NUMBER 67 | JUNE 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

CYBERSECURITY AND CYBERATTACK TRENDS IN 2022

If we want to see where we are heading in terms of cyberattack trends, we need to look at how we fared in 2021. As a precedent, it warns us of what is to come in 2022, as it was an intense year in terms of incidents and cyberthreats. To sum it up, the difficulties of the public sector facing this problem in Europe and the US, the expansion of ransomware towards more important targets, and its disclosure through significant media attention on hospitals and critical infrastructures, **threats to data confidentiality, skills shortages** or zero-day vulnerabilities, are some examples in this regard.

According to Stormshield, ransomware attacks increased by 62 percent in 2021. However, supply chain attacks, or the Log4Shell zero-day vulnerability, were also important.

In 2022, these attacks will be more sophisticated and will target a greater number of companies and public entities. This year will reinforce the trends observed in the professionalisation of hackers and the emergence of a data shaming economy, in addition to the creation of an environment conducive to attacks thanks to the rise of telecommuting and the increased exposure of applications to the Internet. Not to be forgotten within these vulnerable scenarios are the supply chain systems through which technology companies provide services to these enterprises. Recent geopolitical and health events have highlighted the vulnerability of these complex processes, full of strategic data, which can easily paralyse an entire organisation.

Experts predict that hackers will become even more effective at stealing data thanks to increasingly advanced phishing campaigns. Workers remain the main entry point for cybercriminals.

Cloud services are major players in this exposed scenario. To talk about cybersecurity is, of course, to talk about the cloud. By 2022, vulnerabilities in microservices are likely to contribute to the launch of large-scale attacks.

All these scenarios are also of concern to our governmental authorities, who, in order to mitigate this exponential increase in attacks and mitigate the weaknesses in strategic sectors with the repercussions that result in economic instability, have come up with numerous standards that focus on strengthening IT security, technological resilience, control of providers and technological supply chains, data protection and Cloud security through the updating and creation of standards that regulate and compel companies to cover all these aspects: the new ISO 22002, in European standards such as the D. O.R.A. regulations, EIOPA, critical infrastructure security regulations, standards for security in public services such as the Spanish ENS, etc., which convey the message that IT security and resilience to cyberattacks are part of the security of economies and sectors to be protected by government entities.

They must not only react to new forms of threat, but also reinforce the measures, tools, and processes currently in place in relation to known threats. While organisations and governments are certainly aware of this, many currently still need to develop their competencies in this area.

Maribel Patón Pérez

Cybersecurity Technical Manager at NTT Data Europe & Latam

CYBER NEWS

Today we start our cyber chronicle focusing on the attack that has affected GitHub users, which allowed the download of repositories with private source code. The attack was confirmed on 18 April, when GitHub Security detected unauthorised access to the NPM production infrastructure using a compromised API key.

Investigations into what happened are still ongoing, however, on 12 April an unauthorised anonymous user was detected accessing the production infrastructure of the NPM repository using an API KEY found on an "AMAZON WEB SERVICES" server, managing to download a number of private NPM repositories belonging to GitHub using this stolen OAuth token.

> "Attakers are targeting multiple vulnerabilities in WordPress plugins and themes".

On the other hand, massive redirection campaigns to malicious sites have been detected from sites that have implemented WordPress technology, which allow malicious code to be injected into database files of sites that implement this technology.

"It has been discovered that attackers are targeting multiple vulnerabilities in WordPress plugins and themes to compromise the website and inject their malicious scripts," said Konov.

In addition to this, over the last few weeks, the "Pegasus" software has been in the news due to its use in political cyber-espionage. This spyware is so powerful that it is able to gain access to almost any device without any problems. For this, zero-click attacks are used, where no user interaction is required for the software, in this case Pegasus, to end up installed on the terminal.

"They have managed to penetrate devices in several ways. The traditional one is the use of links via SMS messages and instant messaging platforms. In these cases they try to convince the user to 'click' on the link. However, they also have more advanced ways of achieving this," says Albors.

Finally, in recent months, the "Spring4Shell" vulnerability has been in the news due to the fact that the "Spring" technology is currently being used by many companies.

