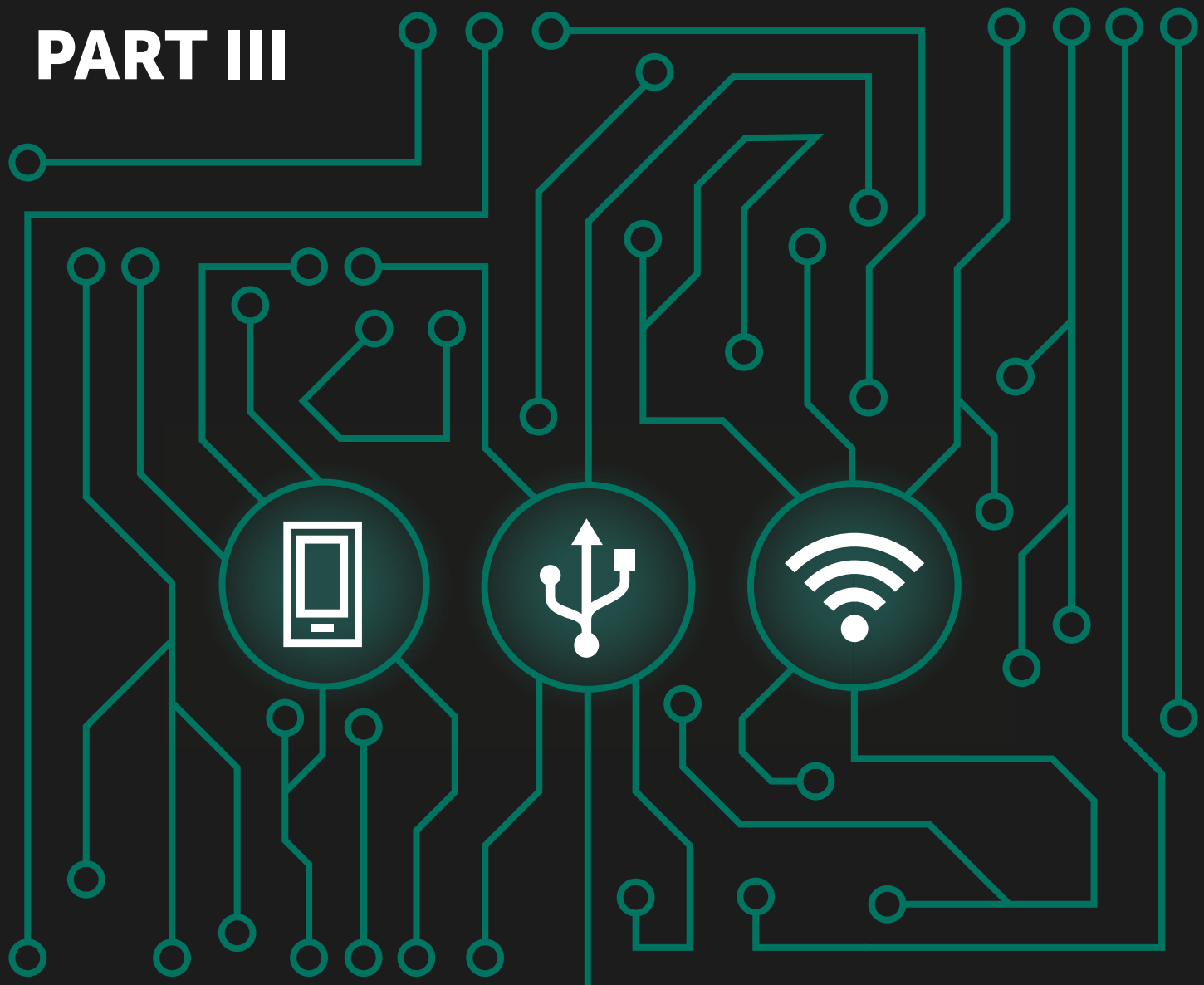
PART III



Kaspersky Security Bulletin:

THREAT PREDICTIONS FOR CONNECTED LIFE

INTRODUCTION

To be awake is to be online

The average home now has around three connected computers and four smart mobile devices. Hardly surprising, considering that 86 per cent of us check the Internet several times a day or more, and that's outside of work. Chatting, shopping, banking, playing games, listening to music, booking travel and managing our increasingly connected homes. The risk of cyberattack can be the furthest thing from our mind.

Every year, Kaspersky Lab's experts look at the main cyberthreats facing connected businesses over the coming 12 months, based on the trends seen during the year. For 2018, we decided to extract some top predictions that also have big implications for everyday connected life.

SO WHAT COULD THE HACKERS BE AFTER IN 2018?

Security gaps in the gadgets you connect to your car

Earlier this year, researchers showed how a hack could shut down all safety features in a car, including airbags. Such attacks will become easier as connected cars contain more and more components that could be accessed digitally. For example: mobile phones can be paired with a vehicle's head unit via Bluetooth; and Bluetooth was recently found to have more than 8 serious software vulnerabilities. A hacker only has to use one and they will have an access to car systems to conduct further attacks. Some cars have cellular or Wi-Fi connectivity and almost any modern car has a USB-port – all of these can be used in order to deliver infected code to the car's systems.

