CURRENTS

■ JAMES HEIN

4K may save the day for Blu-ray

As I predicted a number of years back Blu-ray discs never really made it into the market in the same way that DVDs did. With the advent of 4K that may change, or at least the Blu-ray industry is hoping that it will. It turns out that 288,000 4K Ultra Blu-ray discs were sold in the first half of 2016. The 4K discs were only released last year and they are only worth it if you have a 4K Blu-ray player and a TV to match. According to the British trade association BA, a third were sold between October and Dec as gifts so looking for a trend at this point is hardly conclusive. Since to take advantage of the technology means replacing major components in your home entertainment system, then I expect it will be as slow as the original Blu-ray to be adopted. Given the TV world is not transmitting in 4K this may provide some temporary boost but I don't see it being a major one. Also to keep you confused most "4K" TVs sold are actually Ultra HD (3840x2160) and not 4K (4096x2160).

Minecraft for the Oculus Rift. Think about that for a moment. The Windows 10 Edition Beta of Minecraft from Mojang has been updated so that you can run the Oculus Rift virtual reality headset. For those that have seen Minecraft it is reminiscent of the 1980s block graphics games but with a few more colours. So those with the headset can relive those heady graphics days in 3D. Woot, woot.

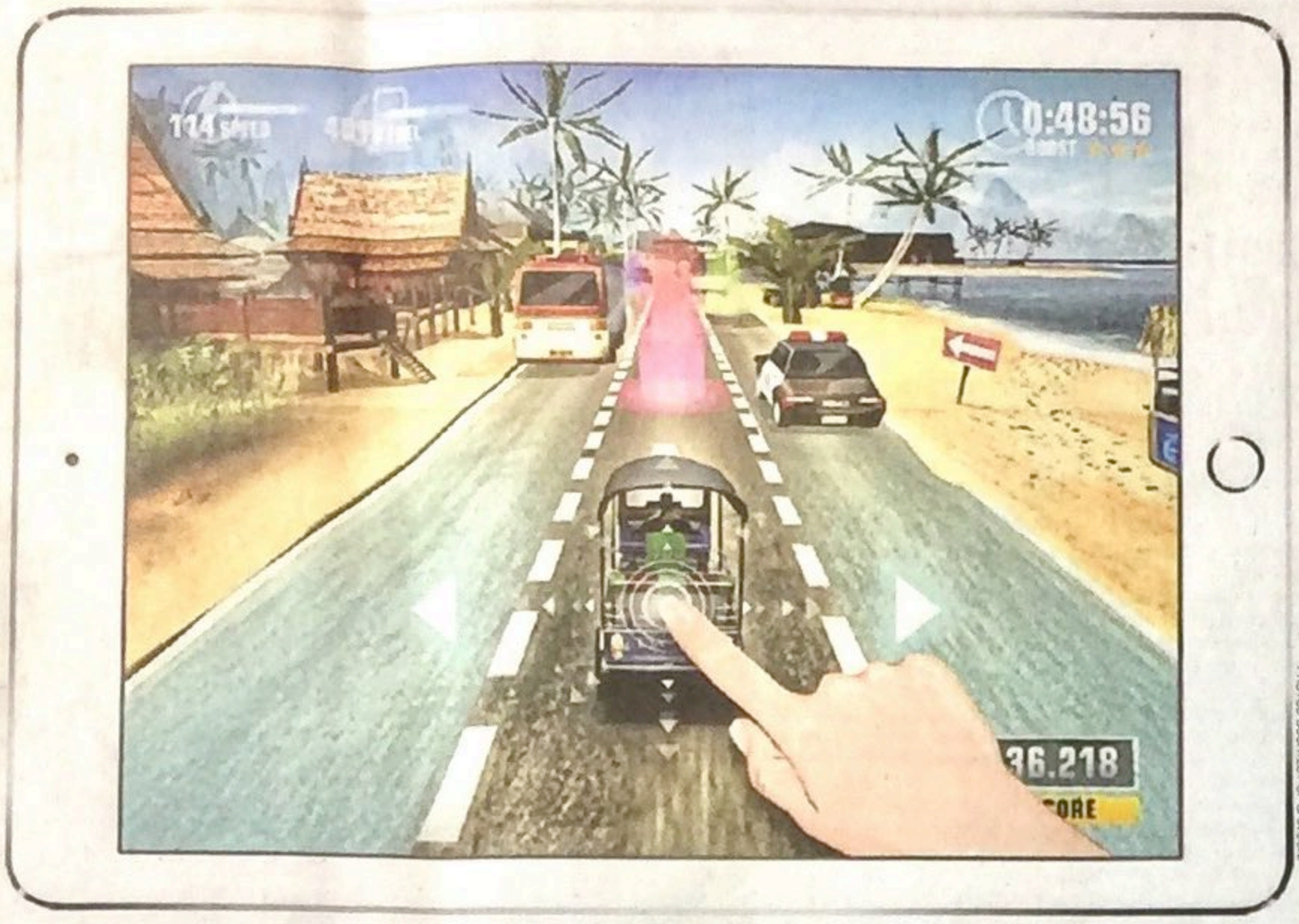
For those that haven't heard of homomorphic encryption, and you will be in the majority, it was a plan to secure data in the cloud by allowing data to be worked on without software encrypting it. If that didn't make sense, they do this by operating directly with the encrypted data so that when the results are decrypted they would match the same operation carried out on plain (unencrypted) text. It is processor intensive, slow, and now it has been found to be vulnerable. Enter some researchers from the Swiss Federal Institute of Technology in Lausanne who showed that a relatively simple plain text attach was good enough to break the encryption. The good news in this case is that the system is not yet implemented so those working on it can go back to the drawing board and see if they can strengthen it. Given that people can crack encryption before it comes out, James' theory of anything in the digital world is crackable is still safe.