However, today there are still many vulnerable assets that have not updated their version of Spring, and therefore continue to fall victim to cyber-attacks exploiting the "remote command execution" vulnerability.

SECURITY CHALLENGES IN VIRTUAL ENVIRONMENTS

By: NTT DATA

One of the most talked-about technological changes in recent times is the emergence of virtual reality (VR), which allows us to enter a completely new and fictional world through our senses. But what risks does this new technology bring with it?

The aim of this technology is to provide a user experience that pushes your senses to the limit, making it difficult to distinguish between the real and the virtual, thanks to a sensory immersion unprecedented in this type of platform in which objects interact with the actors.

Immersion in this type of environment can be achieved in various ways (simulators, avatars, helmets, smartphones, costumes, etc.), but the most common way is usually through a headset. Depending on the type of glasses chosen, the user experience can be defined as an Augmented Reality or Virtual Reality experience.

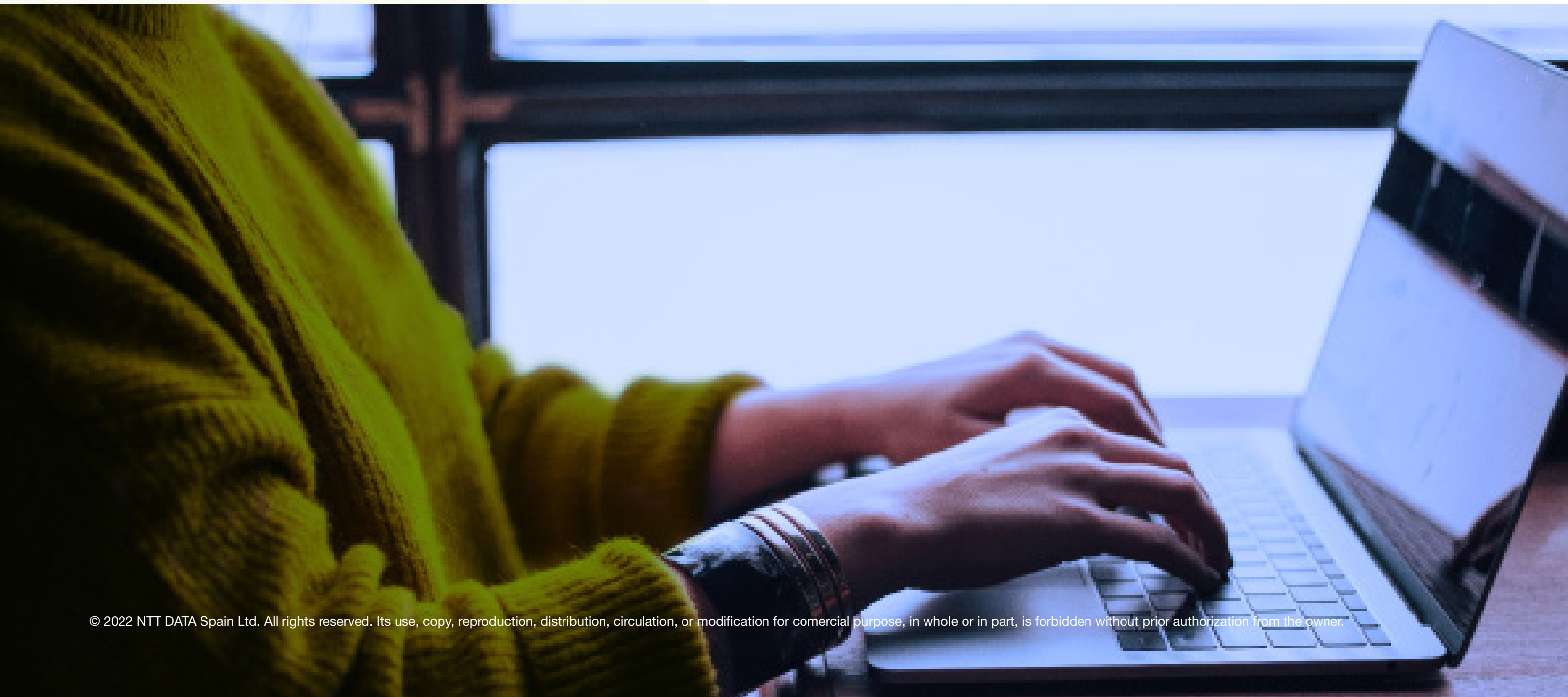
What is the difference between them? Both technologies are complementary, but while the first (AR) can help us to obtain more information about a product, for example, when visiting a museum, checking a rack to find out which cable is faulty or finding out about the features of a car we want to buy without having to leave our sofa; the second (VR) focuses on the user living new experiences and interacting with them as if they were another protagonist in the film they are watching or the video game they are playing.

