatedly; many have since left the company in frustration. Poor password control, slack security, infrequent monitoring of internal systems and evidently an unwillingness to listen to warnings are to blame in many of these situations; Mark Mulready admitted that a combination of education and time were the only things that were going to lead to significant changes within large organisations so vulnerable to attack.

"Money is a good teacher, and with the significant disruptions management has seen in recent attacks, they are becoming more aware of the potential impact." However, it is not that simple. Mark went on, "The other side of the coin is that executives are not keen to pay for security, because security itself is not making your business any money. Nobody likes to pay for insurance either. Over time, management are starting to become more aware of the risks of how much they need to invest to reduce those risks to an acceptable level.

It is all very well to assume that large organisations will be obvious targets for ransomware and phishing attacks, but Mark had a warning for smaller businesses too. "The most vulnerable segment of all is small businesses, who perhaps don't have the knowledge and funds to adequately protect their networks. National initiatives like StopRansomware.gov will help these organisations and many more to take simple steps to protect their networks and respond to ransomware incidents. We have noticed companies increasing their spend on cybersecurity. Staff awareness campaigns and training are very important, as most ransomware attacks start with a phishing exploit."

The unfortunate disconnect between technical experts and management leads to glaring holes in security. Assumptions at work yet again. Mark said, "The experts need to be able to explain the risk in a clear way and most of today's risk management methods in cybersecurity cannot do that. Some external vendors provide advice which is vague and highly technical, and as a result of that, it can be difficult for management to understand the risks and what steps need to be taken to mitigate them appropriately."

Kaseya is not the only company with egg on its face. Solar Winds, another American IT firm supplying its customers with security software was the victim of a supply chain ransomware attack in late 2020, affecting an embarrassing number of high-profile government agencies, from the Department of Homeland Security to the Treasury Department. The damage is still unfolding now and allegations have been made that Chinese as well as Russian hackers were to blame.

It was unfortunate timing and likely to have been politically motivated as the breach occurred within weeks of the departure of the government's Cybersecurity and Infrastructure Security Agency (CISA) chief, whose concerns that Trump's election fraud claims were bogus got him fired. This rudderless ship was therefore ripe for an attack and the red faces it caused the US administration and Solar Winds at the time would have been considerable, never mind the ransom.

However, probably the most humiliating aspect of all was the confirmation in the press by an independent security researcher who warned SolarWinds last year that the password the company used to get into its own systems was laughable: solarwinds123. The warning was ignored. Anyone still using their date of birth and their pet's name as a password for everything should probably act now.

Many companies have wearily paid the ransom when attacked, knowing that an insurance premium would likely be as expensive and, knowing insurance underwriting, they may not be covered should the time come anyway. Cynical and understandable though this is, it is feeding into the hands of ransomware attackers who are becoming bolder all the time.

Protection

Against such a backdrop it is a wonder that more attacks aren't happening on a daily basis, but there are things we can all do to mitigate things.

In 2021 data is king. It is difficult to even order a pizza without parting with your date of birth, but such data gathering is risky and unnecessary. While it is valuable to the organisation collecting the data, it also puts the organisation at considerable risk from cyberattackers. The value of your customers' data is far less than the ransom you will be charged if hacked.

The best practice, according to everyone *Broadband Journal* spoke to, was to control the appetite for data. Only ask for what you absolutely need to function as a business. Secondly, separate the administrative from the operational. If the organisation is hacked, only one part of the organisation is affected; one compromised database is better than all of them. The military has been operating along these lines for years, and successfully too. Only Stuxnet has managed to bridge that gap. Caution should however, be approached with caution.

The risk of being hacked needs to be viewed in terms of overall operability. "The military has tied itself into knots trying not to be hacked," Ben told me. "It can barely operate at all. Better to bring in experts who know what they are talking about. Trying to figure it all out alone isn't going to work, as invariably you will find yourself taking on an inappropriate level of protection, or not enough. It is a very complex, highly technical area. There is a lot of risk."

Finding the sweet spot where a company can comfortably operate and still handle that element of risk is the challenge, as is education. Another assumption we are all guilty of and that is that a firewall is all a company needs and once installed, it never needs looking at again. Again, senior executives should be listening to their junior IT staff closely and acting quickly as intelligence changes all the time.

If your company is large enough to require software updates from an external third party supplier, then you must operate in a zero-trust architecture. This is where Kaseya and SolarWinds, and all their 1500 affected customers fell short. Monitor constantly. "Think about how you would protect yourself against the software that should be protecting you," Ben warned.

Another industry insider agreed. "You need to be rigorous in your management of your suppliers as much as your own staff, equipment and processes. You can't trust anyone."

Ben also said that "There needs to be a contingency plan agreed in an organisation, so that a minimum operating

level is agreed company-wide, including how that level is orchestrated is played out and even rehearsed. What does that shadow network look like? Do we work with a pen and paper in the interim? Are we ready to shut down immediately if we need to?"

The fallibility of people means there is no one-stop-shop solution, Ben says, "There is an assumption in organisations that 'malware and ransomware are technology problems so let's get IT to fix it. IT then say, let's buy technology then'. They buy firewall technology, install it and assume that's all they need." The discipline to constantly monitor their systems, their updates and their server activity after that point is where many companies fall down.

Surely the application of machine learning can circumvent the inadequacies of the human condition? Up to a point, yes. However, we are in an arms race situation, and if a machine is built to combat ransomware, remember a better one will be built to combat that, and so it goes. "It is a panacea only," Ben says.

The Future

It would appear we are in a middle of specific time frame; criminal activity is rife because the legislation is so far behind, but it will not be like this forever. "Criminals are always early adopters of new technology," Mark pointed out and he is right – it is well known that the VHS industry got kickstarted in the early 80s by the criminal production and distribution of pornography. "I think it will become worse in the short term, but as it becomes more and more visible how vulnerable our digital infrastructure is to attacks and the problems, there will be a more robust response as education improves, and it will get better in the long term.

"We saw a similar evolution with piracy and security threats in video entertainment, from smartcards, to control word sharing to streaming rebroadcasting piracy to credential stuffing and theft to exploiting weakness in OTT infrastructure."

Everybody that *Broadband Journal* spoke to had a different set of recommendations but they broadly covered the same themes – technology, education, risk management and response.

Seth Adler, Editor in Chief at the Cyber Security Hub in New York put it this way. "Innovative cyber security technology abounds. Those that have the resources and the talent to source and utilise the best and brightest tools in the space will certainly find benefit. But the basics and the fundamentals also matter. Kaseya, and Solar Winds before it, have proven that organisations must have a solid TPRM (Third Party Risk Management) practice in place along with cogent IDR (Intelligent Disaster Recovery) techniques to ensure dwell time and lateral movement are reduced to seconds, minutes and days not weeks, months and quarters."

Governments and bruised organsations are mobilising and confronting the threat of cybercrime together for the first time, which is encouraging. Big tech task forces are humming with activity and legislation is being drafted, so that is also good. Security agencies worldwide have their heads together and all those sensational, embarrassing headlines will have knocked the hubris out of CEOs and IT departments everywhere.

However, within days of this article being written, a powerful assembly of three ransomware companies, REvil, DarkSide and LockBit launched on the dark web, calling itself BlackMatter Ransomware. Brazenly targeting companies with a turnover of $100,000+, outlining its business model on the homepage, it takes care on to point out it too has morals and would not target hospitals, governments or utilities companies, which is touching. A chilling reminder that it is still an arms race and for as long as the sun continues to rise each morning, ransomware remains a considerable threat and and we must all remain vigilant.

* https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest