NUMBER 73 | DECEMBER 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

QUANTUM KEY DISTRIBUTION

It is quite common in recent years to find news about quantum computing in the media, however there are other “**quantum elements**” called to play an important role, which for the moment are not so common in the press. One of them is quantum key distribution (**QKD**). It is not for nothing that this year’s Nobel Prize in Physics went to the pioneers of quantum entanglement (one of those puzzling effects of quantum mechanics where two particles behave as a single unit even though they are separated), which is the basis of QKD.

QKD is a secure communication method, it implements a cryptographic protocol involving quantum mechanical components, and allows two parties to produce a shared random secret key that only they know, which can then be used to encrypt and decrypt messages. Quantum key distribution is only used to produce and distribute a key, not to transmit any message data.

What makes this method interesting, especially from a cybersecurity point of view, is an important and unique property of quantum key distribution, which is the ability of the two communicating users to detect the presence of any third party attempting to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics, i.e., the process of measuring a quantum system in general perturbs the system. For example, a third party trying to spy on the key must be able to measure it in some way, thus producing detectable anomalies, so in the quantum world, observing leaves a trace.

But QKD also has some drawbacks. For example, to deploy it, special optical equipment is needed for communications, either fibre optic or through free space, which makes the cost quite high.

In short, the main difference between QKD and classical means is the ability to detect any interception of the key. We will always know if we are being spied on, although we must be aware that at least for the time being, the actual security provided by a QKD system is nowhere near the theoretical full security of the laws of physics, but rather the more limited security that can be achieved by hardware and engineering designs.

We will have to keep an eye on developments, especially regarding initiatives for new QKD communication channels. One example is the **Caramuel project** (the first satellite mission in geostationary orbit for the distribution of quantum keys) involving 20 Spanish public and private institutions, where the exchange of keys would be carried out thanks to a geostationary satellite located 36,000 kilometres from Earth. The satellite sends photons in a special format to two stations equipped with telescopes, which receive them and share them with the two devices interested in communication. In this way, Spain is present in the European initiative to deploy the first quantum communications nodes in various countries of the European Union, which will be connected to each other via satellite.

Fernando Vilchis

Cybersecurity Director at NTT DATA México

CYBER NEWS

We begin our Cyber-Chronicles by talking about major sporting or cultural events, such as the World Cup in Qatar, which kicks off this November, and major commercial campaigns such as Black Friday or the Mexican Buen Fin, which promise the best deals on products and services and which will also take place this month, are the perfect breeding ground for cybercriminals who use phishing to try to take advantage of the most clueless customers.

This has been denounced by the airline Iberia on its Twitter account, indicating that a group of cybercriminals has launched a phishing campaign on its behalf encouraging customers to participate in fake sweepstakes to travel for free on its flights. This type of scam allows victims' data to be stolen.

> "The Emotet botnet refuse to die, after a four-month hiatus, it is back again".

Cybercriminals are also taking advantage of the upcoming World Cup in Qatar to launch their phishing campaigns. Cybersecurity firm ESET has already detected several scams in which cybercriminals are taking advantage of the upcoming sporting event.

In addition to the classic scams that seek to trick victims by telling them that they have won a prize, such as tickets or a trip to the World Cup, with the aim of stealing data or even money with the excuse of having to pay some kind of fee to receive the prize, the creation of numerous fraudulent websites has been detected. These websites impersonate legitimate World Cup-related sales or deliveries, trips, or services, with the aim of stealing both money and information.

In the face of this type of attack, the simplest and most effective measure is mistrust, and the main cybersecurity companies warn of the importance of paying attention to suspicious messages and advertisements, being wary of unsolicited communications, not clicking on links and avoiding downloading files that you do not trust.

In other news, the Emotet botnet refuses to die. After a four-month hiatus, it is back again and able to evade detection. In less than a year since a police operation shut down its original infrastructure, it is back in business.