The data exchange between the internal systems of a car has been proven to be vulnerable to external interference, both by external researchers and Kaspersky Lab own findings. Given the fact that car industry is planning the development and production cycles years ahead, it is unlikely that all reported issues will be fixed in new connected cars coming on the market in 2018. Most of these cars were designed before cybersecurity became an issue for the automotive industry. That said, we expect that cars coming off the production line after that will have the most critical cybersecurity features implemented and will therefore be safer.

Vulnerable car apps

Most leading car manufacturers now offer apps to make life easier for drivers – they can locate, lock/unlock your car, check tire pressure, request assistance, schedule maintenance and more. Researchers have already shown how many such apps can be hacked to partly take over a car. 2018 could see the first appearance of an infected app that can manage a car or spy on its owner by tracking their location, or collecting authentication data. This data could then be sold on the underground market. Kaspersky Lab researchers have seen signs that authentication data to access connected car apps is already in demand on underground markets. As the number of connected cars increases, this trend will become a bigger problem.

Security gaps in wearable medical devices/implants, for data theft or sabotage

In 2018, there will be an estimated 19 million connected medical wearables, such as insulin pumps, pacemakers, monitors etc. in use, up from 12.8 million today. Companies are already issuing warnings about security gaps, knowing that, in an extreme case hackers could tamper with devices, set them to administer a fatal dose or to otherwise malfunction. This threat will rise in 2018 and probably keep on rising,

Ransomware. Still everywhere

The global pandemic that is ransomware shows no signs of abating. Our data shows that just under a million of our users were attacked with ransomware in 2017, only slightly less than in 2016 – but the actual global number of those attacked in 2017 will be much higher. For example, the WannaCry ransomware victim count may exceed 700,000. With malware and distribution tools freely available on the web, attackers have discovered that locking or encrypting people's data and devices – and those belonging to big companies, hospitals and smart city networks – is an easy and effective way of making money. In 2018 expect more of the same.

Malware, ditto – particularly that targeting Android mobile devices

We live in an increasingly mobile-driven world and hackers have upped their game. In 2017, we saw Android malware poisoning hotel booking, taxi service and ride-sharing apps, targeting mobile payments (SMS- and WAP billing), and using new techniques to bypass OS security. In 2018 we expect to see even more innovation.

Getting you to mine for cryptocurrency coins or stealing your coins

Cryptocurrencies are becoming more popular, so experts predict hackers will tap into people wanting to get a share of the action. In 2018, this could see more people going over to mining cryptocurrencies on their work-computers. We'll certainly see more attacks designed to steal crypto coins from users, or install hidden mining tools on machines, particularly mobiles. Kaspersky Lab research shows that the number of people hit by such attacks have already exceeded two million in 2017. On the other hand, if handled properly and with the user's consent, some forms of cryptocurrency mining may become a legal way of monetization for websites and/or apps.

Taking control of your connected stuff to create big botnets

Your home routers, connected webcams and smart thermostats are all great, but they're likely full of software bugs and if you don't set a proper password, hackers can pull them into a huge zombie botnet. The infamous 'Mirai' botnet that nearly broke the Internet in 2016 was largely made up of CCTV cameras and connected printers – and in 2017 researchers found attackers improving Mirai's tools. Proven as reliable and effective denial-of-service tools, new botnets built out of insecure devices may emerge in 2018.

Taking control of the world's connected stuff for large scale disruption

Speaking of smart city technology such as CCTV cameras, what would happen if there was an attack on a city's light control systems, causing not just blackouts but stroboscopic effects? Over the next year, smart city technologies such as traffic control, lighting, speed cameras, public transport and power supplies, as well as air traffic control infrastructure and more, will be a growing target for hackers. It's estimated that by 2020 there will be 9.6 billion connected things used in smart cities around the world. Many of them just as buggy and vulnerable as your home router. Disruption to and disabling of these vast connected systems could do untold damage.

CONCLUSION

Stay awake when online

So there's some scary stuff and a few not very nice people out there. That shouldn't stop you from making the most of what connected devices and systems have to offer over the next year and beyond. Fortunately, there are a lot of simple things that you can to stay safe. Here's a few examples:

- Make use of the security features that come with your devices: set a decent password and keep the software updated. Not just phones and computers, but everything that is connected.
- Be selective when choosing a smart device. Ask yourself: Does this really need an Internet connection? If the answer is yes, then take the time to understand the device options before buying. If you discover that it has hard-coded passwords, choose a different model.
- Consider cryptocurrencies as another way of saving and treat them accordingly. Just like you treat your 'regular' money.
- Only install apps from reputable stores like Google Play, created by reputable developers.
- Last but not least, consider supplementing the OS/device security with some additional software – particularly to keep your family and finances safe. A free version of Kaspersky Lab's security software is available here.

For more information and advice on staying safe online please see the Kaspersky Daily blog.