NUMBER 69 | AUGUST 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

POST-QUANTUM CRYPTOGRAPHY

Lately there have been many questions about post-quantum cryptography. It is a topic of interest, although there is some confusion about it, as there are many expressions that incorporate the word quantum (some of them seeking a certain “marketing” effect). Thus, we have, among others, post-quantum cryptography, quantum cryptography, quantum computing, quantum mechanics, etc. concepts that are related, but which are different issues with different degrees of maturity. In case it may be of help, we will give a brief description of each of them, since explaining them is another matter altogether.

Back in the 1960s, Richard Feynman said “I think I can safely say that no one understands quantum mechanics”. Since he said these words, I do not know if we have made much progress in understanding it. According to a survey published by New Scientist magazine, physicists do not agree on exactly what is the reality quantum mechanics explains, and it is quite another thing when it comes to its application.

We start with post-quantum cryptography. It is one of the most attention-grabbing topics, but perhaps one of the least “glamorous, quantum-speaking”, since it is, after all, about finding algorithms that are resistant to quantum computing, but it is still the same old cryptography, selecting from all the mathematical problems those that are resistant to quantum computing. In other words, it is the development of new types of cryptographic approaches that can be implemented with today’s computers but are immune to attacks by tomorrow’s quantum computers.

And what are the potential problems? Well, in 2016, the US National Institute of Standards and Technology initiated a process to develop standards in post-quantum encryption for the government and that project is now in its final phase and the winners are expected to be announced soon. The main problem categories where new asymmetric algorithms resistant to the quantum threat are being sought and proposed are:

1) Lattice-based cryptography
2) Hash function based schemes
3) Isogenies on elliptic curves
4) Multivariate cryptography
5) Code-based cryptography.

None of them is simple or easy to implement in real environments since, among other things, they require larger keys than those currently used. However, there are already precedents of use, for example, Google has been testing for a while a hybrid algorithm (CECPQ1, the post-quantum suite) in Google Canary and although it openly acknowledges that this is not a good enough solution, it is a first step.

As to whether we need to worry about the robustness of our current encryption systems, any company or government planning to store data for decades should think about the risks of their encryption systems, as it will become vulnerable sooner or later and it would take many years to go back and re-encrypt huge amounts of historical record data with more robust solutions.

Therefore, it would be much better to start from scratch, not only because of the threat of quantum computing, but also because asymmetric cryptography, like any other system, has always had weaknesses.

It should be remembered that current asymmetric cryptography is based on three mathematical problems:

1) The difficulty of factoring large integers

2) The Discrete Logarithm problem

3) Multiplication on elliptic curves, which may seem insufficient.

On the other hand, we have only been talking about asymmetric cryptography so far, but what about symmetric cryptography? It is worth noting that most of the current algorithms of symmetric cryptography (symmetric ciphers and cryptographic hash functions) are quite secure against quantum computation.

This is because the only known applicable quantum algorithm is that of Grover35, which has the advantage of speeding up the capacity of attacks, but this advantage can be reduced by something “relatively” simple, such as doubling the size of the key used. Therefore, post-quantum symmetric cryptography will not be very different from symmetric cryptography.

In conclusion, apart from the threat of quantum computing, it does not hurt cryptography to work on new alternatives that will help to strengthen it.

María Pilar Torres Bruna

Cybersecurity Director at NTT Data Europe & Latam

CYBER NEWS

Today we begin our cyber-chronicles with the advancement of technology, ICTs have become a crucial part of our lives, and even more so, the problems it can bring to our private information. At any time, a 'Remote Command Execution' vulnerability, or the all too desirable 'SQL Injections' can appear. However, the automotive world is also not free from the threats that may exist in their designs, such as the not so recent but little-known news in which a 'random man', together with his 'gadgets', managed to open or even start a well-known and appreciated car model in its brand (Honda Civic).[1]

Who would not want to break into someone else's car, being aware of the legal problems that this may entail? Sounds good, right? For those who are interested, there have been several public proofs of concept developed on GitHub in recent months that might help (we do not recommend it, unless it is your own 'car').

> "Joker, this malware, after infecting a device, donwloads a series of files that allow it to steal data from your phone, especially text messages and contacts".