A little bit of history...

The first simulator that combined 3D images with sound, wind, and smell to create an illusion of reality was developed by Morton Heiling in 1957. From there, the industry grew steadily, and in 1965, the concept of virtual reality was introduced by Ivan Sutherland and the first VR headset (known as "The Sword of Damocles"), which required a computer connection to work. However, it was not until 1982, with the appearance of the film Tron, that the concept of virtual reality did not reach the general public and devices such as gloves with movement sensors and the first VR glasses began to be developed, precursors of the Oculus (the main glasses used today), whose first model (Oculus Rift) was developed in 2010 by Palmer Luckey, raising more than 2.5 million dollars and provoking the starting signal for multiple large companies to begin a race to develop the best VR headset prototype.

Today, the virtual reality market is a multi-billion dollar market. It is known to have moved more than 16 billion dollars globally in 2020 and is expected to grow by at least 18% by 2028, mainly linked to VR gaming.

Linked to this is the vertiginous growth of the concept of metaverse, where we jump from the world of video games to the creation of persistent virtual worlds such as, for example, virtual factories that allow us to test what they are going to put into production in real environments. Although we are still some way from being able to make this concept 100% real, what is clear is that this kind of alternative reality is going to change the way we see things and that, as in the computer world, it will not be free of cyber risks. Therefore, we must be cautious and take into account certain security measures both when developing these environments and when using them.



Creating secure VR/AR solutions

When designing, implementing and, finally, auditing the security of a virtual reality or augmented reality solution, one of the first doubts that may arise is whether there is already a methodology that we can follow to ensure that all possible attack vectors have been covered.

Since the Oculus ecosystem is primarily based on Android devices, our thoughts are likely to go straight to the OWASP guides, the Mobile Security Testing Guide for the client side, and the Web Security Testing Guide for the server side, both of which provide a series of checks to be performed during dynamic application analysis.

The lessons we can find in these guides regarding, among others, the configuration of the platform, the correct management of identities and their sessions, the validation of entries, and the protection of the information that travels and is stored in the devices, are transversal to any implementation.

However, these checks have been devised for systems where the user interacts with information in a relatively limited and predictable way, contrary to the premise of a dynamic, surprising world of almost unlimited freedom promised by virtual reality ecosystems.

Fortunately, there is already an industry that has been walking the path of security in such environments for years:

Ever since the video game SGI Dogfight implemented support for local network play for the first time, curious gamers have sought ways to tip the balance in their favour by creatively manipulating the rules of the game.

Virtual mischief

From gamers simply looking for an easy advantage that allows them not to miss a shot, even if it means the computer plays the game for them, to virtual explorers looking for the slightest flaw in the geometry of online worlds, entering forbidden areas not designed to be seen, there is a wealth of literature on the art of exploiting vulnerabilities in video games.

While the vulnerabilities being exploited are not new, the applications and the impact in an online multiplayer environment are, as demonstrated in the late 1990s in the early days of online poker rooms: In some implementations, the server would send card information to all clients, even though the clients would only display the user's cards.

It was only necessary to analyse the traffic or read the memory of the client application to see the cards of the other players.

In a virtual world, where environmental textures need to be loaded into graphics memory to make the experience as seamless as possible, it is easy to overlook the fact that information contained in custom objects may be relayed to other users. If the design of the application is to send this information to all clients, relying on them to enforce line-of-sight restrictions to hide this information, or distance restrictions to suppress the volume of a conversation, an adversary could exploit this weakness to illicitly obtain information.

Do not feed the troll

A practice as old as the Internet itself is known as trolling or griefing, which is based, in short, on annoying other users for the sake of entertainment, and is the main reason it is so difficult for a virtual world where freedom is truly unlimited to exist.

