NUMBER 72 | NOVEMBER 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

THE IMPORTANCE OF INVESTING IN CYBERSECURITY

With European Cyber Security Month (ECSM) now over, we reflect on the trends around which the activities planned for the tenth anniversary of this campaign have been developed: phishing attacks and ransomware. It is not surprising that these, and not others, are the two cyberthreats chosen to promote and enhance cybersecurity awareness among citizens and organisations during this month.

According to “The Global Risk Report 2022”, published by the World Economic Forum, 95% of cybersecurity problems stem from human error. Cybercriminals are aware of this problem and are increasingly developing more sophisticated and personalised campaigns that try to take advantage of citizens and employees to gain access to sensitive information that allows them to commit fraud, gain access to an organisation or even cause a cyber incident by infecting systems with ransomware. It is therefore essential to ensure that both end users and organisations are well informed about these cybersecurity risks and know how to identify and respond appropriately to any suspicious email, SMS, call, link, or website to avoid falling victim to either of these two cyberthreats.

Furthermore, not only is it important to promote training and awareness among employees and end-users, but organisations must also invest in the implementation and adaptation of security systems, drills, and procedures to prevent this type of threat, as failure to do so can lead to significant financial and reputational damage down the line.

That is why, at **NTT DATA**, we help our clients to be prepared thanks to our cybersecurity training actions, to the monitoring of their exposure surface, identifying the cyber threats that may pose a greater risk to them. This is conducted through threat intelligence techniques, pentesting and network team exercises to simulate a real attack and identify if they have adequate monitoring and detection systems in the organisation. In addition, we develop action and recovery plans for security incidents that can help them to contain and/or mitigate the attack.

Carolina Pizarro Díaz

Cybersecurity Director at NTT Data Chile

CYBER NEWS

We kick off our cyber-chronicle with the statement published by Uber on 16 September 2022, in which they reported a serious security incident. In this publication, they reported a cyber-attack that has seriously affected their critical infrastructure. However, Uber claims that there is no evidence that the incident involved access to users' personal data.

The attacker has reportedly gained access to Uber's credentials on Amazon Web Services (AWS), although this is not yet confirmed. However, according to the screenshots provided by the cybercriminal himself, he appears to have gained full access to IT systems, including security software and the Windows domain. It is suspected that the attacker gained access by relying on a company employee to gain access to the VPN.

> "The hotel chain IHG has been affected by a cyberattack for using Qwerty1234 as a password in its databases".

Zoom, on the other hand, has detected several security flaws in the Zoom On-Premises Meeting Connector MMR resource (versions prior to 4.8.20220815.130) that would allow unauthorised access to meetings.

Also noteworthy is the phishing campaign (based on EvilProxy) detected by Proofpoint. This campaign aims to steal Microsoft account credentials by taking advantage of the death of Queen Elizabeth II. To do so, they offered a platform for signing a supposed book of condolences, thus taking over her data and attempting to steal the multi-factor authentication (MFA) codes to take control.
In other news, The European Commission has unveiled a proposal for common rules to protect European consumers when purchasing electronic devices, both at the time of purchase and during their lifetime.

New vulnerabilities have been found in Ezviz cameras as well, which could allow an attacker to control the camera, download images and execute code remotely, affecting more than 10 million devices.

Revolut, a financial technology company, has suffered a data breach affecting 0.16% of its users (50,000 accounts, estimated 20,687 users at European level). In addition, the company's system has been affected, displaying unprofessional chat messages.

It is worth highlighting the rapid response of the technicians in identifying and isolating the attack immediately, preventing funds, accounts, and cards from being affected, and thus significantly reducing the impact.

The attack, according to experts, may have relied on social engineering techniques, although they have not detailed the method.

Another surprising news is the cyber-attack on the hotel chain IHG, as they apparently used Qwerty1234 as a password in its databases. The attack relied on social engineering tactics to gain access to the internal network. Fortunately, the company managed to secure the servers at the last minute before the cybercriminals finished implanting ransomware to encrypt the data and demand a ransom. However, the attackers were able to permanently delete data, including files, documents, and information, making the service unavailable. In addition, a certain amount of information was exfiltrated, such as corporate data and email logs.

Several simultaneous malware (formbook) campaigns have also been detected that impersonate DHL and TNT mainly for the theft of credentials typed by the user or stored in browsers, mail clients, FTP clients and VPNs.