Meanwhile, the French defence and technology group Thales has acknowledged being the victim of a cyberattack by the LockBit 3.0 cybercriminal group and that its data on the Dark Web has been compromised, although it has had no impact on its operations.

Another attack has taken place, but this time against the U.S. Federal Network, where they installed XMRig crypto-mining software, moved laterally to gain access to the domain controller (DC), compromised credentials and also deployed reverse proxies on several hosts in order to maintain persistence.

Cybercriminals do not take any time off. Recently, two Todo apps were discovered in the Google Play Store: Day Manager and Expense Keeper, which were embedded with a banking Trojan, Xenomorph. This Trojan steals credentials from banking apps and is able to intercept messages and SMS from infected devices, thus intercepting multi-factor authentication (2FA) codes and one-time passwords.

We conclude our Cyber Chronicle with two zero-day vulnerabilities (CVE-2022-41040 and CVE-2022-41082) confirmed by Microsoft that are being used together in campaigns to gain access to Microsoft Exchange servers and remotely execute code on compromised systems. They affect Microsoft Exchange Server versions 2013, 2016 and 2019.

THE PRICE OF YOUR DATA ON THE DEEP WEB

By: NTT DATA

We constantly hear and talk about the number of data thefts and data leaks or identity thefts that are growing exponentially nowadays. But what happens when data is stolen and what is it used for after such an attack? In this article, we will explain the causes and motivations for stealing and using this data on the internet.

How are personal data collected?

The personal data that travels through the Internet is one of the greatest sources of information and power that can be managed. It underpins the pillars of companies and at a personal level it enables them to carry out and facilitate transactions.

An example of this could be an online shop, since users need to give personal data such as: addresses, credit cards, identification documents...

The company needs this data to carry out its tasks.

What data is being traded?

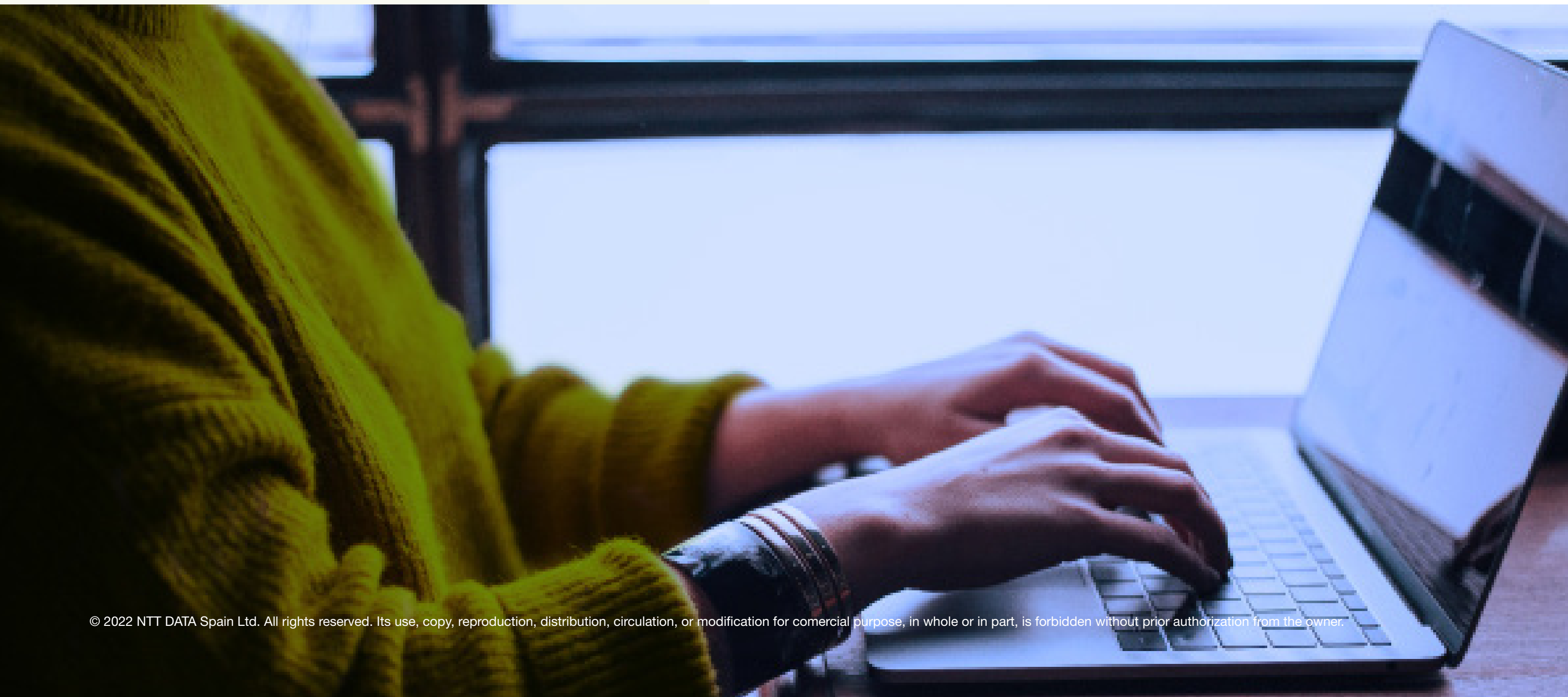
Over the last few years, the demand for data has remained the same as it was ten years ago. The main demand has been for bank details such as credit cards, but other types of data such as Netflix and Spotify accounts, personal medical records and selfies showing personal identification documents have also been in demand. Currently, cryptocurrency accounts and wallets are the most in demand.

