Les Echos
The Innovator

#5 – February 2018 - Mobile World Congress/4YFN
Distributed in Barcelona and in Les Echos # 22643

CHINA RACES AHEAD
WHY HIGH-SPEED WIRELESS IS A HIGH-PRIORITY NATIONAL STRATEGY

PUTTING AR/VR TO WORK
BUSINESSES ARE PROVING TO BE FAST ADOPTERS

A $1 TRILLION TELECOMS OPPORTUNITY?
Q&A WITH MOBILE WORLD CONGRESS SPEAKER BRIAN BEHLENDORF

HOW 5G WILL IMPACT COUNTRIES CITIES AND COMPANIES

SUPPLÉMENT GRATUIT AU #22643 DU QUOTIDIEN
"LES ÉCHOS" DU 26 FÉVRIER 2018
NE PEUT ÊTRE VENDU SÉPARÉMENT

Cybercrime Is Going Mobile

— Innovative startups are helping corporates combat security risks posed by smartphones and tablets.

By Chris O'Brien

Sometime last November an anonymous group of hackers began hijacking smartphones and redirecting their browsers to a website that conducts "crypto-mining," the term for using computing power to tally transactions made on the blockchain, a type of digital ledger technology. By the time cybersecurity firm Malwarebytes detected the campaign against Android phones in late January, it estimated that millions of phones had been compromised. "The threat landscape has changed dramatically over the past few months, with many actors jumping on the cryptocurrency bandwagon," Malwarebytes researchers wrote in a report. "Malware-based miners, as well as their web-based counterparts, are booming and offering online criminals new revenue sources. Forced crypto-mining is now also affecting mobile phones and tablets en masse."

Rather than attempting to infiltrate inside a mobile phone user's network to steal information, forced crypto-mining makes use of 100% of the processing power of each compromised phone to make money for the hackers. (As payment for their mining or processing services, miners are paid cryptocurrency as fees.) It is just the latest example of how the long-feared security risks posed by gadgets such as smartphones and tablets have finally become a reality. Over the past two years, the number of malware attacks and vulnerabilities on mobile devices have exploded, leading 4YFN, an innovation conference taking place in Barcelona at the same time as Mobile World Congress, to put cyber-security on the agenda for the first time. While innovative technologies, startups, and strategies are emerging mobile offers too many entry points to prevent the bad guys from getting in. The goal now is to use deceit and vigilance to isolate the hackers' movements and limit the damage. "Companies use to think of security as putting up walls and creating a fortress" to prevent anyone from getting in, says Nico Goulet, a scheduled speaker on the February 27th 4YFN cyber-security panel and a partner at Madrid-based Adara Ventures, which focuses on cyber-security and Big Data investing. "Now you assume the world is more open and the walls are not going to protect us. Now you have to assume people are going to get in."