Many years before the metaverse, the Second Life platform already promised a vast online universe of limitless possibilities, where users could create content and own a piece of electronic space in which to build complex personalised zones.

However, while the creation of objects, props, and clothing was simple, allowing their use in private zones created a major dilemma: Do I allow visitors to my space to express themselves with the objects they own, or do I force the users I invite to have a limited repertoire of objects they can access?

This important issue, coupled with, at the time, complex authorisation controls over the use of custom objects in private areas, led to one of the most high-profile events in the history of the platform:

A virtual interview with Second Life "Virtual Tycoon" Ashe Chung was interrupted several times through the use of a script that generated a large number of extremely offensive custom objects. After moving the location of the interview to another area, where the incident was repeated, the interview was cancelled.

Attacks like this highlight the need for strong rules for authorisation and control of both public and personal spaces that impose reasonable limits.

Similarly, access controls to private areas and spaces should always be based on server-side controls, with well-defined zones that do not rely on the geometry of the virtual world or objects in the virtual world to control access to unauthorised users.

Secure space…

One of the first systems implemented in Meta's applications allowing interaction between users was a security zone that makes any object or avatar disappear when entering the zone. Other virtual chat rooms also implement similar solutions, such as the possibility to push avatars that are too close, or the definition of a boundary zone that can be adjusted according to the user's preferences..

In addition to implementing these security systems that allow users to feel comfortable interacting with other players, it is imperative to ensure that they are implemented in such a way that they cannot be circumvented. The same applies to other traditional user protection measures, such as parental controls, privacy controls, or the moderation capacity of those responsible for ensuring the security of the platform's inhabitants.

… and secure devices.

The other big question an organisation must ask itself, once it knows that the AR/VR solutions it deploys are secure, is: How do I know if the devices I am introducing into my network are secure? What must I do to prevent them from becoming an entry point for potential adversaries?

To do this, it is necessary to acquire all the necessary knowledge about the types of headsets on the market, as well as the type of applications and operating systems they use to realise their functionalities. This analysis, which was initially complicated, was turned upside down with the announcement by John Carmack, CTO of Oculus VR (although veterans may remember him as the man who brought classics like "Doom" and "Quake" to life, among others), in October 2021 to release the Oculus Go goggles. This allows users full access to the device and, therefore, an open door to research in the field of cybersecurity.

On this last point, from NTTDATA, we wanted to participate by contributing our knowledge in the talks at the **RootedCon 2022** with "**Ready Hacker One**", where, among other points, we showed the operation and evasion of the Oculus app shop. This is similar to the Android mobile app shop and has similar restrictions, among which is a primarily static analysis of malicious content. Our research showed that it is possible to circumvent the established controls by including the malicious content in the code before generating the app file.

It is therefore important to stress the importance of establishing the necessary security controls for these new environments that will form part of our daily lives in sectors as important as medicine, logistics and education, and which may handle sensitive information in the operations we carry out.

PEGASUS: WHO IS SPYING ON WHOM?

Pegasus is a surveillance software created by the Israeli company NSO Group, whose main objective was to combat terrorism and cybercrime. This technology, in the first instance, was not available to everyone, as it was designed to be accessible to different governments around the world.

Its operation is quite sophisticated: a message with a link, which the user could access, led to the installation on the phone. The capabilities and modules it has are diverse: reading the user's messages and emails, listening to calls, taking screenshots, logging passwords and accessing the browser's history, among others. It also has the capacity to self-destruct if, after a certain period of time, it has not achieved its objective or if the device is the wrong one.

In 2018, a report by the company Citizen Lab and information from The Wahington Post revealed how Pegasus, which was supposed to be used to prevent crime and terrorism, had been used against activists, journalists, politicians, etc. It had affected more than 45 countries around the world. In Spain between April and May 2019 it affected almost 1500 people.

Finally, some companies have developed specific software for detecting Pegasus on mobile devices. We can highlight Verification Toolkit. This was developed together with Amnesty International in mid-2021 and is free and open source, as well as being compatible with Linux and macOS systems.

.

