NUMBER 82 | SEPTEMBER 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

SAFEGUARDING THE DIGITAL FRONTIER WITH CIAM

Cybersecurity and data protection are the foundation for building trust with customers, as safeguarding their data is the number one priority for any business. To this end, companies have typically relied on Identity and Access Management (IAM) solutions that focus on an organisation's internal users. However, Customer Identity and Access Management (CIAM) is a state-of-the-art solution that enables organisations to securely manage their customers' identities and access to their services. CIAM specifically addresses the unique requirements of external customers, partners, and providers, ensuring a secure and user-friendly experience.

Importance in Modern Cybersecurity

CIAM provides robust authentication and authorisation mechanisms, mitigating the risk of unauthorised access and identity fraud. With the rising number of data breaches and cyberattacks, protecting customer identities has become an urgent priority for businesses seeking to maintain a competitive edge while retaining their customers' trust.

Its role is also important in the wake of stringent data protection regulations like the General Data Protection Regulation (GDPR), as businesses managing customer data must comply with these regulations. It offers a comprehensive approach to meet compliance requirements, reducing the likelihood of legal penalties and reputational damage. CIAM solutions are designed to handle a vast number of customer identities and transactions simultaneously. This scalability ensures that organisations can effectively manage identity and access requirements, even during peak usage periods. All of this is done through a personalised user experience that enables businesses to gain valuable insights into customer behaviour and preferences. Such information can be leveraged to deliver personalised services and experiences, enhancing customer satisfaction and loyalty.

Key components

From streamlined registration processes to advanced security analytics, let us uncover the essential elements that make CIAM a game-changer in the realm of digital identity management.

1. **Registration and Onboarding:** Seamless registration process. Customers should be able to create accounts easily and securely, allowing them to access services with minimal friction.
2. **Authentication:** Employment of various authentication methods such as multi-factor authentication (MFA), biometric verification, and single sign-on (SSO). These mechanisms ensure that only authorised users can access the resources they need.
3. **Consent Management:** Consent management features, giving customers control over their personal data and how it is used. This aligns with data privacy regulations and reinforces transparency and trust.
4. **Profile Management:** Enabling customers to manage their profiles and preferences, such as updating personal information, email preferences, and communication settings.
5. **Security Analytics:** Security analytics to detect suspicious activities and potential threats, allowing organisations to proactively respond to emerging security risks.

The challenges of CIAM implementation

Implementing CIAM, despite its numerous advantages, is not without its challenges. One of the key obstacles is striking the delicate balance between implementing robust security measures and providing a seamless and user-friendly experience. While strong security protocols are essential to safeguard customer data, creating overly complex processes may deter users, leading to abandoned registrations or transactions. Handling and storing customer data securely while preserving data privacy is another significant challenge for organisations. With increasing data protection regulations, CIAM solutions must ensure strict compliance and prioritise protecting the customer's right to privacy.

Moreover, as businesses grow and customer bases expand, this system must be able to scale accordingly to meet the escalating demand for access and identity management services. Ensuring smooth performance during periods of high user activity is crucial for maintaining a positive customer experience.

Road to innovation

CIAM is an essential component of modern cybersecurity strategies. Organisations can build and maintain customer trust, foster brand loyalty, and create a safe and personalised digital environment for their customers. As cyber threats continue to evolve, this could be a powerful ally in safeguarding the digital frontier and fortifying the customer-business relationship.

Enrique Bernao Rosado
Manager de Ciberseguridad en NTT DATA Europe & Latam

CYBER NEWS

We begin this new edition of RADAR with the following news: Microsoft has raised the alarm after discovering that a known hacker group linked to the Russian government has been using the Microsoft Teams chat application to conduct phishing attacks on specific organisations.

The group, known as “Midnight Blizzard”, has been identified as a threat linked to the Foreign Intelligence Service of the Russian Federation (SVR). Using Microsoft Teams, the hackers have conducted a phishing campaign directed against targets in government sectors, non-governmental organisations (NGOs), technology services, manufacturing, and media.

> “It is critical to be alert to phishing tactics and to strengthen online defences to protect against these sophisticated attacks. Collaboration and constant vigilance are essential in the fight against growing cyber threats.”