The sale of all this data on the Deep Web poses a host of problems for the owners of this information, including corporate espionage, financial fraud and, in some cases, impersonation of friends, family and co-workers.

What is its price?

Having a wide range of different information, the trade in personal data is very broad and diverse, and as long as you have enough money, you can buy practically any type of information. Here is a list of the average prices for personal data:

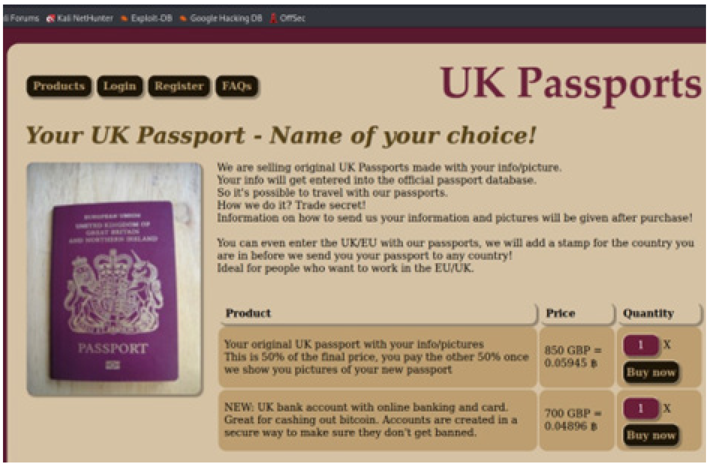
- Online Banking: 40 €
- Cards with data : 15€ to 30€
- Social media accounts (depending on followers): 75€ to 200€
- Cryptocurrency wallets: 300€ to 1000€
- Emails: 10€
- Spanish ID card : 120€ to 300€
- Passports: 600€ to 4000€
- Unfiltered lots extracted from companies: 50€ to 5000€



As can be seen from the price variations, these prices change depending on the power and or value of the data to be purchased.

An ID card to be able to impersonate someone and carry out illegal actions costs around €120 while a cryptocurrency account, depending on its content, ranges from €300 to more than €1000.

Accessing some of the pages published on the Deep Web we find sales of this type of information.



UK Passports

Your UK Passport - Name of your choice!

