NUMBER 81 | AUGUST 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

CYBERSECURITY: A STRATEGIC OBJECTIVE

In today's digital age, cyber security has become a vital strategic objective for individuals, businesses, and governments around the world. As technology advances and our lives become increasingly dependent on computer systems and interconnected networks, so do the risks associated with information security and the protection of sensitive data.

In this context, cyber security has become fundamentally important and strategic, both individually and globally, for a number of reasons.

1. Firstly, due to the exponential growth of cyber threats. Cybercriminals have developed sophisticated techniques to infiltrate computer systems and networks, stealing sensitive information, damaging digital infrastructure, and causing significant disruptions to our day-to-day operations. These attacks can have devastating consequences, both economically and politically. From identity theft and financial fraud to sabotage of critical infrastructure or cyber espionage, the risks are multiple and constantly evolving. Therefore, these attacks must be prevented and mitigated, safeguarding the interests of organisations and nations.
2. Secondly, due to the increase in global interconnectivity. Today, we are more connected than ever before, thanks to the expansion of the internet and digital networks. This has obviously created new opportunities for commerce, collaboration, and communication, but it has also created a larger, more complex, and dynamic attack surface for cybercriminals. Organisations and governments are increasingly dependent on information and communication technologies to conduct their daily business. Cybersecurity has therefore become a strategic component to protect the integrity, confidentiality, and availability of data in such a globally interconnected environment.
3. Third, because of the political and geopolitical implications. Cyber-attacks can have consequences beyond the economic sphere, affecting national security and international relations. Governments and organisations must protect their critical infrastructures (power grids, transport systems, communication networks, etc.) from possible cyber-attacks that could jeopardise a country's stability and security. In addition, state and non-state actors can use cyberspace as a tool for espionage, disinformation, and political influence. Cybersecurity is therefore necessary to protect national interests and ensure geopolitical stability.
4. Fourth, because of the protection of privacy and individual rights. As we increasingly collect and share personal information online, it is critical to protect privacy and ensure that sensitive data does not fall into the wrong hands. Individuals have the right to maintain control over their information and to be protected against identity theft, online harassment, and other forms of online abuse. Cybersecurity must therefore safeguard trust in the digital world and protect people's fundamental rights and freedoms.

In short, we are facing a scenario where cybersecurity is embedded in our lives, both in a personal and professional sphere, and is key and strategic in our digital society. The growth of cyber threats, global interconnectivity, political and geopolitical implications, as well as the protection of privacy and individual rights, have driven the need to prioritise it in the digital sphere. This is why organisations and governments alike must invest in effective cybersecurity measures to protect themselves and individuals against cyber-attacks and ensure trust and stability in the ever-evolving digital world.

Enrique Bernao Rosado

Cybersecurity Manager at NTT DATA Europe & Latam

CYBER NEWS

In this edition, we will discuss the rise of new entry vectors that are emerging as a result of the creation of new tools based on artificial intelligence and other innovations, with an emphasis on the well-known browser extensions.

Entry vectors in cybersecurity refer to access points to systems and networks that can be exploited by cybercriminals to carry out malicious attacks.

From artificial intelligence to blockchain and even cloud computing, these innovations are transforming entire industries and opening up an unprecedented range of possibilities. However, along with technological progress also come challenges related to security. Artificial intelligence has been booming during 2023.

> “the Spanish National Cybersecurity Institute warns that malicious users could use ChatGPT for criminal purposes”

As a result of the appearance of ChatGPT, a multitude of tools are appearing that use artificial intelligence, and among these are browser extensions and web applications that allow tasks to be carried out much more quickly (searching for information, writing specific texts, photo retouching, etc.). However, this increase in the appearance of tools also means an increase in the risk of some of these applications containing malware that can access information on our device.

Recently, security experts from the company Kolide have conducted a study showing that many of these AI extensions are designed to steal information from users (something that is not new, but as we have said, there is a massive trend at the moment in the use of this type of tool).

In March 2023, guard.io analysed and reported a tool called “Quick access to Chat GPT” which was hijacking users’ accounts by capturing their browser cookies. Google is reacting in the case of its browser (Google Chrome) to quickly filter and remove these tools from its extensions marketplace, however, the high demand for these tools makes it a complex task to detect all the malicious applications that come out every day and are available to users. The risk is also mostly that, during the time it takes for browsers to remove these extensions, a large number of users may be downloading, installing, and promoting the use of these tools.

Another important aspect is the attempt to develop an extension or tool in an agile and fast way in order to get to market first. This means that many applications, although not developed with malicious intent, contain many code vulnerabilities, since in this agile development process, security coverage is often overlooked, thus producing a large number of weaknesses in terms of privacy. That said, it is particularly important that, when adding an extension to our browser, we make sure that the source that has developed this tool is reliable and that it has the approval of the entities that distribute it.

If we talk directly about the use of ChatGPT, the Spanish National Cybersecurity Institute warns that malicious users could use ChatGPT for criminal purposes, since, as with other tools, “there are several attack vectors that cybercriminals can take advantage of to exploit vulnerabilities and attack potential victims”.

Although ChatGPT is equipped with security protocols that prevent it from responding to certain malicious requests and questions, it can allow someone without technical knowledge to develop scripts and perform attacks of all kinds, circumventing the existing restrictions. In addition, and returning to the subject of tools and extensions, many of these applications can help the user for these purposes, by rewording their questions or performing tests that allow these controls to be breached.

INCIBE pointed out: “By relying on the tool, cybercriminals could obtain more specific information about the company they want to attack. In this way, they manage to make the message more credible and there are more chances for the victim to “take the bait”” referring to impersonation and phishing attacks.

In short, and as is the case every time a modern technology comes onto the market, new vulnerabilities and attack vectors are appearing. This will lead to new security requirements when developing, analysing, and publishing tools that contain these technologies. Once again, a race between cybercriminals trying to exploit vulnerabilities and cybersecurity experts trying to protect users from them.

SECURITY AND MALWARE ON SMART DEVICES

By: NTT DATA

In the age of connected technology, smart devices have become an integral part of our lives. From smartphones and smartwatches to internet-connected TVs and home appliances, these devices offer us convenience and efficiency in our daily tasks. However, along with the benefits they provide, there is also a growing concern: smart devices have become targets for cybercriminals. In this article, we will explore this concern and discuss why it is important to be aware of the risks associated with these devices.

The rise of smart devices

The rise of smart devices has been impressive in recent years. The interconnectivity of devices has led to the creation of the Internet of Things (IoT), which allows multiple devices to communicate and share information with each other. This has improved the way we live, giving us greater control and remote access to our belongings and services.