VULNERABILITIES

CISCO

CVE-2022-20777, CVE-2022-20779, CVE-2022-20780

Date: 04/05/2022

Description. On Cisco's security portal which reports security advisories as of the date they are aware of, a vulnerability report has been published on 4 May regarding Cisco Enterprise NFV infrastructure software: 3 vulnerabilities, 1 of them of critical severity and 2 of them of high severity. The first vulnerability, CVE-2022-20777, allows an authenticated attacker to gain root-level access to the host through the virtual machine via an API call. Vulnerability CVE-2022-20779 allows an unauthenticated attacker to cause the host to install a virtual machine image that allows root-level commands to be executed. Finally, vulnerability CVE-2022-20780 could allow an attacker to obtain sensitive information from the host and leak it to a virtual machine.

Link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9

Affected Products.

- Affects Cisco Enterprise NFVIS in default configuration, versions 4.x and prior.

Solution: Apply software updates provided by the supplier.

Mitsubishi

CVE-2022-0492

Date: 12/05/2022

Description. Mitsubishi Electric has published a report identifying 8 vulnerabilities, 5 of critical severity, 2 of high severity and 1 of medium severity, in the open source software used by VisualSVN Server. The vulnerabilities CVE-2020-13938, CVE-2021-34798 and CVE-2022-0778 can lead to a DoS situation. The vulnerabilities CVE-2021-26691, CVE-2021-3711, CVE-2021-44790 and CVE-2022-23943 can lead to information manipulation, malware execution and DoS situations. Finally, the vulnerability CVE-2021-26691 can lead to information disclosure and manipulation..

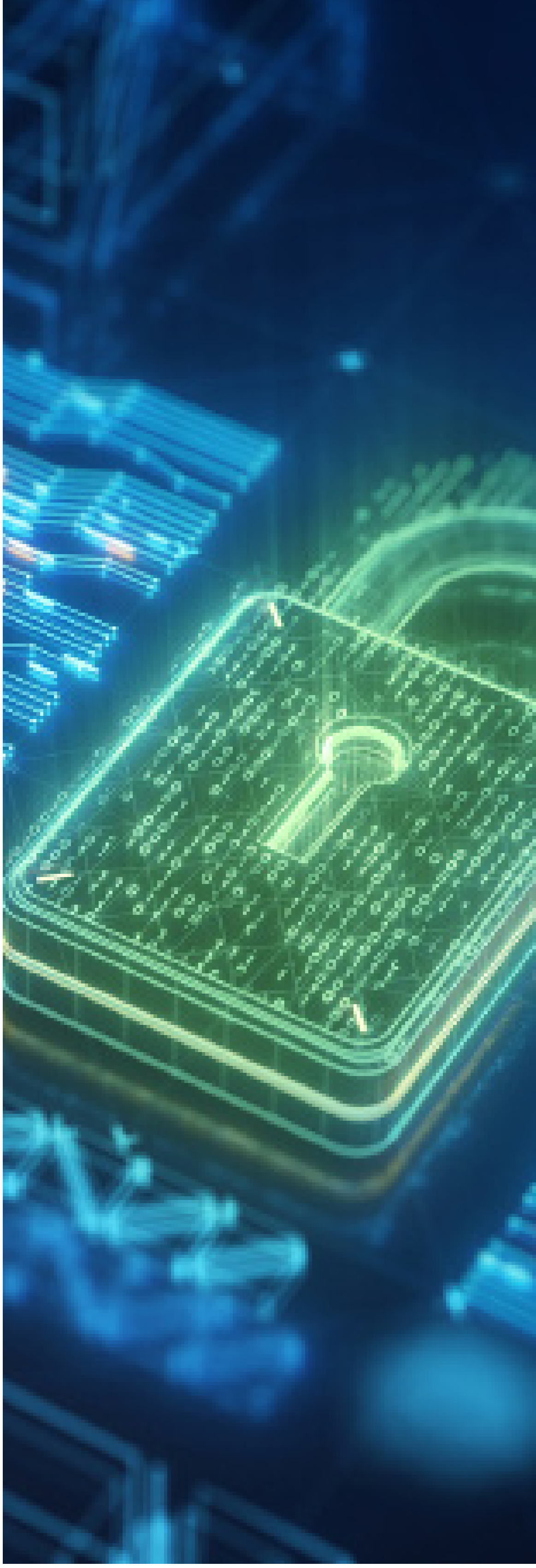
Link: https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-003_en.pdf

Affected Products.