This man (nonamecoder according to his GitHub account), together with his 'RF hacking' team, has found a way to send the specific sequences to open/close doors or start the engine. This attack is simple since the signals are not encrypted and can be intercepted by anyone within range of their power and later replicated for obscure purposes.

The vulnerability has been listed as CVE-2022-27254 and the proofs of concept can be found at the following link: https://github.com/nonamecoder/CVE-2022-27254
In short, Civic models from 2016 -2020 are the ones affected by this security issue, but they will not be the only ones.

From security flaws in cars, we move on to the risks on our own mobile devices. As usual with app shops, every so often they offer us a list of apps that were available in their download shops and that unfortunately "had a freebie". Because of this, their focus has been the search for a malware known as "Joker". This malware, after infecting a device, downloads a series of files that allow it to steal data from your phone, especially text messages and contacts. Among other functions, it subscribes the user to fraudulent websites and services where the criminals keep most of the money, as it is difficult to reclaim it due to its origins. The 4 applications detected in this analysis were:

- Blood Pressure Monitor
- Smart SMS Messages
- Voice Languages Translator
- Quick Text SMS

They racked up more than 500,000 downloads each, so if you have any of them installed, the recommendation is to delete them and factory reset your phone, as well as change the credentials of the accounts used on your devices.
Although Google Play and Apple Store periodically notify of apps that are removed from the shop when malware is detected, it is always advisable to keep an eye on shop notifications and keep apps updated to the latest version.

1. https://noticias.coches.com/noticias-motor/honda-llave-hacker/467311

For reasons such as this, companies are focusing on protecting users on smartphones, such as Apple, which, for its recently released new version of its operating system, offers a new security feature called “Lockdown Mode”.
After activating this function and restarting the device, the security level of the device is raised to the maximum by taking measures such as:

- Messages: Most types of attachments to messages other than images are blocked. Some features, such as link preview, are disabled.
- Web browsing: Some complex web technologies, such as just-in-time (JIT) JavaScript compilation, are disabled unless the user excludes a trusted site from blocking mode.
- Apple Services: Incoming invitations and service requests, including FaceTime calls, are blocked if the user has not previously sent the initiator a call or request.
- Wired connections to a computer or accessory are blocked when the iPhone is locked.
- Configuration profiles cannot be installed, and the device cannot enrol in mobile device management (MDM), while lock mode is enabled.

In addition, Apple has decided to listen to and engage more with the user community, which is why it has enabled a way to report bugs, and the new platform for reporting security flaws, for which Apple is offering a reward for reporting and helping to resolve them of up to 2 million US dollars. The highest figure given by any company so far. So, if you want to venture to exploit this new mode developed by Apple, and get a juicy reward, you just have to follow the steps provided on their website and try it.

After talking about offensive security, we end with Vectra’s security research team, which has been able to design an AI (Artificial Intelligence) to detect attacks in real time and block them at their earliest stage, in order to prevent a possible compromise of information.

This research by the Vectra team does not only focus on specific tools or attack groups but goes to a higher level where it can directly detect the methods (both current and future) that adversaries are likely to use. Its efficiency is based on having researched the optimal threshold at which the tool will consider an event as malicious or benign. This task of calibrating the AI makes it a fairly reliable system for threat detection.

Vectra employs a recurrent neural network architecture known as ‘long- and short-term memory’ (LSTM) to identify attack behaviour. Real samples generated by algorithms are used to train this LSTM. In addition, Vectra’s so-called ‘streaming model’ uses algorithms that extract the strictly necessary data from events to convert them into new references for the models. As this ‘sifting’ of data comes from large amounts of data and events, it will ensure the highest quality of alerts.

PRIVACY, WIDESPREAD DISINTEREST

By: NTT DATA

With the evolution of technology, new services have become available to people, ranging from voice shopping from home to complete monitoring of our health parameters on our smartphones.

The development and improvement of these services and methods of interacting with technology requires the collection of data on how people use them, which has allowed processes to be optimised and adapted to the needs of consumers.

In addition to the purely technical purpose of data collection, new opportunities have arisen, based on the collection of usage data for commercial purposes, i.e. selling it to third parties to identify users' tastes and preferences in order to build a profile that ad companies will use to target their content to a more specific audience, thus achieving a greater impact on their advertisements.

As technology has developed, new data collection mechanisms have emerged, which have made it possible to extract data from areas that were previously inaccessible without a digital medium.