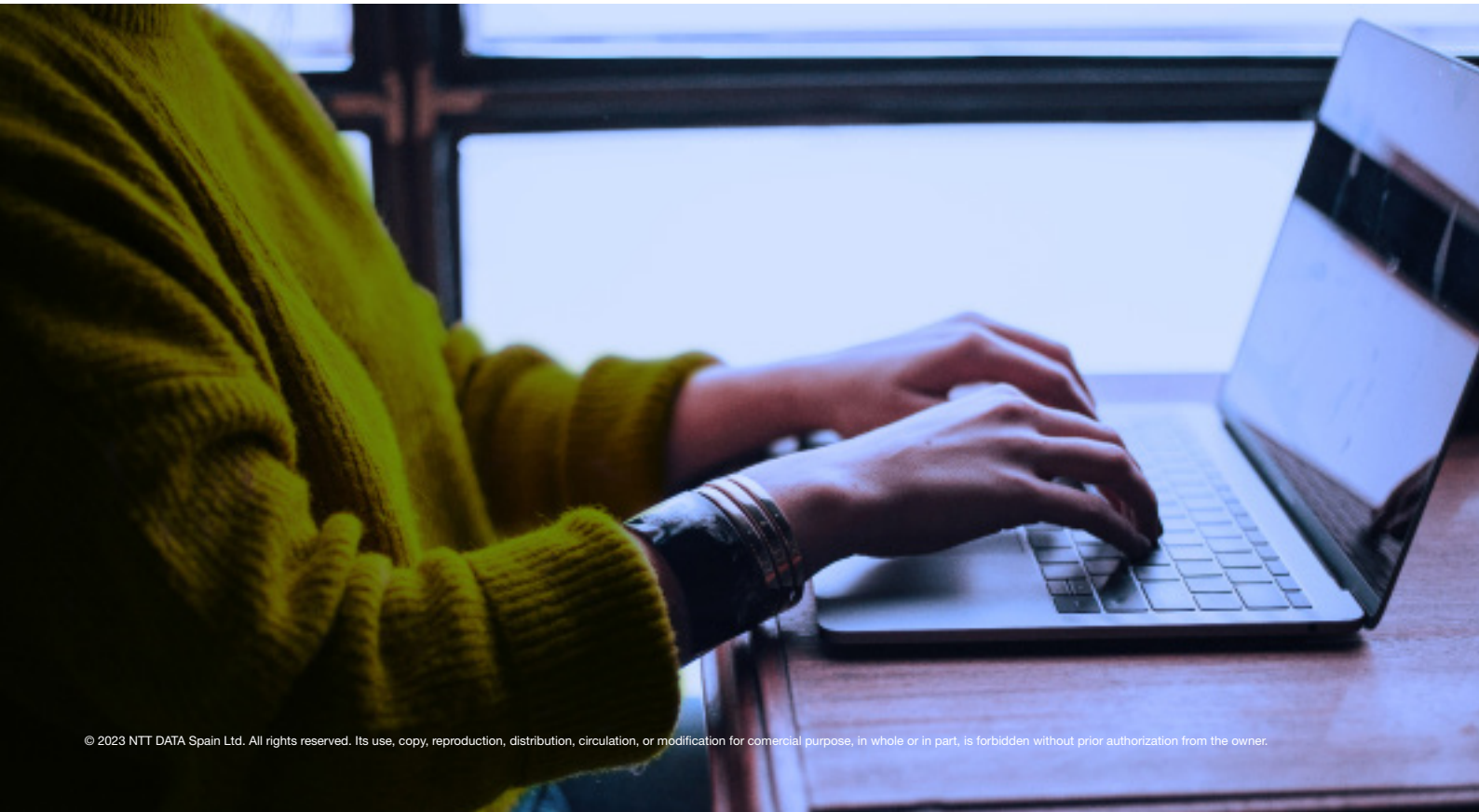
Security risks

However, with the increasing number of smart devices in our homes and lives, we have also seen an increase in the associated security risks. Cybercriminals are exploiting vulnerabilities in these devices to access our personal and financial information, spy on our activities and, in some cases, even take control of the devices.

One of the main concerns is the lack of security in the design and manufacture of these devices. Many manufacturers do not pay sufficient attention to data protection or the implementation of robust security measures, in some cases failing to comply with established security standards. This leaves users exposed to cyber-attacks that could have devastating consequences.

In addition, smart devices are often connected via Wi-Fi networks, which can also be vulnerable to intrusion. Weak passwords or lack of security updates can make home networks easy targets for cybercriminals.

This can result in the loss of sensitive personal information, such as locations and routes tracked by GPS, banking information, health, etc., and can even expose and monitor personal habits.



Latest known scams

The gift with a “surprise” within

Recently, a disturbing pattern has been detected in which some citizens receive surprise packages containing devices such as wireless headsets, smartwatches, smart-bands, and other wearables. However, behind this seemingly friendly gesture, a dangerous secret lurks.

These devices contain malware, malicious software designed to compromise users’ privacy and security.

Once these devices are linked to other computers, the malware is silently activated, allowing criminals to access personal and confidential information without the knowledge or consent of those affected.

This malware can access both voice and cameras, allowing fraudsters to access conversations and accounts linked to smartwatches (GPS, payment methods and messages).

In the event of receiving an unwanted package containing electronic devices, the authorities recommend not to switch them on and to report it immediately or hand it over to the police.

These products can also be used for brushing. This is the practice of sending unsolicited, often counterfeit, products to seemingly random people by mail to allow companies to write positive reviews on behalf of the recipient, allowing them to compete with established products.

Prevention and advice

While there is no such thing as absolute security, there are steps users can take to protect themselves from cybercriminals:

- Keep your devices up to date: Make sure you install the latest software and firmware updates on your smart devices. These updates often contain important security fixes.
- Strong passwords: Use strong and unique passwords for your devices and Wi-Fi networks. Avoid predefined or easy-to-guess passwords.
- Secure networks: Set up your home Wi-Fi network with appropriate security measures, such as WPA2 encryption and a unique network name.
- Do some research before you buy a smart device: Before you buy a smart device, research the manufacturer’s reputation for security and privacy. Opt for those that take these aspects seriously. Checking the locations and security standards recognised and applied by the manufacturer.
- Data protection: Make sure you read and understand the privacy policies and terms of service of the devices and apps you use. Consider limiting access to personal information to only necessary functions.

TRENDS

The rise of malware on mobile devices and other concerns

In today's digital age, mobile devices have become an integral part of our lives, providing us with connectivity, convenience, and access to a wide range of applications and services. However, this growing dependence has also led to an increase in cyber risks and threats affecting mobile devices. Experts predict that mobile security threats will increase dramatically by 2023. According to a recent report by **Cybersecurity Ventures**, the number of mobile security threats is expected to increase by more than 500% in the next three years.

Mobile malware has evolved rapidly. In the past, cybercriminals have focused on the lack of security controls in operating systems and weak controls in application marketplaces to conduct malicious activities. However, as these areas have evolved, malicious actors are importing techniques and tactics from the general threat landscape to the mobile world.

Fraud, identity theft, service disruption and credential theft continue to increase despite the efforts of hardware and software vendors to implement countermeasures to these attacks. This is mainly due to the difficulty of maintaining a balance between the human and the systems along with their processes. This human factor, being inherent in these devices, will always be the focus of these malicious activities acting as an entry vector allowing the use of more sophisticated techniques that can compromise, among other things, the keys to digital identities stored on the mobile device.

In recent years, for example, the Pegasus malware has been a recurring theme in the news headlines and has caused concern in the IT security community. Developed by the Israeli company NSO Group, Pegasus is an advanced spyware designed for mobile devices that has been used to target journalists, politicians, human rights activists, and persons of interest around the world.

One of the most alarming features of Pegasus is its ability to infect devices without the aforementioned human factor by exploiting vulnerabilities in mobile operating systems. Once installed on a device, the malware is able to collect sensitive information such as text messages, emails, call recordings, GPS location and passwords.

While it is difficult to control such advanced state-sponsored cyberattacks, there are certainly attack vectors that can be stopped, such as smishing or the more common malware on mobile devices. In the wider mobile app ecosystem, official app stores such as **Google Play** have traditionally been regarded as safe and perfectly trustworthy places to download apps. However, in recent times, it has been shown that they do not use foolproof methods to prevent the uploading of fraudulent apps, with an alarming increase in the presence of malware within these shops.

Recently, a malware called **Clicker** infiltrated Google Play by masquerading as useful tools such as torches, QR readers, cameras, unit converters or task managers. This type of Trojan performs advertising scams, through recurring connections to websites in the background, allowing cybercriminals to earn revenue through ads and clicks. In total, this Trojan has been confirmed in 16 apps considered safe and available on Google Play, with more than 20 million downloads.

While users need to be aware of the potential risks and take steps to protect their devices, it is also crucial that developers are proactive in ensuring the security of their applications. This may include implementing better security measures such as two-factor authentication or encryption to keep users safe. In addition, they should always keep this human factor in mind and try to implement additional measures to avoid the most damage when this fails.