- Affects MELSOFT iQ AppPortal, module SW1DND-IQAPL-M, versions 1.00A to 1.26C.

Solution: Update to software version 1.29F or later.y.

PATCHES



SAP

Date: 10-05-2022

Description. SAP has published the monthly security patch notification for the month of May with 14 security notes for the correction of 11 vulnerabilities: 1 of critical severity, 2 of high severity and 8 of medium severity. The most important of these vulnerabilities, CVE-2022-22965, refers to the so-called Spring4Shell vulnerability that can allow remote execution of malicious code.

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

Affected Products:
Some of the affected products are:

- SAP Business One Cloud, version – 1.1
- SAP Commerce, versions – 1905, 2005, 2105 y 2011
- SAP Customer Profitability Analytics, version – 2
- SAP Netweaver AS for ABAP and Java, versions – KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, 8.04, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 8.04
- SAP BusinessObjects Business Intelligence Platform, versions – 420, 430
- SAP NetWeaver Application Server for ABAP and ABAP Platform, versions -700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788
- SAP Employee Self Service (Fiori My Leave Request), Version -605
- SAP Host Agent, Version -7.22

Solution: Apply the necessary updates and patches provided by the manufacturer.

Microsoft

Date: 10-05-2022

Description. The security update release for the month of May has been launched. This release fixes 226 vulnerabilities of which 17 are of critical severity, 175 of high severity, 1 of medium severity, 2 of low severity and the rest, with no severity established. One of the critical vulnerabilities that have been fixed corresponds to CVE-2022-29972 and allowed a local user to execute arbitrary code remotely in Azure Synapse Pipelines and Azure Data Factory.

Link: https://msrc.microsoft.com/update-guide/releaseNote/2022-May
https://media.cert.europa.eu/static/SecurityAdvisories/2022/CERT-EU-SA2022-033.pdf

Affected Products: See the complete list of affected products in the first reference link.

Solution: Apply the security update provided by Windows.

EVENTS

RSA conference

6 to 9 june 2022 |

RSA Conference is the premier global forum for the cybersecurity industry. This year's RSAC will be a blended experience, with both an in-person event and a virtual space. Once again this year, you will be able to enjoy its extensive agenda of keynotes, networking events and a large exhibition area.

Linnk: https://www.rsaconference.com/usa

International Cybersecurity Forum

6 to 9 june 2022 |

The FIC, or International Cybersecurity Forum, is one of the leading European events on digital security and trust. During the proposed 2022 days, presentations will be made in connection with the concept of the "Digital Decade" being promoted in Europe in 2021. Therefore, the main theme will focus on proposing measures for Europe to be able to respond to the proliferation of cyber-threats in the field of information security.

Enlace: https://www.forum-fic.com

CISO Day

9 june 2022 |

CISO Day aims to bring to the table the different issues facing cybersecurity managers (CISOs, CIOs, etc.) and to bring their point of view together with that of cybersecurity researchers.

Link: https://cisoday.es/

Cybersecurity Expo

15 june 2022 |

Ciberseguridad Expo (Cybersecurity Expo) is the National Congress where IT security managers, CISOs, CIOs and System directors can learn from leading experts about the most cutting-edge experiences and practices in cybersecurity, cyber risk control and the fight against cyber-attacks.

Link: https://www.ciberexpo.ifaes.com

OWASP Global Appsec Europe

9 to 10 june 2022 |

The well-known OWASP organisation is proposing two days for development and defence teams to join forces to build a more secure web. The conference will bring together several well-known speakers in the world of cybersecurity, as well as the community itself with its articles and blogs, to set the expectation of this event at the highest level. In addition, 3 days (6-8 June) will be dedicated to paid courses on different security technologies and applications.