Generally, the form of communication to users about what data is being collected and how it is processed is through a privacy policy, which must be read and accepted before they can use any service that processes and collects data.

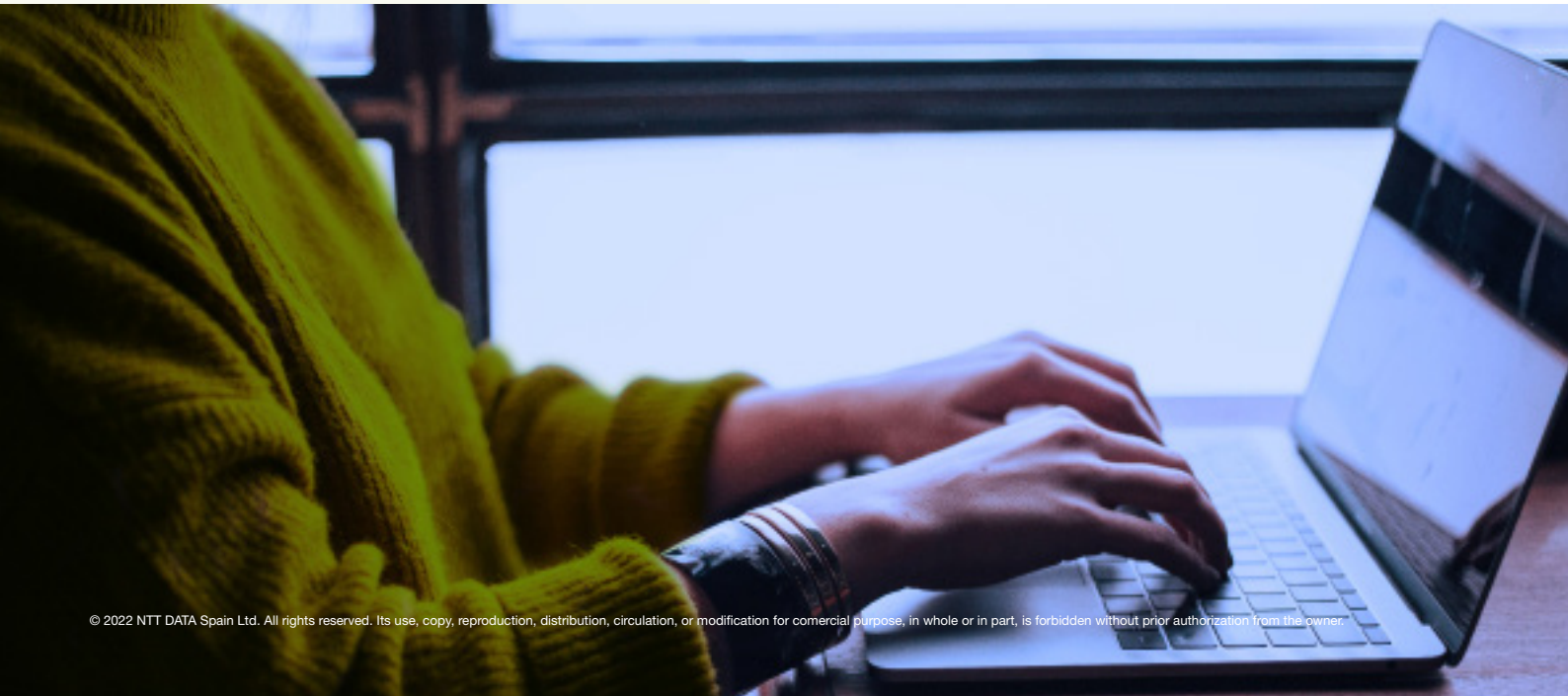
The use of this information has led to a number of privacy issues, both from a commercial point of view and from a governmental perspective, where ideally, data on citizens is used to enhance their security.

As discussed below, the processing of people's information is far from an ideal scenario, as various practices have come to light that make us question the extent to which users' privacy is being respected, acting in the supposed interest of optimising applications and services or maintaining citizens' security.

Origins and evolution

A few years ago, privacy was almost unknown to many people, the same people who made use of new technologies to make their daily lives easier, making a phone call, sending an email, surfing the internet, or using an instant messaging application.