So you have an air gapped computer, i.e. one that is not connected to a network so that people can't hack into it from the outside. Think again. Some video researchers from Israel's Ben-Gurion University of the Negev Cyber Security Research Center have found a way to find out what is going on in your computer by listening to the noise generated by hard drives. It requires malware to be loaded into your machine first. This uses the drive's actuator arm to generate audio tones that can be listened to from some distance away.

This kind of technology is not that new, with earlier versions using the computer speaker, the cabinet fans and so on to generate similar noise that is then decoded. Even earlier versions detected the signals sent to the old cathode ray tube. Since then people have removed fans, speakers and microphones and use LED screens. That leaves hard drives, until you replace them with SSDs that is. For the time being the malware would search for sensitive information and then transmit it to the waiting listeners. The researchers have tested the process on hard drives with automatic acoustic management (AAM) that are designed to reduce drive noise and they could still pick up the information on the normal setting. There is some good news. Using a smartphone you need to be within six feet and the data transfer speed is around 180 bits per minute which is really slow. At those speeds you won't be able grab an unreleased movie or detailed engineering plans but you could grab some passwords. If you are interested, you can find out more here arxiv.org/pdf/1608.03431v1.pdf.

This week's feel-good story is brought to you by hackers. It turns out that some Indians running a tech support scam picked on a security expert's parents. You may have seen these scams yourself. You get a message saying that your computer is infected and you have to call a number. Ivan Kwiatkowski, a French malware analyst, responded by giving them a call. He hooked the Indians in with a Virtual Machine they remotely logged into where they pretended to demonstrate that it was indeed infected. He then sent them an image of his supposed credit card to fix his machine but it contained the infamous Locky ransomware. When the scammer opened the picture it started moving through their computer encrypting files and possibly all connected devices, but that is unknown since the scammer hung up. Some people would call this karma.

James Hein is an IT professional of over 30 years' standing. You can contact him at jcfhein@gmail.com.



Tuk-Tuk Rush.

PHOTOS COURTESY OF GAWOONI

GOING FOR A RIDE

A new arcade game seeks to replicate the experience of the tuk-tuk ride

STORY: **SASIWIMON BOONRUANG**

One of the national symbols of Thailand, the tuk-tuk will also soon serve people around the world in a new arcade racing game.

Dubbed *Tuk-Tuk Rush*, the game is developed by a creative team of German and Thais, headed by Frank Holz, managing director of mobile and online game developer Gawooni, who has been in Thailand for over six years.

"Thailand has a very good potential for creative ideas. The game's project management was handled in Germany while the testing was carried out in India, so this [is the product of] mixed talent," said Holz, who entered the game industry in 1996 and once served as marketing director at Infogrames and Atari.

Holz founded IEM Consulting, specialising in the game industry, and has supported a lot of developers and the Software Industry Promotion Agency (Sipa). His company, Gawooni, also develops and publishes mobile and online games, with a special focus on Southeast Asia and India.

"I like this country, I love elephants, and I ride a lot of *tuk-tuks* here," he said. "I had an idea that when I have my own game company, I will do a tuk-tuk game because I know most tourists really enjoy riding them," he said.

> "This is the perfect tool to promote Thailand at the international level

Frank Holz.

Tuk-Tuk Rush's key features are casual racing action with two fantastic game modes: ultra-competitive endless mode and beautiful and enjoyable story mode. The design is authentic, with more than 40 hotspots from all over Thailand, and over 10 outstanding tuk-tuks of different parameters.

The game's pattern is quite similar to that of *Temple Run*. To play the game, players choose their tuk-tuk, get on the track and challenge the rush, drive as far as they can and unlock beautiful hotspots in Thailand. "It's easy to control, but hard to master," Holz said, adding that *Tuk-Tuk Rush* is promoting Thailand in a unique and interactive way. Players can explore the country from the North to the South.

Players can also enjoy the entertaining skins and vehicle designs, challenging missions, attractive scoring and levelling system, interactive garage and support crew, and social-media integration. The Interactive photobook includes fantastic pictures and information about relevant hotspots all over Thailand.

Tuk-Tuk Rush is in line with all relevant trends in the gaming industry of cross-platform gaming (mobile phone, tablet, PC), free-to-play and microtransactions (a business model where users can purchase virtual goods via micropayments).