We are selling original UK Passports made with your info/picture.
Your info will get entered into the official passport database.
So it's possible to travel with our passports.
How we do it? Trade secret!
Information on how to send us your information and pictures will be given after purchase!

You can even enter the UK/EU with our passports, we will add a stamp for the country you are in before we send you your passport to any country!
Ideal for people who want to work in the EU/UK.

Product	Price	Quantity
Your original UK passport with your info/pictures This is 50% of the final price, you pay the other 50% once we show you pictures of your new passport	850 GBP = 0.05945 ฿	1 X Buy now
NEW: UK bank account with online banking and card. Great for cashing out bitcoin. Accounts are created in a secure way to make sure they don't get banned.	700 GBP = 0.04896 ฿	1 X Buy now

How to protect data

It is a personal responsibility to prevent our documents and data from ending up in the wrong hands and being sold to the highest bidder.

To maintain that security, we offer the following tips:

- Make sites and services earn your trust: Hackers get a lot of data by targeting websites and services where you share your personal information.

  You cannot personally secure the servers that store your data, but it is possible to think in your own interest.

  Make the security of your data a priority. If a site or service asks you for sensitive data, ask tough questions about how the company secures it and what it will do if your data is breached.
- Inform yourself: You can do a lot individually to protect your data. This will largely depend on where you spend your time online, but you can be proactive and research ways to stay secure on the devices and services you use.
- Be vigilant: Knowing how to protect your data is one thing but knowing how to react quickly and effectively when your sensitive data is used without your permission is another.
- Take control of your accounts: Request weekly bank statements or enable transaction notifications in your app. Activate security settings on all your accounts so you know when login attempts are made from suspicious devices. Make use of tools offered by the sites or services you use (a password manager, NordPass, for example, offers a password strength checker that will tell you if your personal password is present in any leaks).

TRENDS

The rise of automotive hacking

The rise of automotive hacking is on the rise, with this area becoming a new market for hackers as cars become more automated.

Car hacking has been difficult in recent decades because cars were designed to be protected from the outside by security measures such as steering wheel locks, door locks, immobilisers, and anti-tampering software.

These features were implemented to protect the car from thieves and prevent owners from gaining unauthorised access to the car's computer systems. Only a few people were able to study and learn about these safeguards, as it was difficult to have a real car to experiment with.

What is automotive hacking?

Automotive hacking is based on gaining unauthorised access to a vehicle's computer systems. This can include a stranger approaching and opening a car door, but a newer and more sophisticated method of gaining access is to connect wirelessly via Bluetooth or Wi-Fi. The most common problem associated with this type of access is that it overrides the car's security measures, but it is also a new way to disrupt normal vehicle functions, such as the car alarm, an oil change reminder or even the air conditioning or heating system.

Initially it was thought that the economic opportunities for cybercriminals were small because cars have little exploitable information, but controlling cars, especially autonomous vehicles, may have more worrying undertones such as creating traffic disruptions, spying on occupants, or being used in acts of terrorism. Still, as vehicles gain computing power, they may become victims of malware or even ransomware.

VULNERABILITIES

Citrix and ADC

CVE-2022-27510, CVE-2022-27513 and CVE-2022-27516

Date: 08/11/2022

Description. Citrix published a security bulletin on Tuesday in which it reports three vulnerabilities affecting Citrix Gateway and Citrix ADC. CVE-2022-27510 is the most relevant vulnerability, classified as critical, which allows bypassing authentication through the use of a different path. CVE-2022-27513, high criticality, allows taking control of remote desktop due to insufficient data verification, and CVE-2022-2751, medium criticality, which allows bypassing protection mechanisms against brute force login attacks.