Privacy concerns first came to light in 2013, when a former Central Intelligence Agency (CIA) and National Security Agency (NSA) employee named Edward Snowden revealed information indicating the NSA's use of mass spying programs such as PRISM and XKEYSCORE.



This global scandal revealed how citizens around the world had been secretly spied on. Snowden wanted to make this information public so that people would be aware that their privacy had been compromised without their consent. Additionally, he revealed his identity and decided not to hide anonymously from the leaks, as he claimed he had done nothing wrong.

It has been a few years since Snowden showed the world how vulnerable privacy is because users do not have as much as they think they do. In this latest high-profile case, the protagonist is an Israeli company called NSO Group, which has developed spying software known as Pegasus.

This software allows a device to be infected and controlled with almost no user interaction, giving the software full control to extract information on demand, such as listening to calls, viewing exchanged messages or geolocating the device.

In both cases, the "justification" for the creation of such intrusive spying software is none other than to prevent terrorism or more serious crime. This only raises concerns for those who ask: To what extent is this intrusive behaviour permissible and how much does it endanger users' privacy?

As a result of this issue, and from a commercial point of view, there have been several high-profile cases in which some companies have violated users' privacy by processing users' data in ways that have been found to be abusive, or not in accordance with their privacy policies.

One of the most prominent recent cases involved three of the largest technology companies. With the rise of the smart personal assistant market, the processing of their users' voice data became increasingly common. While in most cases the data processing is done by automated means, all three companies were found to have employees who listened to some of their users' voice messages without first informing them of the possibility that their voice recordings could be listened to and processed by humans. All companies stated that this processing was done in such a way that the recordings remained anonymous, but some reports pointed to the possibility that the recordings could include the user's name, user identifiers or the device that was used. Following these findings, all companies duly report on human review of voice recordings, giving users of their smart assistants the possibility to decide whether their voice samples can be analysed by humans or not.

Data use and current trends

In a person's day-to-day life, there are numerous interactions with different technological devices, such as a computer, mobile phone, or voice assistant. What people have probably not thought about is the amount of information that is being provided by the simple use of these devices.

It is common that while browsing the Internet, the configuration of cookies is requested in order to continue displaying content. This request usually comes in an intrusive way with a message that prevents the display of content and which requires you to pay attention by selecting one of the available options. At first glance the most prominent option will be to "Accept all cookies" and continue viewing the desired content, perhaps the quickest option, but what if instead of accepting everything you review the settings? Surprise, you are providing more information than would a priori be required.

On the other hand, many users have a wearable, such as a smartwatch, which is monitoring heart rate, sleep quality, counting steps, sharing location or even messages coming from the mobile device. All this information is handled by the manufacturer of this product, who has the power to decide what to do with it, whether to sell it, share it or opt for privacy and not to make it known to third parties.

In recent years, thanks in part to the exposure of certain practices, such as those mentioned above, initiatives have emerged to provide users with greater protection against abusive collection of their data. For example, app Marketplaces (first in the iOS App Store and later in the Android Play Store), incorporate a notice about the data that will be collected from the user when using any app downloaded from the Marketplace. This gives a more adequate view that summarises part of the app's privacy policy, which otherwise the user would not normally read to check how their data will be used.

Also, the system that manages permissions on popular mobile operating systems has been improved to give more precise control over which options on the device an application can and cannot use. Users are given the possibility to select more privacy-friendly options, for example, when sharing their device's location data with certain applications, they are allowed to give an approximate location, rather than providing an exact location.

Along with native improvements to operating systems, applications have emerged with the idea of protecting users' privacy, as opposed to traditional applications in different areas. For example, in the case of messaging apps, while Facebook Messenger collects and associates with users data such as financial information, location, contacts, search histories, user content (photos, videos, etc.) or contact information (name, email, physical address, etc.), other apps such as Signal do not collect this type of information in order to link it to each user and use it for commercial purposes.

Consumers' perceptions of privacy have been evolving, giving it more and more weight when choosing one service over another, although much work remains to be done to move from a sales pitch to real control that allows users to decide with whom their data can be shared and for what purpose.

TRENDS

TrusPid

The use of third-party cookies is coming to an end and will mean a change when it comes to personalised advertising for users in their browsing experience on the Internet by collecting information about their preferences and habits. Major web browsers such as Safari and Firefox already block the use of these cookies, and soon Google's Chrome browser will be the next to take this big step.