On the other hand, there has been an attack on the information systems of the Consorci Sanitari Integral de Salut de Catalunya (Integral Health Care Consortium of Catalonia). Following the cyber-attack, three large hospitals were affected, as well as several private care centres.

As for this month's chronicles related to the Russian-Ukrainian war situation, the Ukrainian Ministry has warned that Russia is planning cyberattacks targeting power supply facilities in the east and south of the country. The aim would be to rely on the impending winter, thus gaining a head start on the invasion. Ukraine also warns its closest allies (Polynesia, Estonia, Latvia, Lithuania, Finland, Sweden, Germany, and Denmark) of Russia's intention to increase DDoS attacks on their critical infrastructure.

In addition, the Russian group Anonymous attacks the websites of major banks, airports, taxi services and accommodation providers in Slovakia over Slovak support for Ukraine's NATO membership.

It has also perpetrated attacks against the identification service created by the Defence Manpower Data Centre (DoD Self-Service Logon) targeting several US government agencies.

Given the news presented throughout this article, and the current war situation in Ukraine, cyber-security precautions should be taken more than ever, with several factors in mind at all times:

- There is no such thing as 100% security
- Security is a process, not a product.
- Security will always be as strong as the weakest link; usually the user.

AI IN CYBERSECURITY

By: NTT DATA

As we have already heard on numerous occasions, the number of security incidents in information systems has increased dramatically in the last two years. This is due both to the current global circumstances and to the rapid evolution of the technologies used in these systems, as well as the emergence of new ones. This situation raises the issue that the tools, protection measures and processes to prevent and mitigate cyber-attacks must be equally modernised and able to cope with them in terms of both complexity and volume.

Challenges

Cybersecurity therefore faces, among others, the following challenges:

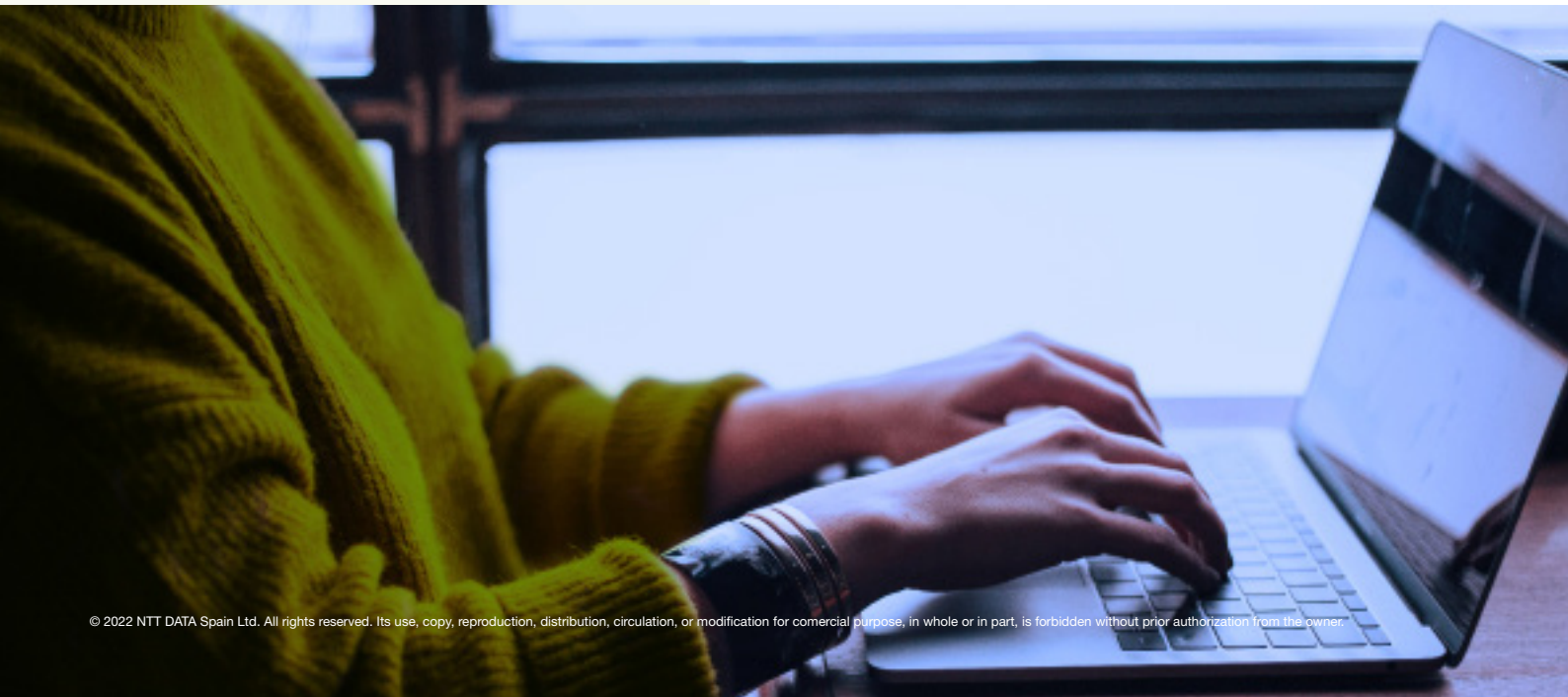
- **Vulnerability detection:** Agility in continuous software delivery (CD) is a determining factor in vulnerability detection, as bottlenecks can occur, especially during manual filtering of false positives from *AST tests. Coupled with this agility and the growing volume of threats mentioned above, the quality of detection may become compromised.
- **Threat hunting:** More oriented to threats in the organisation's infrastructure, but similar to the previous point. Carrying it out manually may not be cost-effective, either financially or in terms of time. In addition, as with vulnerability detection, as it requires more effort on the part of the cybersecurity analyst given the volume of threats, human error in detection is more likely to occur, resulting in a greater number of incidents going undetected.
- **IP obfuscation:** On the attacker side, usually in cyber security incidents the perpetrators use various tools (VPNs, proxy servers, TOR browsers, etc.) to cover their tracks. This makes it very difficult to identify those responsible.