This increase in mobile security threats is due to the increased use of mobile devices for sensitive activities such as banking and shopping. Over the years and with improvements in mobile devices, more and more people are exclusively mobile users without a personal computer.

On the other hand, the rise of the IoT world is greatly increasing the potential for cyberthreats aimed at mobile devices, given that, at the beginning, they were systems that had hardly any security, as their objective was to offer this type of technology at the lowest cost, with security being one of the characteristics where they cut back to reduce costs, favouring the development of multiple entry vectors.

These predictions show the need for increased mobile security measures. It is essential to understand the potential threats and take steps to protect ourselves with the collaboration of users and developers to keep their devices safe and secure. As in any area of cyber security, defence is always one step behind the attack, which is why plugging as many holes as possible that can serve as an entry vector is of paramount importance.

VULNERABILITIES

Linux

CVE-2023-3269
Date: 11-07-2023

Description. On 11 July, a vulnerability affecting the memory management subsystem of the Linux kernel was published. The vulnerability occurs due to improper lock management for accessing and updating virtual memory areas (VMAs), which leads to problems after memory is freed. This vulnerability can be successfully exploited to execute arbitrary kernel code, escalate containers and, in addition, gain root privileges.

Link: https://my.f5.com/manage/s/article/K000135446?utm_source=f5support&utm_medium=RSS
https://www.ccn-cert.cni.es/component/vulnerabilidades/view/34489.html
https://www.cve.org/CVERecord?id=CVE-2023-3269

Affected Products: Linux kernel for Fedora distribution, all affected versions.

Solution: Update to the latest version.

FortiOS/FortiProxy

CVE-2023-33308
Date: 11-07-2023

Description. A critical vulnerability has been identified in FortiOS and FortiProxy. This stack-based overflow vulnerability allows a remote attacker to execute arbitrary code or commands via specifically crafted packets that reach proxy policies or proxy-mode firewall policies in conjunction with SSL deep packet inspection. On the same day that the critical vulnerability was detected, security patches were released in order to implement the necessary fixes in FortiOs and FortiProxy.

Link: https://www.cisa.gov/news-events/alerts/2023/07/11/fortinet-releases-security-update-fortios-and-fortiproxy
https://www.fortiguard.com/psirt/FG-IR-23-183

Affected Products: The resources affected by this vulnerability are as follows:

- FortiOS version 7.2.0 to 7.2.3.
- FortiOS version 7.0.0 to 7.0.10.
- FortiProxy version 7.2.0 to 7.2.2.
- FortiProxy version 7.0.0.0 to 7.0.9.

Solutions: The following patches have been provided by the manufacturer:

- Update to FortiOS version 7.2.4 or higher.
- Update to FortiOS version 7.0.11 or higher.
- Update to FortiProxy version 7.2.3 or higher.
- Update to FortiProxy version 7.0.10 or higher.

PATCHES

Adobe

Date: 11-07-2023

Description. Adobe has released a security update for Adobe ColdFusion to address critical and high vulnerabilities found in April 2023. The critical security vulnerabilities are detailed as follows:

- CVE-2023-29298: bypassing access control by allowing access to different administrator paths from unauthorised sources.
- CVE-2023-29300: untrusted data deserialisation leading to arbitrary code execution.
- CVE-2023-29301: vulnerability related to weak restriction or excessive authentication attempts.

Link:
https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review
https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

Affected products:
- ColdFusion 2018: update 16 and earlier.
- ColdFusion 2021: update 16 and earlier.
- ColdFusion 2023: GA Release (2023.0.0.330468).

Update:
- ColdFusion 2018: update 17.
- ColdFusion 2021: update 17.
- ColdFusion 2023: update 1.