This has led to a search for alternatives, one of the most important and promising being a new technology developed by Vodafone, called TrustPid, based on the generation of a "token", which is a unique and temporary identifier, formed from the telephone number and the IP address used to browse the internet. This identifier will be provided to advertising networks that will be able to uniquely identify each customer and thus launch targeted advertising without the need for cookies.

This supercookie, as it is currently known, will be controlled by telecommunications companies, allowing them to profile their users and provide personalised advertising. Its functioning is simple: once a user connects to the internet, the server generates the user's token and begins to collect information about their behaviour on the network, which is shared anonymously with advertisers who will offer personalised advertising to the user; on this occasion, the data is processed and stored at the level of the mobile internet service provider (IPS).

This alternative to conventional cookies can pose a great risk to users' privacy if they are not handled properly. The personality profiles generated with this new technology cover all kinds of user information, such as sexual orientation or religion, as well as medical conditions, among others, and are a security risk in general.

All this means that, although this technology is still in the testing phase in some countries such as Germany, it shows once again how exposed our data is and how fruitful and important it is for companies to obtain it, providing them with a great benefit from its commercialisation.

.

VULNERABILITIES

CISCO

CVE-2022-20812
Date: 06/07/2022

Description. Several Cisco products have presented a number of vulnerabilities of critical severity. The affected products are Cisco Expressway and TelePresence VCS. The vulnerabilities in these products could allow an attacker to overwrite arbitrary files or perform null byte poisoning attacks. These vulnerabilities are caused by insufficient validation of input data in command line arguments.

Link:

https://nvd.nist.gov/vuln/detail/CVE-2022-20812

https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-cisco-83

Affected Products.

- Versions prior to 14.0.7

Solution: Update to version 14.0.7, which fixes these vulnerabilities.

OpenSSL

CVE-2022-2274, CVE-2022-2097
Date: 01/07/2022

Description. Researchers Xi Ruoyao and Alex Chernyakhovsky have discovered several vulnerabilities related to OpenSSl that could allow remote code execution on a machine running the affected software. The most critical vulnerability is due to a bug in the RSA implementation on processors with X86_64 CPUs. The bug occurred when processing 2048-bit keys, causing memory corruption on the affected system. The other vulnerability, of lesser severity, is related to the implementation of the AES algorithm.

Link: https://nvd.nist.gov/vuln/detail/CVE-2022-2274

https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-openssl-2

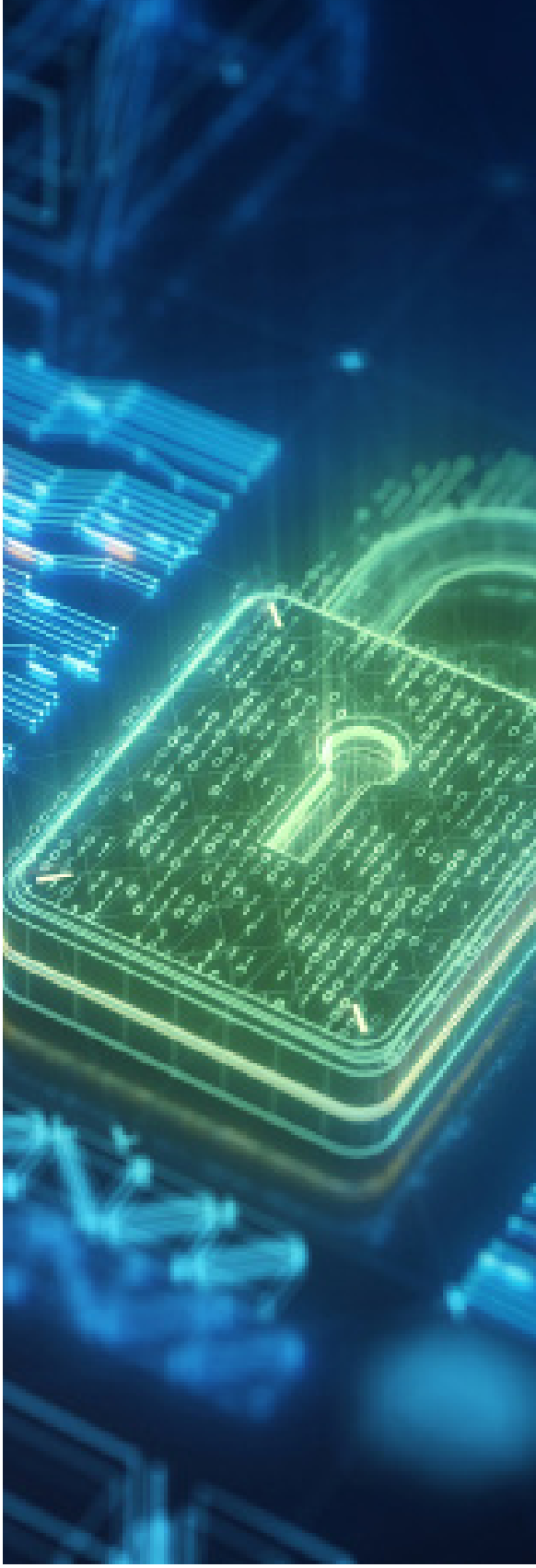
Affected Products. The affected product versions are the following:

- OpenSSL 3.0.4
- OpenSSL 1.1.1
- OpenSSL 3.0

Solution: The manufacturer has released the following patches to mitigate these vulnerabilities:

- OpenSSL 3.0.5
- OpenSSL 1.1.1q

PATCHES



Festo

Date: 07-06-2022

Description. New firmware versions have been released for the Festo CECC-X-M1 controllers, which had vulnerabilities that allowed remote command execution without the need for authentication with root privileges.

Link: https://www.incibe-cert.es/alerta-temprana/avisos-sci/vulnerabilidad-inyeccion-comandos-festo-cecc-x-m1

Affected Products:

- CECC-X-M1 controller version 4.0.14, version 3.8.14 and prior,
- CECC-X-M1-MV controller version 4.0.14, version 3.8.14 and prior,
- CECC-X-M1-MV-S1 controller version 4.0.14, version 3.8.14 and prior,
- CECC-X-M1-YS-L1 controller, CECC-X-M1-YS-L2 controller, CECC-X-M1-Y-YJKP controller, Servo Press Kit YJKP and Servo Press Kit YJKP- versions 3.8.14 and prior.

Solution: Install firmware versions 3.8.18, 4.0.18 or higher.

Google Chrome

Date: 04-07-2022

Description. Google Chrome has released version 103.0.5060.114, which fixes a number of high-risk vulnerabilities in the browser. These vulnerabilities were related to the following aspects:

- Buffer overflow in WebRTC.
- Multiple security flaws related to memory corruption in Chrome OS Shell.
- Type confusion in V8 (Google's JavaScript engine).

Link: https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop.html

Affected Products: Browser versions prior to 103.0.5060.114.

Solution: Update to versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 or 7.18.1

EVENTS

DAYS OF THE DEFENDERS

From 2 to 3 August 2022 |

Hosted by Microsoft security architects, this intensive demo experience is designed to give you an insight into the latest Microsoft security tools. You will discover how to position, design and plan common scenarios with Microsoft Defender for Cloud, Microsoft Sentinel and Microsoft 365 Defender workloads. Finally, there will be a fun and competitive Capture The Flag game where you can test your skills.

Link: Days of the defenders

BLACK HAT 2022

From 6 to 11 August 2022 |

Founded in 1997, Black Hat is an internationally recognised cybersecurity event series that delivers the most technical and relevant research in information security. These multi-day events, which have grown from a single annual conference to become the most respected international information security event series, provide the security community with the latest cutting-edge research, developments, and trends.

Link: Black Hat 2022 (blackhat.com)

DEFCON 2022

From 11 to 14 August 2022 |

Hackers, corporate IT professionals and three-letter government agencies converge on Las Vegas each summer to soak up the cybersecurity research of the world's brightest minds and test their skills in hacking contests.

Link: DEFCON 2022 (defcon.org)

CYBER SECURITY ASIA

From 15 to 16 August 2022 |

This event will bring together top experts and professionals to offer in-depth talks and exclusive networking opportunities. It is a platform for partnership and strategy development and highlights the latest technologies that are securing government, industry, and people.