A key concept in dealing with these challenges is artificial intelligence (AI), which gives autonomy to those tools that make use of it, ideally no longer relying on auditors to carry out the work of detecting weaknesses and incidents in information systems.

DevSecOps

Emphasising the first point, one area of cybersecurity where AI is making great strides is DevSecOps. This branch of cybersecurity works on establishing automatic controls within the software development lifecycle, so that development teams can obtain information on the security status of their applications and have the ability to fix identified vulnerabilities before taking them to production. This type of control is established in CI/CD (Continuous Integration / Continuous Delivery) environments and the following types, among others, can be distinguished:

- **SAST** (Static Application Security Testing): Identifies vulnerabilities in the application by analysing its source code.
- **SCA** (Software Composition Analysis): Identifies known vulnerabilities in third-party libraries used by the application.
- **DAST** (Dynamic Application Security Testing): Identifies vulnerabilities by performing security tests directly against a deployed instance of the application.
- **Detection of secrets** (passwords, API keys...) included in source code.



Some of these controls are based on certain rules set by the auditors or by the automated tools themselves and may therefore in some cases lead to false positives due to, for example, looking for a certain pattern in the source code.

Another reason for the emergence of the DevSecOps field, in addition to having the ability to correct vulnerabilities before deployment, is the large volume of applications that companies tend to have that need to be analysed.

By introducing these analyses in CI/CD, it is possible to reduce the time that auditors spend manually analysing applications and even automate the reporting of identified vulnerabilities. However, the aforementioned existence of false positives in these analyses means that development teams have to filter the results obtained in order to solve those findings that are actually real vulnerabilities, in some cases leading to a loss of trust in the security team and even giving rise to situations in which the much-needed collaboration between teams disappears.

Furthermore, false positives also make it difficult to have a clear vision of the risk to which the application or the company is exposed, as well as the proper management of that risk.

All the problems arising from the existence of false positives can be mitigated to a large extent by using AI to filter out findings from automated tool analysis. This would only report real vulnerabilities that the development team needs to address to mitigate the risk associated with them.

In addition, the security team will be able to more efficiently manage the risk to which the company is exposed without requiring manual reviews to verify it.

Problems

While AI is a powerful tool in the field of cybersecurity, there are also a number of disadvantages that need to be taken into account:

- The amount of hardware resources that companies must allocate to adopt it is significant, as it is a technology whose use requires memory and CPU power, as well as mechanisms to provide it with the data sets that train it and improve the quality of the process it carries out.
- Just as defence mechanisms can make use of AI, so can attackers. The more effective and automatic incident and vulnerability detection mechanisms become, the more complex the attacks become.
- Related to the previous point is the concept of neural fuzzing, the practice of providing an AI with massive volumes of data in order to find vulnerabilities in the process it performs. This can be used by attackers to gather information that allows them to exploit a protected system. However, it is worth noting that this same concept can be used to harden the AI itself, as demonstrated in this article from Microsoft.