Microsoft

Date: 11-07-2023

Description. On 11 July, multiple 0-day vulnerabilities were published that are currently exploitable in Microsoft products.
CVE-2023-32046: elevation of privilege vulnerability in the Windows MSHTML platform. This vulnerability was exploited by opening a specially crafted file via email or malicious websites. CVE-2023-32049: windows SmartScreen security feature circumvention vulnerability. CVE-2023-36874: elevation of privilege vulnerability in the Windows error notification service: This actively exploited elevation of privilege flaw allowed threat actors to gain administrator privileges on the Windows device. CVE-2023-36884: remote HTML code execution vulnerability in Office and Windows: Microsoft has published guidance on an unpatched and publicly disclosed Microsoft Office and Windows 0-day that allows remote code execution using specially crafted Microsoft Office documents. CVE-2023-35311: Microsoft Outlook Security Feature Circumvention Vulnerability: actively exploited 0-day vulnerability in Microsoft Outlook that circumvents security warnings and works in the preview pane. CVE-2023-32057: Remote code execution vulnerability in Microsoft message queues. In addition to the 0-day vulnerabilities, the following number of vulnerabilities have been found in Microsoft products:
- 33 elevation of privilege vulnerabilities
- 13 security feature circumvention vulnerabilities
- 37 remote code execution vulnerabilities
- 19 information disclosure vulnerabilities
- 22 denial of service vulnerabilities
- 7 impersonation vulnerabilities

Link: https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2023-patch-tuesday-warns-of-6-zero-days-132-flaws/

Affected products: Multiple Microsoft products.

Update: Update with the patches indicated for each Microsoft product.

EVENTS

Cybersecurity Summer BootCamp

03 - 13 July 2023 |

The Spanish National Cybersecurity Institute (INCIBE) and the Organisation of American States (OAS) organise the annual Cybersecurity Summer BootCamp, an international training programme specialised in cybersecurity aimed at Law Enforcement, Prosecutors, Judges and Magistrates, Policy Makers, and Cyber Incident Response Centre Specialists.

Link: https://www.sans.org/cyber-security-training-events/sansfire-2023/

Congress on the Digital Transformation of the Catalan Third Social Sector

11 July 2023 |

On 11 July, from the Taula d'entitats of the Third Social Sector of Catalonia, through the m4Social project and in collaboration with the Telefónica Foundation, the 'Congress of Digital Transformation of the Third Social Sector of Catalonia' will be held at the Social Hub (c/ Girona, 34, 08010 - Barcelona).

LInk: https://m4social.org/es/esdeveniment/congres-de-transformacio-digital-del-tercer-sector-social-de-catalunya/

Cybersecurity Financial & Government Ecuador Edition

6 July 2023 |

Cybersecurity Financial & Government Ecuador Edition will be held at Swissotel Quito on 6 2023 showcasing Ecuadorian and international business news related to the Digital Technologies, Security Technology sectors.