Tourists and gamers from other countries are the target group for *Tuk-Tuk Rush*, said Holz, adding that several travel guides recommend a ride in tuk-tuks among the 10 must-dos when visiting Thailand.

"This is the perfect tool to promote Thailand at the international level. Everything is going to digital, application. People like entertainment, so we have a game mixed with a travel guide in a very unique, a high quality [package] with optimised and motivating gameplay."

Tuk-Tuk Rush will be available for download in October. After Thailand, it will be launched in Indonesia, Malaysia, India, China, Japan, South Korea and then Europe and US. The game hopes to secure around five million downloads within six months, with one million downloads in Asia.

In 2006, the team of Gawooni developed and released a game designed for BMW called *BMW M3 Challenge*. It was designed as a virtual test drive for PC and distributed for free via the BMW web page. It was part of the launch activities for the new BMW M3. The game was downloaded more than five million times.

Knowledge Development Centre (KDC), a market research company, expects that by the end of this year gamers worldwide will generate a total of US$99.6 billion (3.4 trillion baht) in revenue, up 8.5% compared from last year.

For the first time, mobile gaming will take a larger share than PC, with $36.9 billion.

Thailand is the 23rd-largest games market in the world, and the largest in South East Asia. Of the 17.2 million gamers, 9.5 million spend money on games, a player-to-payer ratio of 55%, above average for South East Asia. The average annual expenditure per payer, of $35.32, is also above the regional average.

Beware of ransomeware with *Pokémon Go*

STORY: **AKIN**

With all the frenzy around *Pokémon Go*, it was only just a matter of time before attackers leveraged its popularity to spread ransomware, a type of computer malware that prevents or limits users from accessing their system. But unfortunately, a new ransomware was recently discovered impersonating a *Pokémon Go* app for Windows.

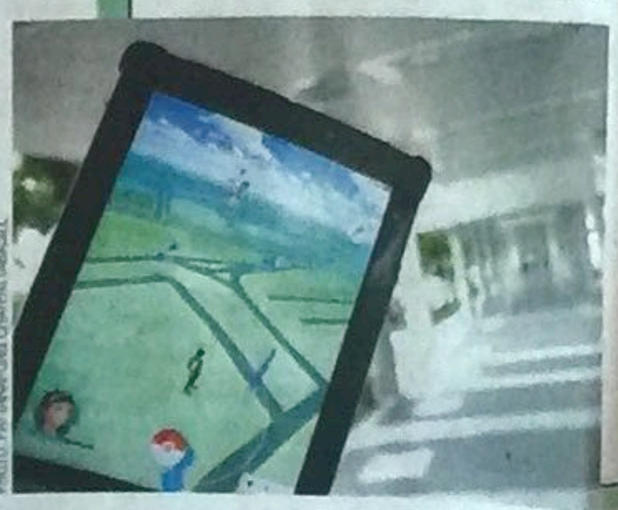


PHOTO: PATTANAPONG CHANTARASIRI

Detected by Trend Micro as Ransom_Pogotear.A, it appears to be like any other ransomware. However, a closer look revealed that its creators based it on Hidden Tear, an open-sourced piece of ransomware released last August 2015, with the intention of educating people.

The *Pokémon Go* ransomware developer designed it to create a "Hack3r" backdoor user account in Windows and is added to the administrator group. The registry is tweaked to hide the Hack3r account from the Windows login screen. Another feature creates a network share on the victim's computer, allowing the ransomware to spread by copying the executable to all drives. Once the executable is copied to removable drives, it creates an autorun file so the ransomware runs each time someone accesses the removable drive. The executable is also copied to the root of other fixed drives. This way, the *Pokémon Go* ransomware will run when the victim logs into Windows.

Based on the language used by the ransom note, the *Pokémon Go* ransomware appears to target Arabic-speaking users, with an accompanying ransom screen that features a Pikachu image. In addition, the screensaver executable is also embedded with an image of "Sans Titre", which is French for "untitled", suggesting a clue to the developer's origin.

The Hidden Tear ransomware isn't new. In January 2015, Trend Micro discovered a hacked website in Paraguay that distributed ransomware detected as Ransom_Cryptear.B. According to the analysis, the website was compromised by a Brazilian hacker and that the ransomware was created using a modified Hidden Tear code. Prior to this discovery, when the source code of Hidden Tear was made public for educational purposes, the creator was very specific about not using Hidden Tear as ransomware. Unfortunately, as expected, the following discovery of Ransom_CrypteaR.B and this current *Pokémon Go*-themed ransomware has shown that even with the best intentions, improper disclosure of sensitive information can lead to troublesome scenarios such as the mentioned discoveries.

To avoid ransomware, users are encouraged to regularly back up files and to have an up-to-date security solution. As the game is introduced in new regions, the *Pokémon Go* craze is expected to continue to gain momentum and cybercriminals will find ways to capitalise on it. In fact, in July, malicious *Pokémon Go* apps were found tricking users into downloading them. This should remind users to remain vigilant of threats that may ride along the popularity of such games.