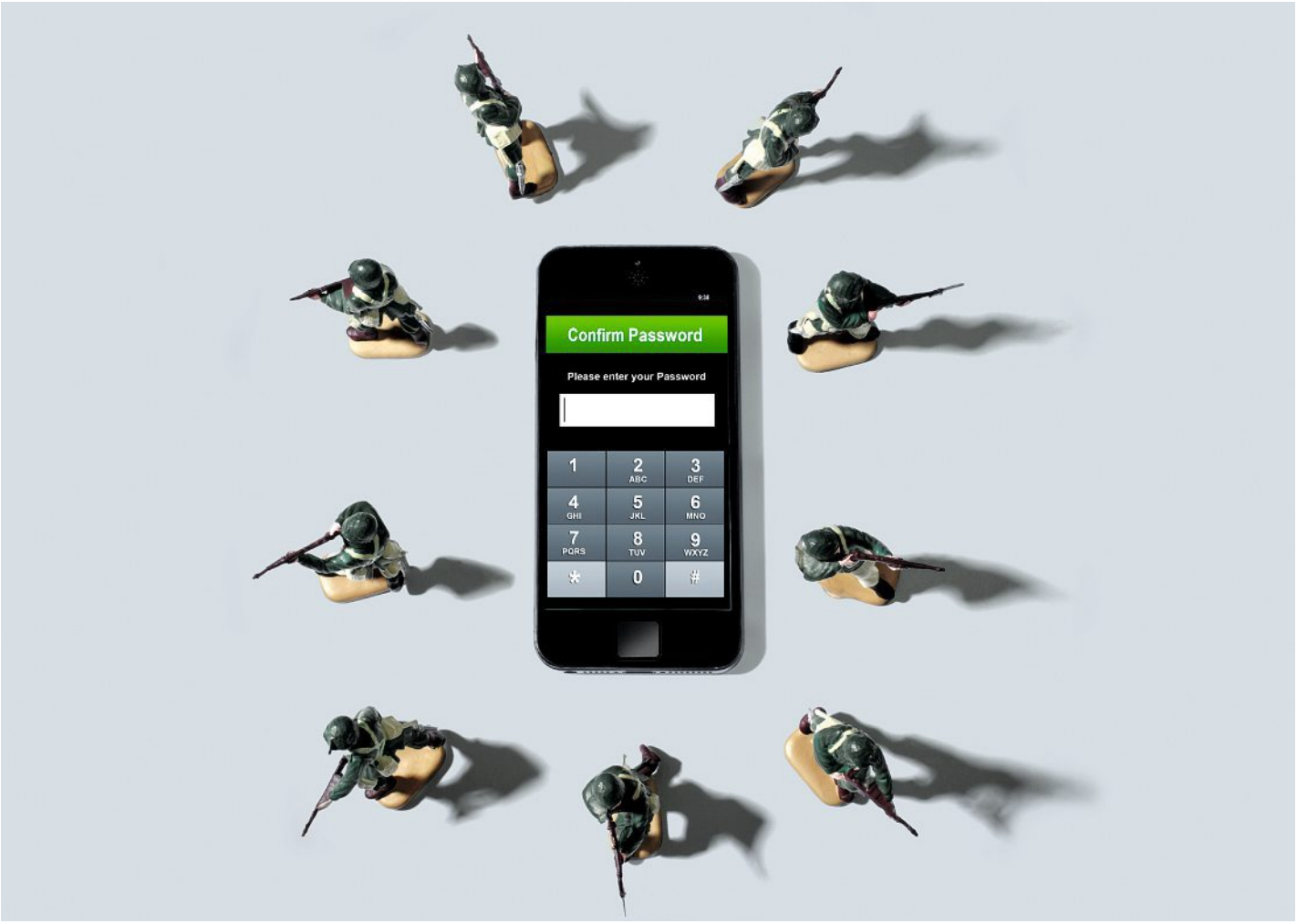
Mobile as the Target

Of course, mobile and the Internet of the Things are extensions of existing corporate networks, which are facing a growing wave of attacks on all fronts. Juniper Research, an analyst firm, recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019.

An increasingly connected world where more information is digitized and stored online has dramatically increased the value of targets, offering tantalizing opportunities for increasingly well-funded international digital crime syndicates and state-sponsored hacking. There's been a non-stop parade of headline-grabbing breaches over the past year, from ransomware cyberattacks such as WannaCry and NotPetya to the catastrophic Equifax hack. As a result, spending on cybersecurity is exploding. IDC projects that the $83.5 billion spent worldwide on security hardware, software and services in 2017 will climb to $119.9 billion by 2021. Even as cyber-security spending overall increases, a report from Thales and research firm 451 notes that mobile will be a particular focus of this investment, with 57% of organizations it surveyed saying they planned to spend more on end point and mobile defense in 2018. That's because over the past two years, mobile has increasingly become the focus of attacks. While security experts have fretted about this possibility since the iPhone ushered in the smartphone age more than a decade ago, it's only more recently that the ubiquity of phones and tablets at work have made them valuable enough to draw more substantial investment and attention from hackers. The lack of security on the devices combined with the growing amounts of data they contain make them much easier access points.

"The evolution of the mobile device into a computing device, I would say it's something organizations didn't put high on their radar for a long time," says Robert Arandjelovic, director of security strategy at Symantec, a U.S.-based global cyber-security software company. "And security is still an unpopular topic. Because people still look at security as a weight that will pull you back rather than something that will allow you do these things."

In an annual security report, Kaspersky, a Moscow-based cyber security



and antivirus software company, notes that during the first half of 2017 it detected almost twice as much ransomware on smartphones as it did for all of 2016. Hackers tend to target Android phones because its open source code and the Google Play stores make development and distribution of apps containing some kind of malware more efficient.