Link: https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516

Affected Products. The affected products are the following:

- Citrix Gateway and Citrix ADC, version 13.1 prior to 13.1-33.47
- Citrix Gateway and Citrix ADC, version 13.0 prior to 13.0-88.12.
- Citrix Gateway and Citrix ADC, version 12.1 prior to 12.1-65.21.
- Citrix ADC 12.1-FIPS, versions prior to 12.1-55.289.
- Citrix ADC 12.1-NDcPP, versions prior to 12.1-55.289.

Solution: Update affected products to the latest available versions that fix the vulnerability.

OpenSSL v3

CVE-2022-3602 and CVE-2022-3786

Date: 04/11/2022

Description. OpenSSL has published a security advisory reporting two high criticality vulnerabilities whose CVEs are CVE-2022-3602 and CVE-2022-3786. Both vulnerabilities can cause buffer overflows when performing name constraint checking in X.509 certificate verification. Although the vulnerabilities were initially classified as critical, the severity is not so high as exploitation would require a CA to have signed the malicious certificate or, to continue certificate verification without having established a path to a trusted issuer.

Link: https://www.openssl.org/news/secadv/20221101.txt

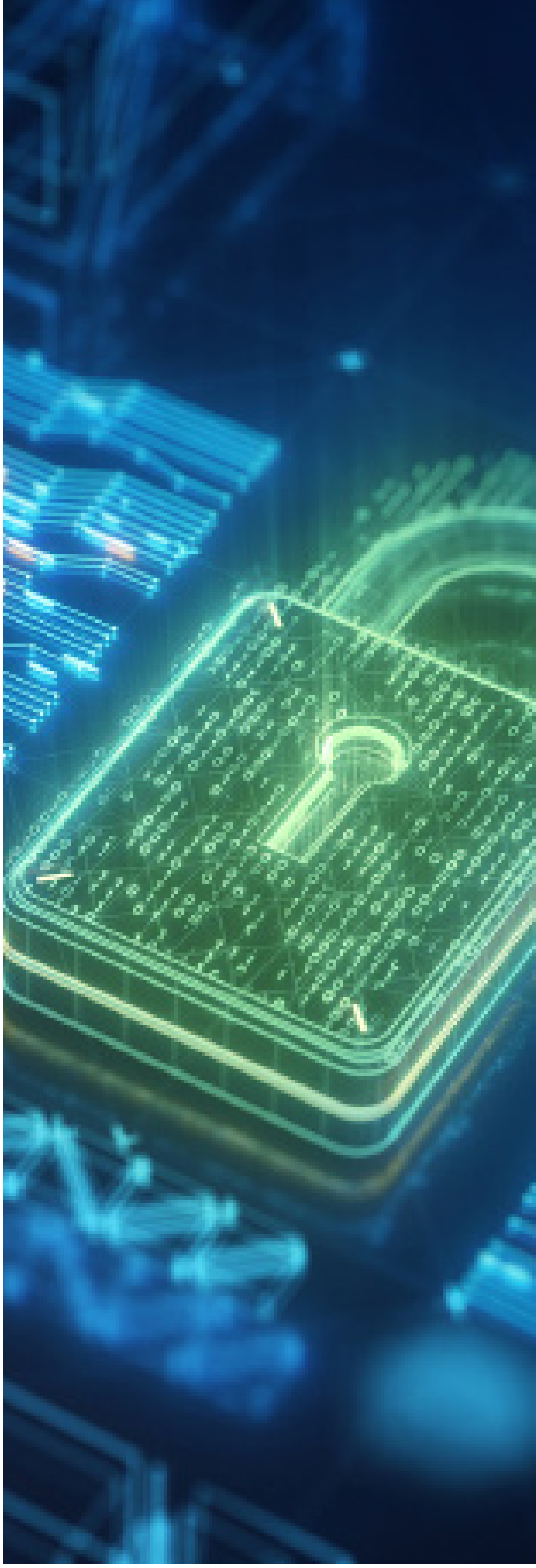
https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

Affected Products.

The vulnerabilities affect OpenSSL versions 3.0.0.0 through 3.0.6.