Conclusions

There is no doubt that AI is here to stay in cybersecurity, as well as in many other areas, as it provides autonomy and automation in a context where speed in processing large volumes of data is key.

Moreover, it should be noted that these advantages also apply to the other side, making their adoption increasingly inevitable when it comes to keeping a company protected against the latest developments in cybercrime.

TRENDS

Scams on offer

This is the time of the year when the offers start with Christmas in mind. We all want to save money and if by moving up our Christmas shopping a little earlier we can do so, so be it.

For the last decade, Black Friday has taken place on the fourth Friday of November, a day in which the offers seek to increase consumption considerably with irresistible discounts. It has been so successful that it has been extended to cover the entire weekend and ends on the following Monday with Cybermonday, which is more focused on online sales.

It is at this time that cybercriminals take advantage of the situation and try to trick users to steal their information.

These scams are commonly carried out by creating fake websites or applications, capturing the attention of users through social media ads. These fraudulent pages often resemble other trusted pages, using similar content and domains, but with minimal changes that are hard to see.

Once they have managed to trick the user, the cybercriminals could have stolen the purchase amount, personal and payment method information and even infected the victim's device by simply accessing the site or downloading an application via the site.

Some common signs that may allow the user to identify a scam are the use of heavily discounted prices (more than usual), contact options limited to everyday email accounts rather than corporate emails, or URLs with strange words or characters.

Finally, there are a number of recommendations to keep in mind for the upcoming offer season¬:

- Check offers carefully and do not rely on prices that are too low or even free.
- If you find a very cheap product on one website, compare the price with other similar websites, which should change slightly but not make too big a difference.
- Be wary of unknown websites and only buy through official websites, where there is a guarantee of return and management of the product.
- Never give out your credit card PIN, as it is not necessary for online purchases.
- You could simply go to the physical shop and make the purchase there.

Let us be careful and act wisely to avoid being charged more for trying to save more.

VULNERABILITIES

OpenSSL

CVE-2022-2068
Date: 01/10/2022

Description. A script distributed by some operating systems has been discovered in such a way that it executes automatically. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. The use of the c_ rehash script is considered deprecated and should be replaced with the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1. 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

Link: https://www.ccn-cert.cni.es/component/vulnerabilidades/view/33748.html
https://www.suse.com/security/cve/CVE-2022-2068.html

Affected Products. The affected product versions are as follows: OpenSSL 3.0.4, OpenSSL 1.1.1 and OpenSSL 3.0

Solution: The manufacturer has released the following patches to mitigate these vulnerabilities: OpenSSL 3.0.5 and OpenSSL 1.1.1

Microsoft Exchange

CVE-2022-41040;41082
Date: 03/10/2022

Description. Microsoft Exchange Server 2013, 2016 and 2019 are at risk for two unpatched zero-day vulnerabilities CVE-2022-41040 (server-side request forgery) and CVE-2022-41082 (remote code execution via PowerShell).

Fortunately, an attacker needs authenticated access to the vulnerable Exchange server to successfully exploit any of the vulnerabilities. In addition, they must be able to execute PowerShell scripts (remotely), but then have the option to elevate privileges.