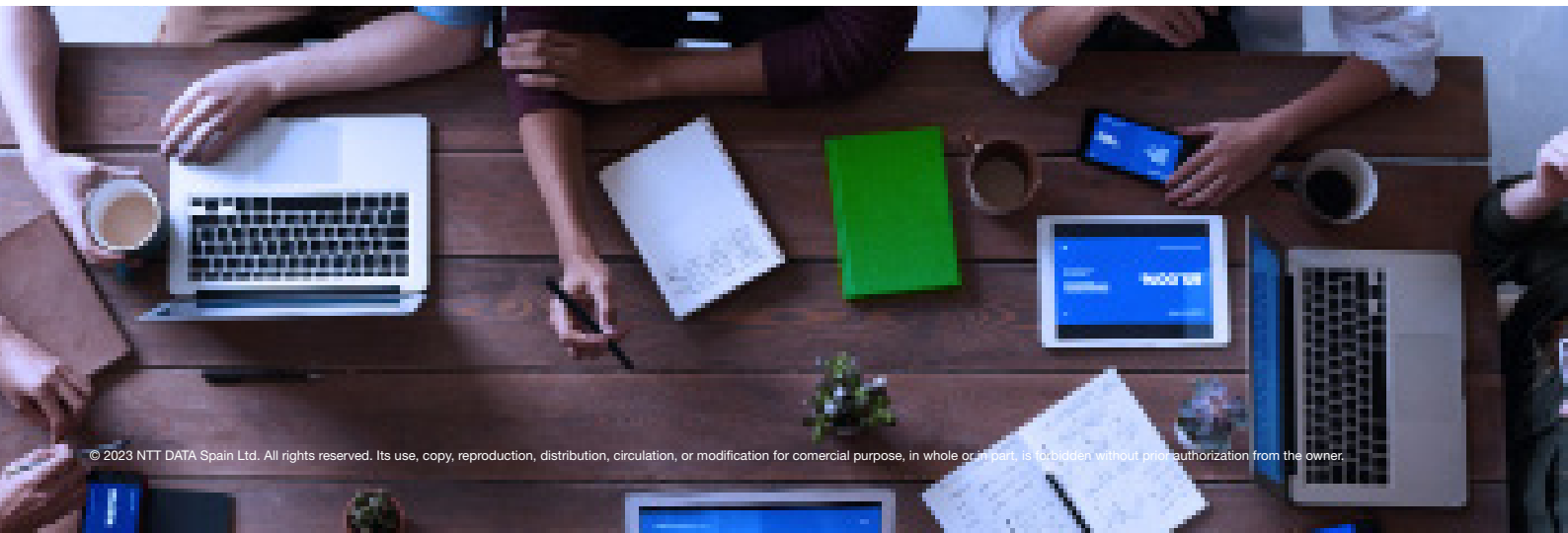
Link: https://www.neventum.es/ferias/cybersecurity-financial-government-edicion-ecuador

Cyber Security EXPO

13 July 2023 |

Cybersecurity EXPO is the only dedicated recruitment event designed for clients and recruitment agencies operating in the cybersecurity sector. Due to the sensitive nature of some jobs and the fact that candidates may wish to remain discreet, the event will be a great opportunity to meet with other candidates.

Link: https://www.cybersecurityexpo.co.uk/manchester



RESOURCES

RULES_OCI WITH BAZEL

Google has recently released Rules_oci, an open source extension for Bazel that aims to ease and improve the security of creating container images. This add-on, known as a “rules set”, supports both the container community and the security of container images.

Link: https://noticiasseguridad.com/tutoriales/proteger-las-imagenes-de-los-contenedores-con-la-herramienta-gratis-de-google-rules_oci-con-bazel/

Cisco announces Extended Detection and Response (XDR)

Cisco is developing an XDR solution that combines network and endpoint expertise for risk-based detection and response. Cisco XDR, in beta, will be available in July 2023. The cloud-native solution applies analytics to prioritise detection and automate response, reducing time-consuming investigations in security operations centres.

Link: https://bitlifemedia.com/2023/05/cisco-presenta-nuevas-soluciones-ciberseguridad-xdr/