Solution: OpenSSL's solution is to update to the latest version, version 3.0.7. As a mitigation, OpenSSL recommends that users with TLS servers disable TLS client authentication until it can be updated.

PATCHES



Microsoft

Date: 08-11-2022

Description. Microsoft's November 2022 patch bulletin has been published, fixing 68 vulnerabilities. Six of these vulnerabilities correspond to 0-days that are being actively exploited. In addition, the patch includes fixes for Microsoft Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082, also known as ProxyNotShell, which were discovered at the end of September this year.

Link: https://msrc.microsoft.com/update-guide/releaseNote/2022-Nov
https://msrc.microsoft.com/update-guide/

Affected Products:
Windows 7, Windows 8.1, Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022

Solution: It is recommended to apply the patch available from Windows Update as soon as possible.

SAP Security

Date: 09-11-2022

Description. SAP has published its monthly update bulletin where several vulnerabilities have been fixed, including 3 of critical severity, affecting a multitude of its products. This includes 9 new security notes and updates to 2 notes published in previous months.

Link:https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10

Affected Products:

- SAP Manufacturing Execution, versions 15.1, 15.2 and 15.3
- SAP Commerce, versions 1905, 2005, 2105, 2011, 2205
- SAP BusinessObjects Business Intelligence Platform, versions 420 and 430
- SAP Business Objects Platform (MonitoringDB), version 430
- SAP SQL Anywhere, version 17.0
- SAP IQ, version 16.1
- SAP 3D Visual Enterprise Viewer/Author, version 9
- SAP Enable Now, version 10
- SAP Customer Data Cloud (Gigya), version 7.4
- SAP Data Services Management Console, version 4.2 and 4.3

Solution: Apply appropriate security updates.

EVENTS

XVI STIC CCN-CERT Conference

29 of november- 2 of december 2022 |

This international, entirely face-to-face event focuses on cyber security and cyber defence, as well as other digital technologies (robotics, big data, artificial intelligence, autonomous systems, and sensors) of key importance to defence.

Link: https://www.ccn-cert.cni.es/xvijornadas.html

Cyber Security & Cloud Expo

1 - 2 of december 2022 |

Public conferences where the latest developments and advances in the sector will be presented. The Cyber Security & Cloud Expo event, taking place 1-2 December 2022, will address the real issues facing today's CISOs and security professionals as modern enterprises evolve. We are showcasing the most innovative and important developments in the solutions market, with a focus on collaboration and support for the security community.

Link: https://www.cybersecuritycloudexpo.com/global/

V National Meeting of MetaRed TIC Argentina Universities

1 - 2 of december 2022 |

This meeting aims to bring together the heads of Information Technology and other areas related to the Digital Transformation of Higher Education Institutions in Argentina, in order to strengthen the collaboration that has taken place between their ICT areas, to present the work done in the last year and to generate debates and spaces for reflection to propose actions for cooperation in the difficult situation brought about by the pandemic.