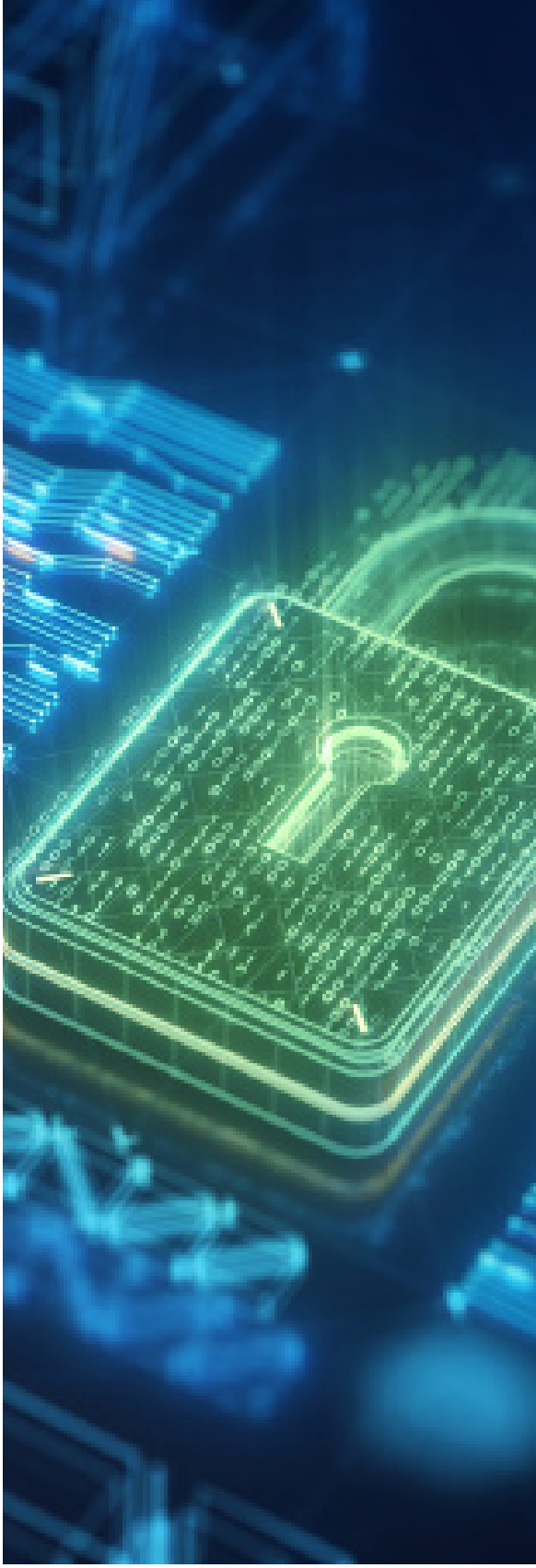
Link:https://borncity.com/win/2022/10/04/exchange-server-microsofts-0-day-schutz-aushebelbar-neue-einschtzungen-3-oktober-2022/

https://nvd.nist.gov/vuln/detail/CVE-2022-41040

Affected Products.
Exchange 2013, 2016 and 2019 (11, 12, 22 and 23).

Solution: Zero-day, no patches at present.

PATCHES



Android

Date: 01-10-2022

Description. The October Android security bulletin has been published, detailing multiple vulnerabilities of critical, high, and moderate severity affecting the Android operating system.
The most critical vulnerability affects the Framework component, which could lead to local privilege escalation on affected systems.

Link: https://source.android.com/docs/security/bulletin/2022-10-01

Affected Products:
Android Open Source Project (AOSP) ; versions 10, 11, 12, 12L y 13.

Solution: It is recommended to check that the manufacturer of the affected device has issued a security patch and install the latest updates from the “Settings” > “System” > “System Updates” menu.

Cisco

Date: 01-10-2022

Description. A vulnerability in the authentication functionality of the Cisco Wireless LAN Controller (WLC) AireOS software could allow an unauthenticated adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient error validation. An attacker could exploit this vulnerability by sending manipulated packets to an affected device. Successful exploitation could allow the attacker to cause the wireless LAN controller to crash, resulting in a DoS condition.

Link:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-mKGRrsCB

Affected Products: Cisco WLC AireOS 8.9 and 8.10

Solution: Install firmware versions 8.10.171.0 or higher.

EVENTS

Dual-Use Technologies 2022

17 - 18 of november 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.cde.ual.es/conferencia-europea-en-malaga-tecnologias-de-doble-uso-2022-ciberseguridad-y-aplicaciones-digitales-en-defensa/

No cON Name Congress 2022

24 - 26 of november 2022 |

No cON Name (NcN) is the oldest computer security and hacking conference in Spain. The annual event brings together promising newcomers to the sector, experts, as well as professionals in the field of computer science in general, telematic networks, programming, or software protection engineering.