CVE Details, which compiles a database of security issues, received reports of 842 Android vulnerabilities in 2017, up from 523 the previous year and only 13 in 2014. "Google has been playing catch up to improve the security posture of apps available within their store," says Pablo Garcia, CEO of Japanese security firm FFRI, which has developed a mobile malware detection product. "Google removed roughly 700,000 malicious apps from their app store in 2017." But Apple's iOS is not completely immune. CVE Details lists 387 iOS vulnerabilities reported in 2017, up from 161 in 2016.

An Uptick in Vulnerabilities

Trend Micro, which specializes in enterprise data security and cyber security solutions for businesses, was one of the earliest to move into mobile security. In 2012, the company released its Trend Micro Mobile App Reputation Service, which scans publicly available apps for suspicious behavior and malware across all app marketplaces. When employees at big corporates first started using their personal devices at work, IT managers kept a pretty tight lid on access, says Loïc Guézo, Trend Micro's cybersecurity strategist for Southern Europe. But as the practice has become more common, those devices have become more integral, and thus more enticing to digital thieves. "There's more data on these phones and there are more privileged access points they can use to get into the corporate network," says Guézo, So it is no surprise that cyber-security startups which are driving some of the more innovative approaches to mobile security, are in hot demand.

For instance, Fireglass, an Israeli startup, founded in 2014 raised $20 million for its pioneering security strategy known as "isolation." The company's technology creates virtual versions of corporate functions that

CYBERSECURITY STARTUPS TO WATCH

WISEKEY SWITZERLAND

WHAT IT DOES: Authentication, identity management and cybersecurity for the Internet of Things.

www.wisekey.com

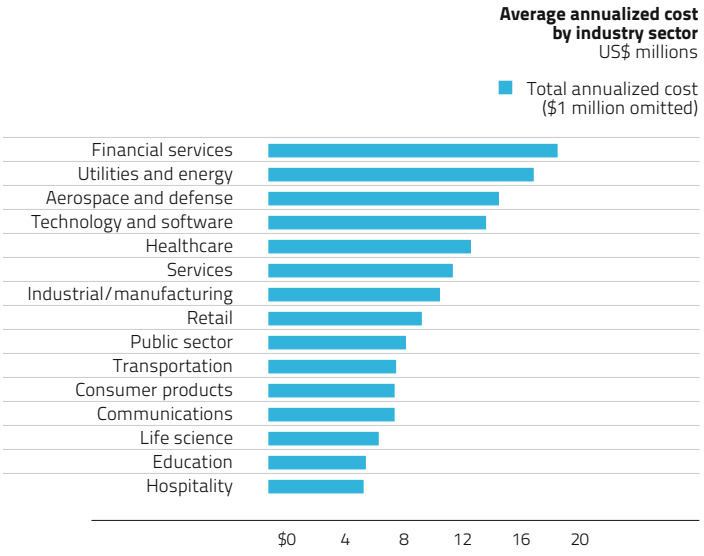
employees can access on mobile browsers without being connected to the main corporate network. If someone hacks their phone, it can't be used as a gateway into the main system. Symantec, a U.S.-based global cybersecurity company, acquired Fireglass in July 2017 for an undisclosed sum. Five days later, Symantec acquired another Israeli security start up called Skycure, which had raised $27.5 million in venture capital.

Skycure created a platform that combined crowd-sourced threat information and artificial intelligence in an attempt to predict and prevent attacks on mobile devices. After the acquisition, Skycure was renamed Symantec Endpoint Protection Mobile.

CounterCraft, a Spanish security startup founded in 2015 that has raised $2.6 million, sets various traps inside networks for hackers who break in, using another strategy called "deception," which assumes hackers will find a way to break-in. These include various apps that are placed on a smartphone or tablet that the owner knows not to touch or launch. But if someone steals the phone, or breaks in, and tries to launch or access one of these apps, they can release fake information, or do things like activate the phones' camera to snap a picture of the thief, or send out GPS coordinates, or turn on the microphone. "You have to be one step ahead of any threats, and we try to use concepts from counter intelligence," says David Barroso, co-founder and CEO of CounterCraft, a scheduled participant on the 4YFN conference cybersecurity panel. Still, the assumption remains that information will be stolen. Increasingly, that information is being used for things like accessing accounts, particularly financial accounts. The stolen data is used to create fake identities that mix information from various victims to create new personas that are then used to open fraudulent accounts.