Google Cloud fights money laundering in financial institutions with AI

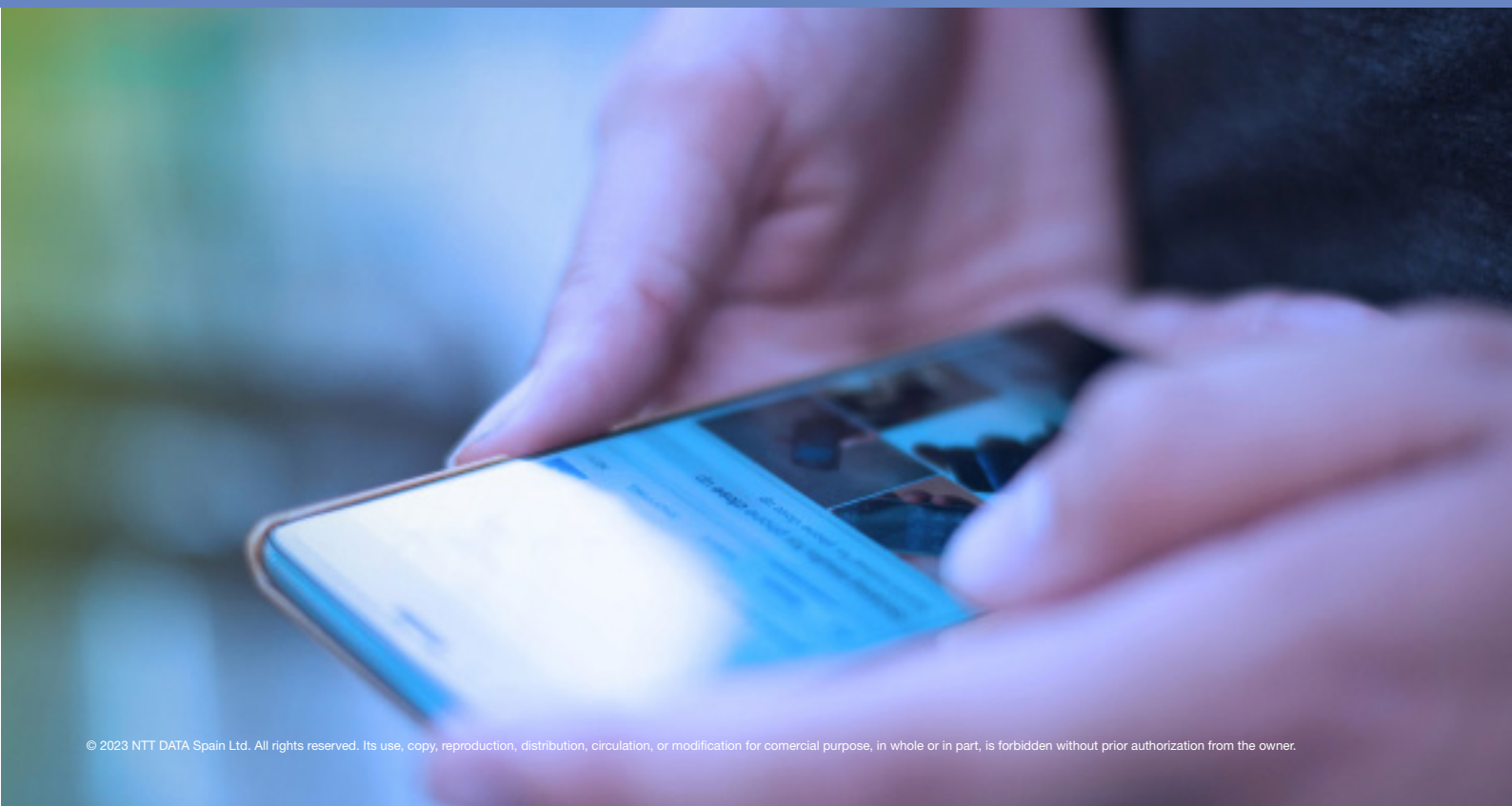
Google Cloud has introduced AML AI (Anti Money Laundering AI), an artificial intelligence (AI) powered product that aims to improve the detection of money laundering in financial institutions. This solution, specifically designed to combat money laundering more effectively and efficiently, harnesses the power of AI to deliver advanced and accurate analytics. With AML AI, financial institutions can strengthen their ability to detect and prevent illicit activities related to money laundering, providing greater protection and security in their operations.

Link: https://cybersecuritynews.es/google-cloud-lanza-un-producto-para-luchar-contra-el-blanqueo-de-capitales-asistido-por-ia-para-entidades-financieras/

New phishing method detected in Microsoft Teams: Impersonating internal users and sending fraudulent messages

A new method of phishing has been discovered in the Microsoft Teams application, which allows attackers to impersonate internal users of an organisation and send misleading messages to other users. As a result, security researcher Alex Reid has created a tool called “TeamsPhisher” using Python, which fully automates this type of attack. The software combines the attack strategies developed by Jumpsec researchers, the techniques of Andrea Santese, and the authentication and assistance functions of the “TeamsEnum” tool created by Bastian Kanbach.

Link: https://github.com/Octoberfest7/TeamsPhisher




NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com