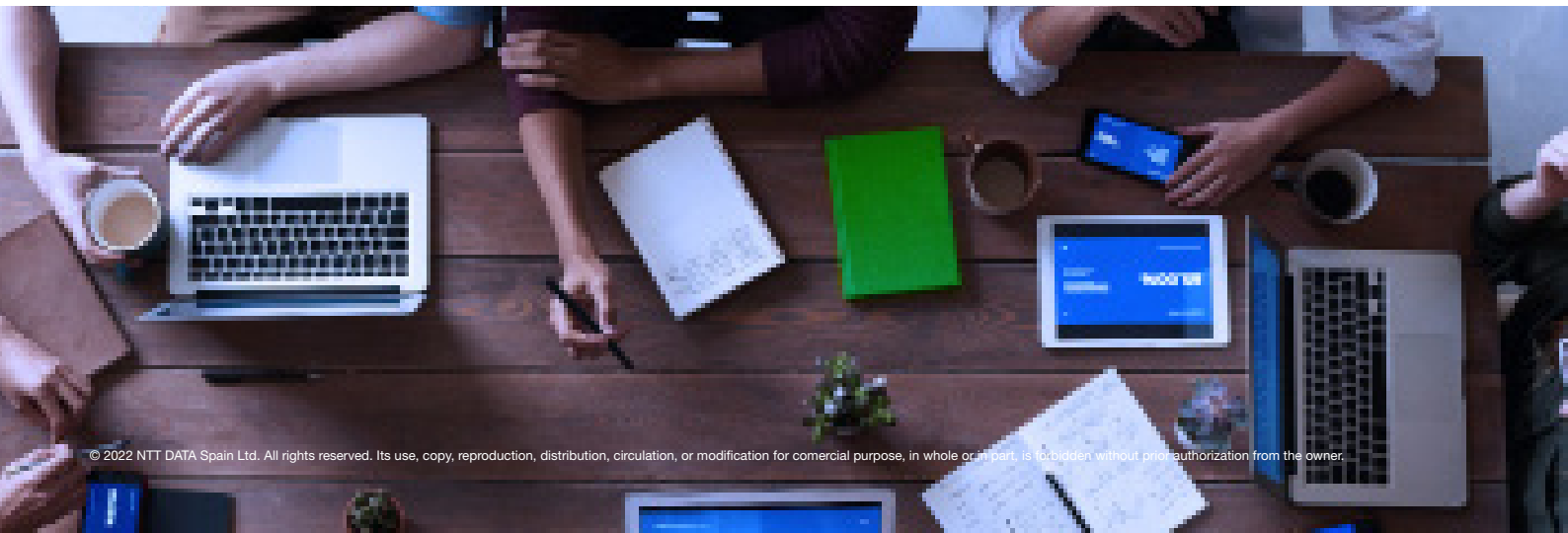
Link: https://www.noconname.org/

8th Annual e-Crime & Cybersecurity Spain Congress

15 of november 2022 |

The 8th e-Crime & Cybersecurity Spain Congress will analyse how new business models are pushing under-resourced security teams to the limit.

Link: https://akjassociates.com/es/event/spain



RESOURCES

Sophos Cloud Workload Protection

Tool that provides lightweight, increased visibility into on-premises environments, data centres and cloud-based Linux hosts and containers, protecting them from the most advanced cyber threats before they can gain a foothold in the environment.

Link: Sophos Cloud

Cyber Guardian

Innovative cybersecurity platform to help protect SMEs. At the same time, the tool offers protection for all company devices by monitoring, detecting, and removing known and unknown viruses, ransomware, Trojans, and spyware. It also helps to detect possible security flaws on websites. This service proactively monitors 24/7 security alerts.

Link: Cyberguardian

Cybereason MDR

Mobile detection and response application, which provides SOC-like monitoring capabilities. The application uses a malicious operation detection engine (MalOP) to generate a detailed report of an active hacking operation, how it relates to the MITRE ATT&CK framework and its threat level.