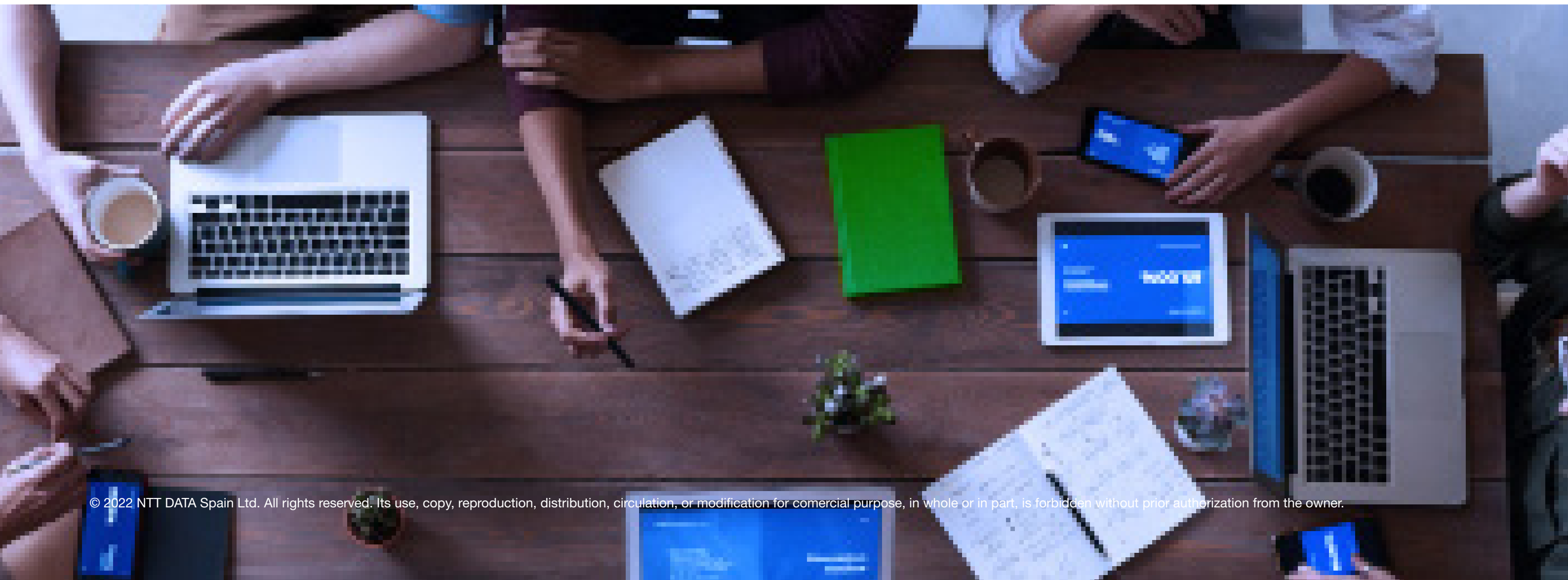
Link: https://whova.com/portal/registration/owasp_202208

CONFERENCIA HYP

30 june to 1 july 2022 |

It is an event of several conferences developed by different speakers that will deal with topics ranging from security in the Cloud to how to develop a ZeroTrust infrastructure or different ways to achieve persistence in a domain controller, among others.

Link: https://www.accelevents.com/e/HIPEurope#agenda



RESOURCES

npm-attacks-code-white-jfrog

NPM attacks: Recently the SNYK team had discovered certain packets in the NPM log that could be or contain malicious code. It was later discovered by software developer JFrog and cybersecurity firm ReversingLabs that these packets were used as an attack vector to perform security audits on various companies in Germany. This attack allowed the auditors to trick the NPM tool into installing dependencies containing backdoor techniques on the machines where they were installed by using a local JSON, which specified the alternative path of the packet to be installed. However, these illegitimate packets were left public, allowing other adversaries to maintain a persistence in the audited German companies.