Enter 4iQ, a startup launched in 2016 with a service that tracks the use of stolen personal identities that are traded on what is known as the "Dark Web." The company was founded by the Spanish developer Julio Casal, who previously launched another pioneering cybersecurity startup called AlienVault. That company, which was launched in 2007, was backed by Adara, as is 4iQ, which has raised $14 million. 4iQ CEO Monica Pal, who previously worked with Casal at AlienVault, says the mobile topography is only going to get more challenging for companies as employees turn to new gadgets and the lines between personal and business uses and applications blur. "The new perimeter is the individual," Pal says. "And the way the individual gets online is their mobile device."

FINANCIAL SERVICES HAS THE HIGHEST COST OF CYBERCRIME



Sources: Ponemon Institute and Accenture

CYBEREASON
UNITED STATES

WHAT IT DOES: Endpoint detection of attacks. Its technology finds a weakness in the attack and then designs a specific response to stop it.

https://www.cybereason.com/

TANIUM
UNITED STATES

WHAT IT DOES: Provides a dashboard that gives visibility and control over every device in a corporate network, with the aim of detecting any security issues within 15 seconds.

https://www.tanium.com/

CROWDSTRIKE
UNITED STATES

WHAT IT DOES: Analyzes endpoint events in real time using machine learning and human intelligence. It aims to detect active attacks at endpoints and disable attacks before a network break-in occurs.

https://www.crowdstrike.com/

SECURITHINGS
ISRAEL

WHAT IT DOES: Provides a platform that lets service providers monitor all activity across IoT devices in real time to detect threats.

https://securithings.com/

POUR NOS LECTEURS FRANCOPHONES

Pour recevoir chaque semaine un décryptage de l'actualité des nouvelles technologies, abonnez-vous à notre newsletter : http://innovator.news

Les Echos

Directeur de la publication, président de la SAS Les Echos
Francis Morel
Directeur des rédactions
Nicolas Barré
Directeur des développements éditoriaux du pôle Les Echos
Henri Gibier
Editrice
Bérénice Lajouanie
Directeur de création
Fabien Laborde

TheInnovator

Editor-in-Chief
Jennifer L. Schenker
jschenker@lesechos.fr
Publisher
Mathieu Fritsch
mfritsch@lesechos.fr
Artwork & Layout
Studio L'Eclaireur
Contributing Editor
Kimberly Conniff Taber
Contributing Journalists
Chris O'Brien, Leila Abboud, David Pringle

Head of Marketing and Distribution
Étienne Porteaux
Head of Strategy and Communication
Fabrice Février
Press relations
Karine Mazurier
kmazurier@lesechos.fr
(+33 1 87 39 73 92)

TEAMEDIA

PUBLICITÉ / ADVERTISING
Présidente **Corinne Mrejen**
Directrice générale
Cécile Colomb
ccolomb@teamedia.fr
(+33 1 87 39 75 08)
Directeur du pôle Réseaux, International et Régions
Nicolas Grivon
ngrivon@teamedia.fr
(+33 1 87 39 75 26)
Directeur commercial du pôle BtoB
Nicolas Danard
ndanard@teamedia.fr
(+33 1 87 39 75 10)
Directrice commerciale pôle Lifestyle & Culture
Anne-Valérie Oesterlé
avoesterle@teamedia.fr
(+33 1 87 39 75 45)

SERVICE ABONNEMENTS
LES ÉCHOS
4, rue de Mouchy 60438
Noailles Cedex
Du lundi au vendredi, de 9h à 17 h 30, au
01 70 37 61 36
serviceclients@lesechos.fr

FABRICATION
Directeur **Jérôme Mancellon**
Responsable fabrication groupe **Sandrine Lebreton**
Directeur de Production
Bruno Santin
Chargés de production
Naima Mansouri
Impression
NewsPrint, France

Origine du papier : Allemagne
Taux de fibres recyclées 42%
Le papier de ce magazine provient de forêts gérées durablement et est porteur de l'Ecolabel européen FI/11/011
Ptot : 0,004Kg/tonne

The Innovator est une publication éditée par Les Échos, SAS au capital de 794240 euros RCS Paris
582 071 437
ISSN en cours d'obtention
CPPAP: 04 21 C 83 015
Dépôt légal : novembre 2017
10 boulevard de Grenelle
CS 10817
75738 Paris Cedex 15
Tél. : +33 1 87 39 70 00

Groupe Les Echos

Principal associé Ufipar (LVMH)
Président-directeur général
Francis Morel
Directeur général délégué
Christophe Victor
Directeur délégué
Bernard Villeneuve

Credits photo :
Getty Images / Thinkstock