Link: Cybereason

INCIBE's Hacker Academy

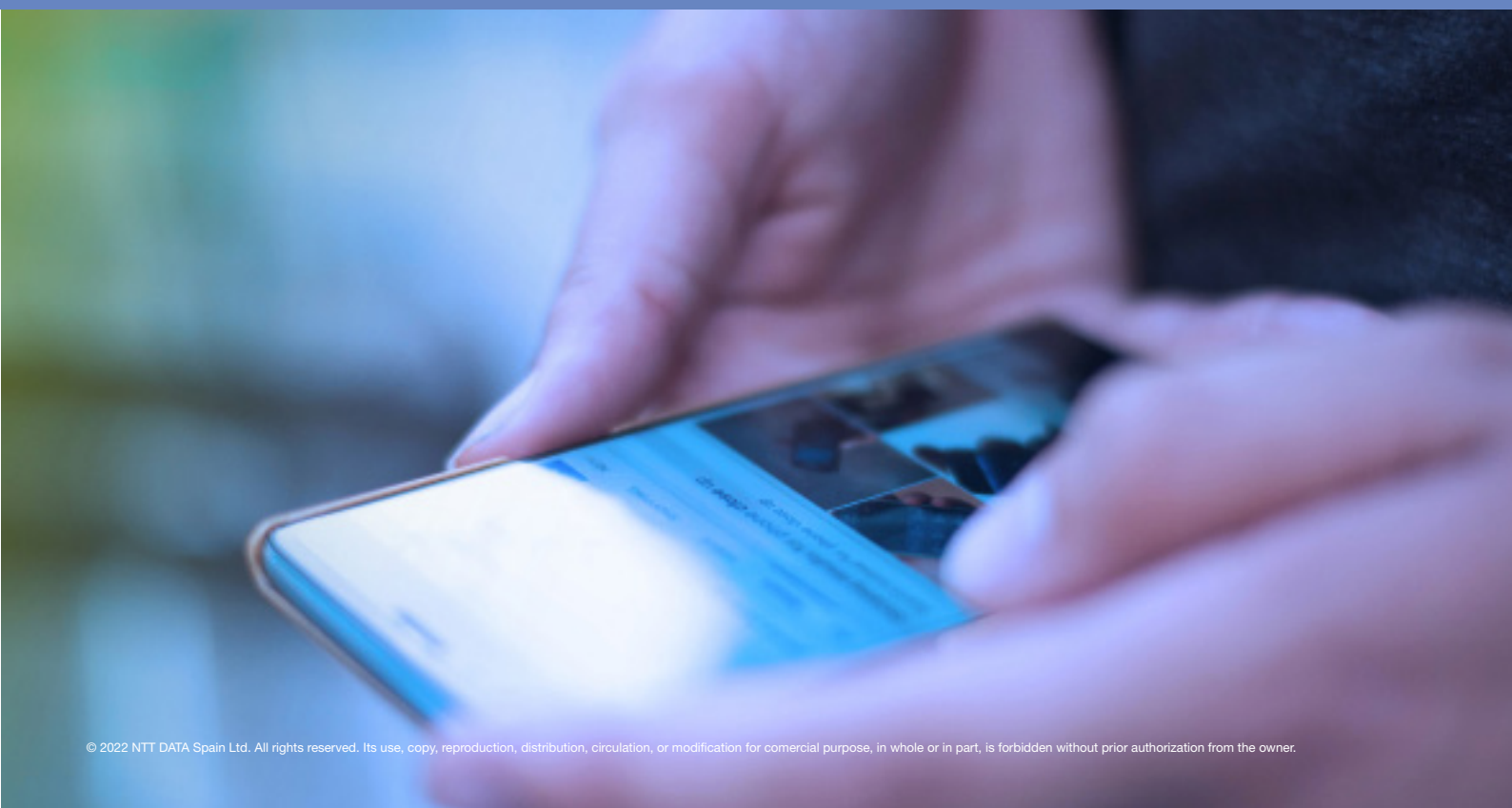
The Spanish National Cybersecurity Institute (INCIBE), under the Ministry of Economic Affairs and Digital Transformation, through the Secretary of State for Digitalisation and Artificial Intelligence, launches the second phase of publication of technical challenges in the Hacker Academy. This will continue to bring the cybersecurity profession closer to society in a practical and entertaining way, especially to the young public, with the aim of awakening their interest in a sector with a great future projection and numerous professional opportunities. In this second phase, which will run until 12 December 2022, two challenges per week will be published, at intermediate and advanced levels.

Link: Hacker Academy

Checkmarx API Security

New application of the Checkmarx One security platform. The application addresses security issues early in the software development lifecycle. Key features include the ability to automatically identify API endpoints; discovery of newly created or updated APIs as source code is registered or compiled by developers; automatic comparison of an application's APIs with its documentation to identify unknown APIs; and remediation capabilities designed to allow security professionals and developers to prioritise remediation of API vulnerabilities and OWASP (Open Web Application Security Project) risks.

Link: Checkmarx



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