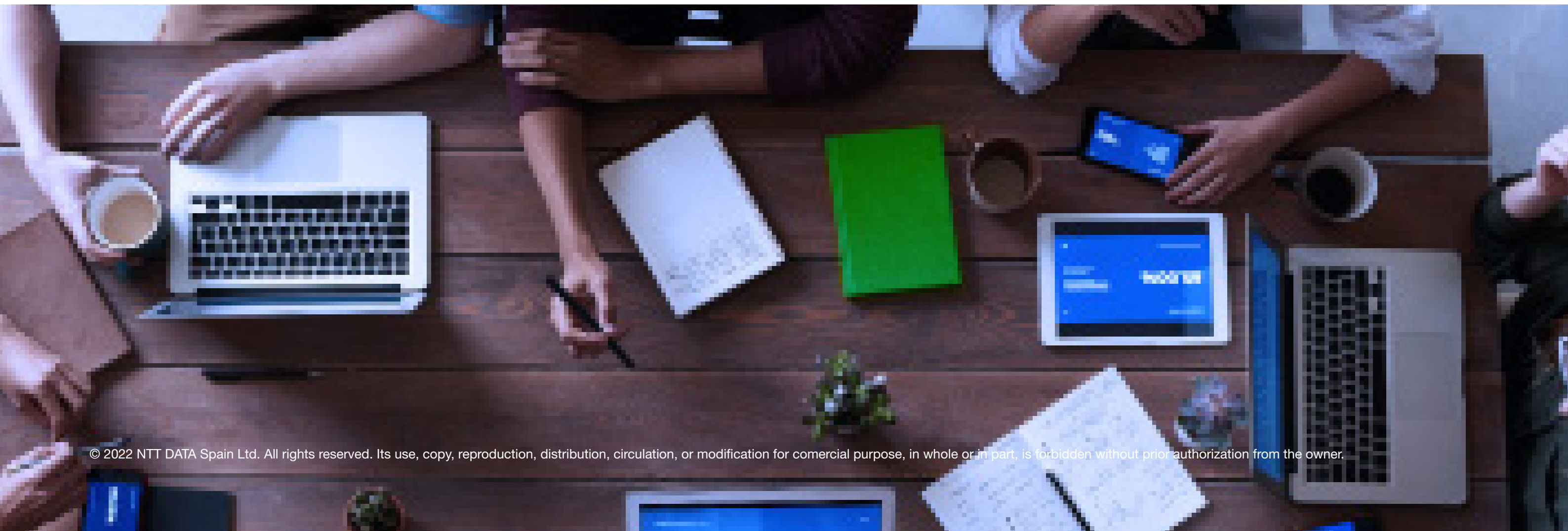
Link: https://eventos.metared.org/90939/detail/v-encuentro-nacional-de-universidades-metared-tic-argentina

SecureWorld West Coast Virtual

8 of december 2022 |

Public conference series with security leaders from a variety of sectors. For more than 21 years, SecureWorld conferences have been connecting, informing, and developing cyber security leaders through regional in-person events and interactive online platforms.

Link: https://events.secureworld.io/details/west-coast-2022/



RESOURCES

Tenable One

New tool from the manufacturer Tenable to manage the exposure surface of an organisation's assets, combining vulnerability analysis in on premise, cloud, and web application environments with integrated asset inventory management.