Link: https://www.theregister.com/2022/05/12/npm-attacks-code-white-jfrog/

Mobile Verification Toolkit

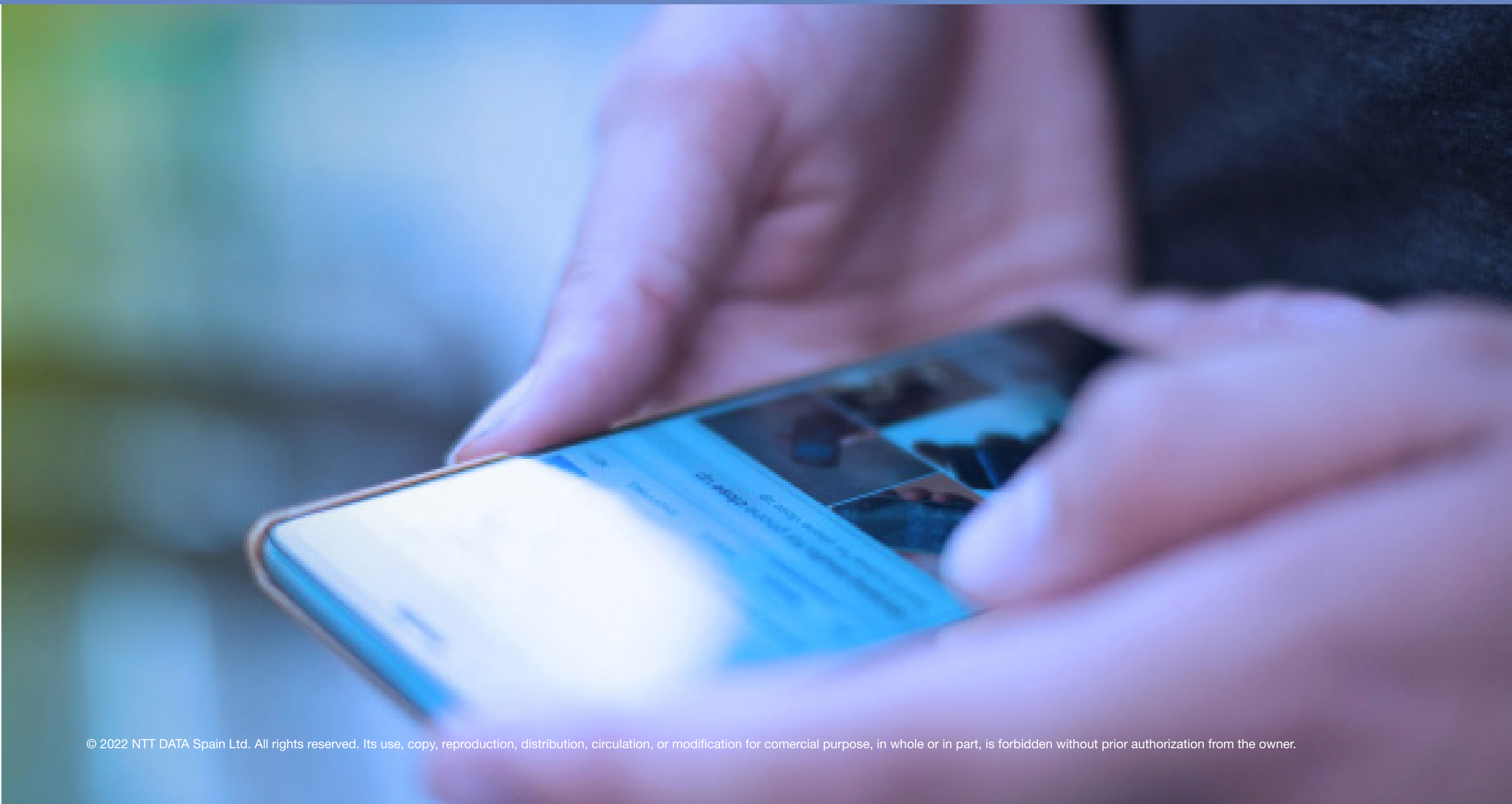
Checking a device breached by Pegasus: In the last month, several scandals have been revealed in connection with the Israeli espionage related to the NSO group, whose root project is called Pegasus. This software will be used to verify whether a device has been infected with this software, in order to take the necessary measures in the event of an affirmative infection.

Link: https://github.com/arainho/awesome-api-security

RCE in firewalls FIG-IP F5

On 4 May 2022, F5 published several vulnerabilities including CVE-2022-1388. This issue has resulted as a remote command execution vulnerability for which there is a working exploit shown in the following link:

Link: https://github.com/ZephrFish/F5-CVE-2022-1388-Exploit



NTT DATA

Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com