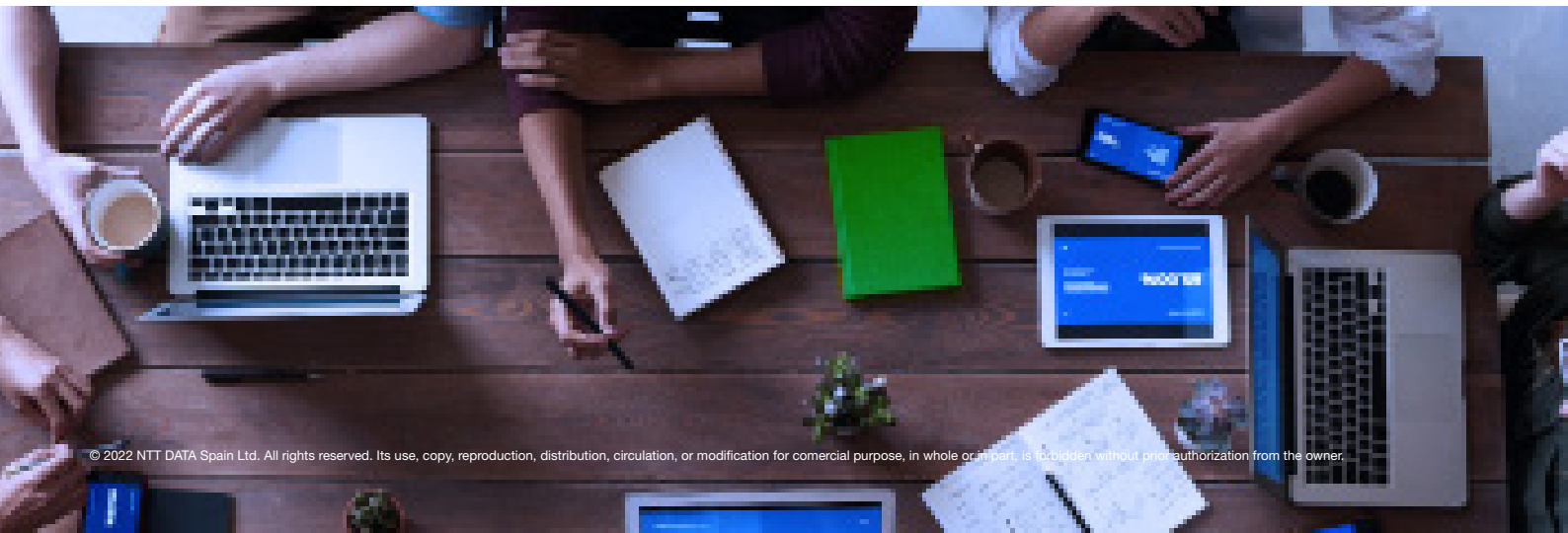
Link: https://cybersecurityasia.tech

SECURITY EXHIBITION & CONFERENCE

From 17 to 18 August 2022 |

The ASIAL Security Conference includes a compelling line-up of experts and academics from today's security landscape who will share their insights on how to protect your business, brand reputation and critical assets along with mitigating risks and vulnerabilities.

Link: https://www.asial.com.au



RESOURCES

LOCKBIT, EL RANSOMWARE MÁS RÁPIDO

In a ransomware attack, response time is essential in order to stop it and “lift all defences”. So much so that Splunk’s security team has conducted a series of tests to determine which ransomware takes the least time to encrypt files, with the clear winner being Lockbit. This article shows the results for each ransomware family along with recommendations to prevent falling victim to this type of attack.

Enlace: https://www.redeszone.net/noticias/seguridad/ransomware-cifra-rapido-archivos/

CYBERSECURITY AND ARTIFICIAL INTELLIGENCE

This article discusses the close relationship between cyber security and Artificial Intelligence, which can be used to improve the cyber security of products and to carry out attacks more effectively (defence approach and attack approach), which is especially accentuated with the development of artificial intelligence year by year.