Link: https://www.tenable.com

TryHackMe SOC Level 1

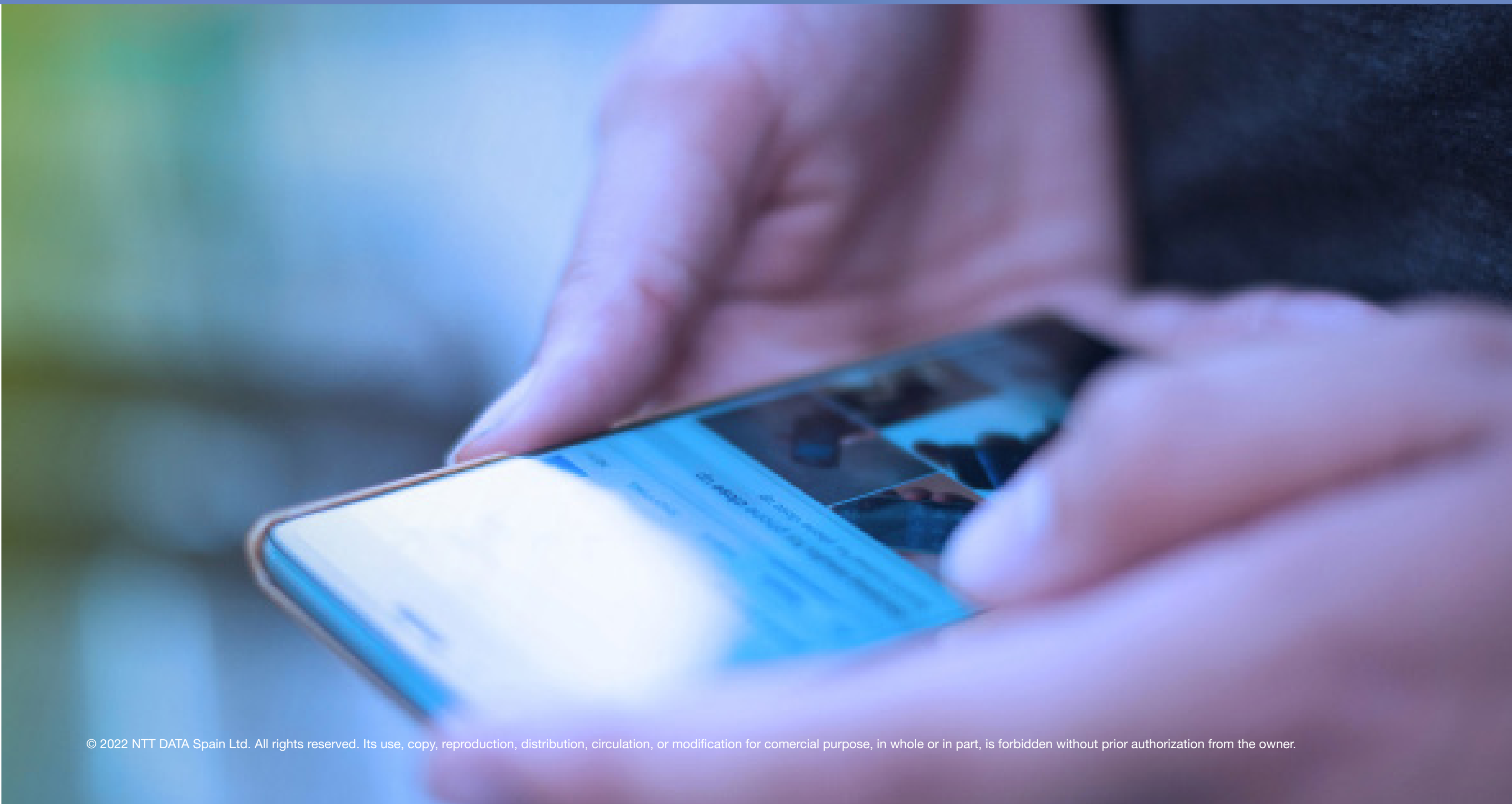
The TryHackMe platform has added new courses and learning modules, this time focusing on Blue Team skills development, such as Threat Intelligence, network traffic analysis, incident response and forensics.

Link: https://tryhackme.com/path/outline/soclevel1

Workshop: Learn cryptography with the Crypto Go game

The aim is to familiarise participants with basic concepts of computer security (confidentiality, integrity, authentication) and symmetric cryptography. The need to raise awareness of the importance of security in digital communications, the risks that exist, and how to protect ourselves from these risks will be presented.

Link: https://eventos.uc3m.es/90402/detail/taller-aprende-criptografia-con-el-juego-crypto-go



RESPONSABLES CIBER

María Pilar Torres Bruna

Cybersecurity Director at NTT DATA Latam y Perú

maria.pilar.torres.bruna@emeal.nttdata.com

Andrea Thome

Cybersecurity Director at NTT DATA Brasil

andrea.thome@emeal.nttdata.com

Javier Mauricio Albarracin

Cybersecurity Director at NTT DATA Colombia

javier.mauricio.albarracin.almanza@emeal.nttdata.com

Fernando Vilchis

Cybersecurity Director at NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Cybersecurity Manager at NTT DATA USA

nestor.ordonez.ramirez@emeal.nttdata.com

Carolina Pizarro

Cybersecurity Director at NTT DATA Chile

carolina.pizarrodiaz@emeal.nttdata.com

NTT DATA
Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com