Enlace: https://www.realinstitutoelcano.org/analisis/la-ciberseguridad-y-su-relacion-con-la-inteligencia-artificial/

MALWARE DISTRIBUTION VIA NPM PACKAGES

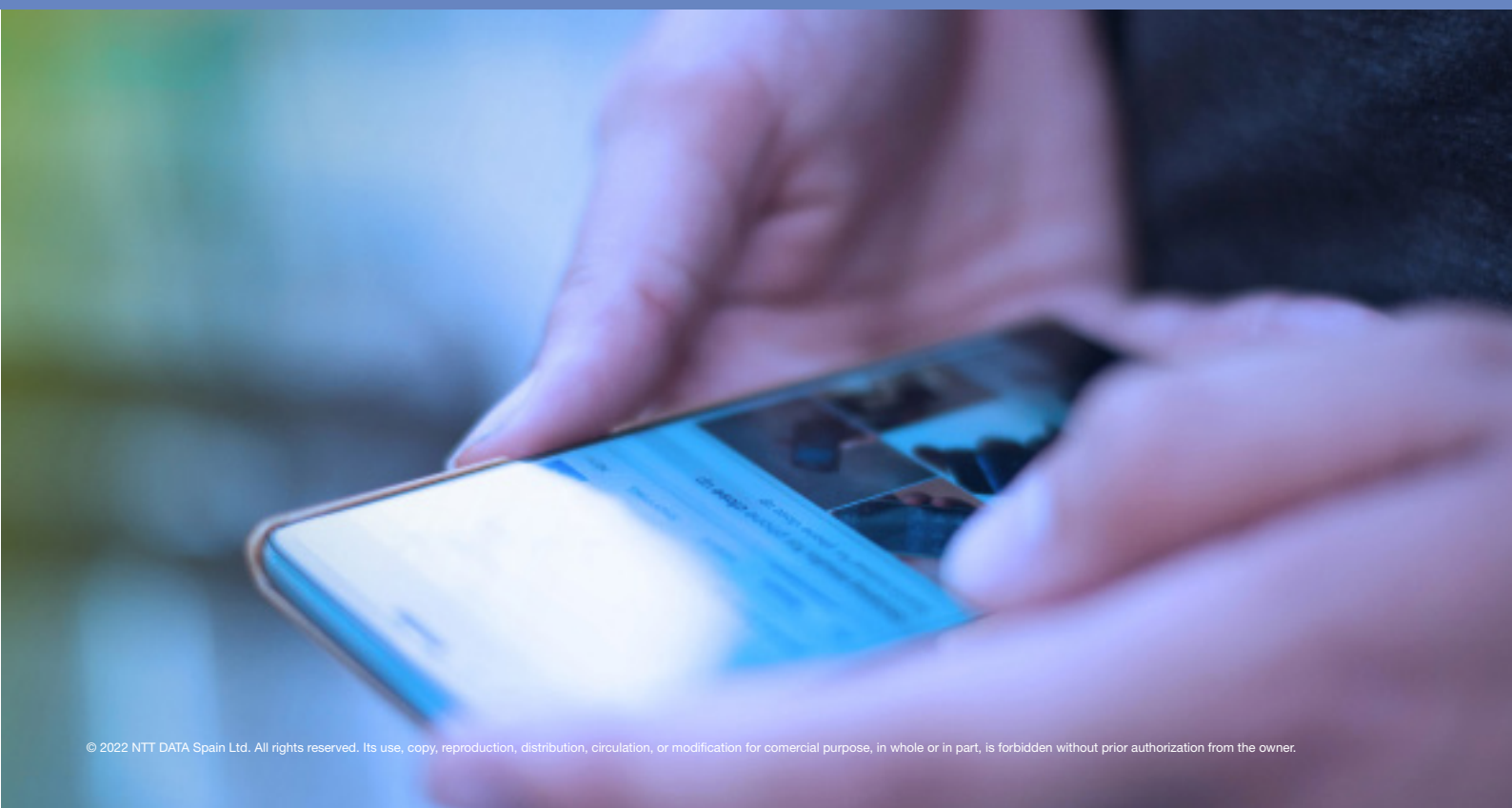
NPM is a package manager for JavaScript from which third-party libraries and dependencies can be downloaded. This article describes how such packages are used to distribute malware to users who use the service by pretending to be legitimate packages. Additionally, some examples of packages that are known to be malicious and that spoof other packages that are known to be in use in order to get downloaded and distributed are shown.

Enlace: https://blog.reversinglabs.com/blog/iconburst-npm-software-supply-chain-attack-grabs-data-from-apps-websites

ATTACKS ON SUPPLY CHAINS

An organisation’s supply chains are one of its most vulnerable attack surfaces and require special attention. The main supply chain attacks from 1982 to the present day are shown and explained in this article with links to more detailed information for each attack.

Enlace: https://blog.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks




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