Midnight Blizzard’s modus operandi involves using previously compromised Microsoft 365 tenants owned by small businesses to create new domains posing as legitimate technical support entities. Through messages in Microsoft Teams, the hackers attempt to steal credentials from targeted organisations by asking users to approve multi-factor authentication (MFA). The highly selective attacks have affected fewer than 40 unique organisations worldwide, suggesting a highly targeted cyber-espionage operation in the United States and Europe.

Once users accept the messages and follow the instructions, hackers obtain valid credentials to access the victims’ Microsoft 365 accounts. Subsequently, information theft activities have been detected on the compromised tenants. In addition, in some cases, hackers attempt to add devices to organisations as managed devices to circumvent conditional access policies.

Microsoft has taken steps to mitigate the use of the domains by this group and continues to investigate other related attacks.This incident highlights the importance of cybersecurity awareness and cybersecurity in organisations.

It is critical to be alert to phishing tactics and to strengthen online defences to protect against these sophisticated attacks. Collaboration and constant vigilance are essential in the fight against growing cyber threats.

On the other hand, a new artificial intelligence (AI) tool called “FraudGPT” is emerging, specifically targeting sophisticated attacks. Malicious actors are promoting it on dark web marketplaces and Telegram channels. Designed for offensive purposes, the tool allows to create spear phishing emails, develop undetectable malware, find vulnerabilities and more... Its author claims there have been more than 3,000 confirmed sales and reviews.

The tool has been circulating since at least July 2023 and is offered through a subscription model costing $200 per month, $1,000 for six months and $1,700 for a year. While the specific language model used to develop FraudGPT is still unknown, this new generation of AI tools for cybercriminals poses significant challenges for cybersecurity.

These tools can function as a launch pad for script kiddies looking to conduct large-scale corporate phishing attacks, which could result in the theft of confidential information and unauthorised payments.
Against this backdrop, it becomes essential to implement defence-in-depth strategies and have rapid security telemetry to detect and counter threats before they become more serious incidents.

Also of note is the following news. The number of ransomware attacks on industrial organisations and infrastructure has doubled since the second quarter of 2022, according to a report by Dragos, an industrial cybersecurity firm. In the second quarter of 2023, 253 incidents were recorded, representing an 18 per cent increase from the first quarter of the same year, where 214 attacks were observed. The company attributes the increase in attacks to a decline in ransomware revenues in 2022, as more victims refuse to pay. In addition, attacks are expected to continue to increase due to political tensions between NATO countries and Russia, which motivates ransomware groups associated with Russia to continue attacking critical infrastructure in NATO countries. It has also been observed that ransomware groups focus on attacking larger organisations to maintain their revenues. The manufacturing sector is the most affected, followed by industrial control systems (ICS), transportation, and oil and gas.

One of the most controversial attacks this month has been that of CardioComm, a Canadian provider of medical cardiac monitoring solutions, which has been the victim of a cyber-attack that has forced the company to suspend operations. Production servers were affected, leading to the disruption of services on its website. The company estimates that its business will be impacted for several days as it works to restore data and server environments.

Although the attack did not compromise customer health information, CardioComm has taken precautions to protect its employees' personal information. It is suspected that the attack may have been perpetrated by ransomware, prompting the company to take immediate action to contain the situation and prevent further damage.

In addition, the cyber-attack could have financial consequences, as CardioComm may face difficulties in finalising required filings due to a cease-and-desist order issued by the Ontario Securities Commission, which also resulted in the suspension of trading in its shares.

CardioComm is known for providing specialised software for recording and analysing electrocardiograms, used by hospitals, doctors and consumer devices to diagnose patients with cardiac problems. The company is working hard to overcome this situation and restore normal operations.

CAN WE TRUST CHATGPT WITH OUR PRIVACY?

By: NTT DATA

Assuming you are not living under a rock, you will know what ChatGPT is. The “Chat” part is more or less clear from the first use, but the acronym GPT hides much more than meets the eye.

Generative, Pre-trained and Transformative. ChatGPT is a model of Artificial Intelligence (hereinafter AI) that is based on OpenAI technology to create new content (texts or dialogues) and is trained using an ample collection that constantly learns and improves thanks to a neural network.

It merely replicates the way humans speak, it learns from many texts, but it remains at the surface layer of semantics and syntax. It does not recognise sarcasm or humour, nor does it check the reliability of information, and with all the misinformation around us that can be dangerous.

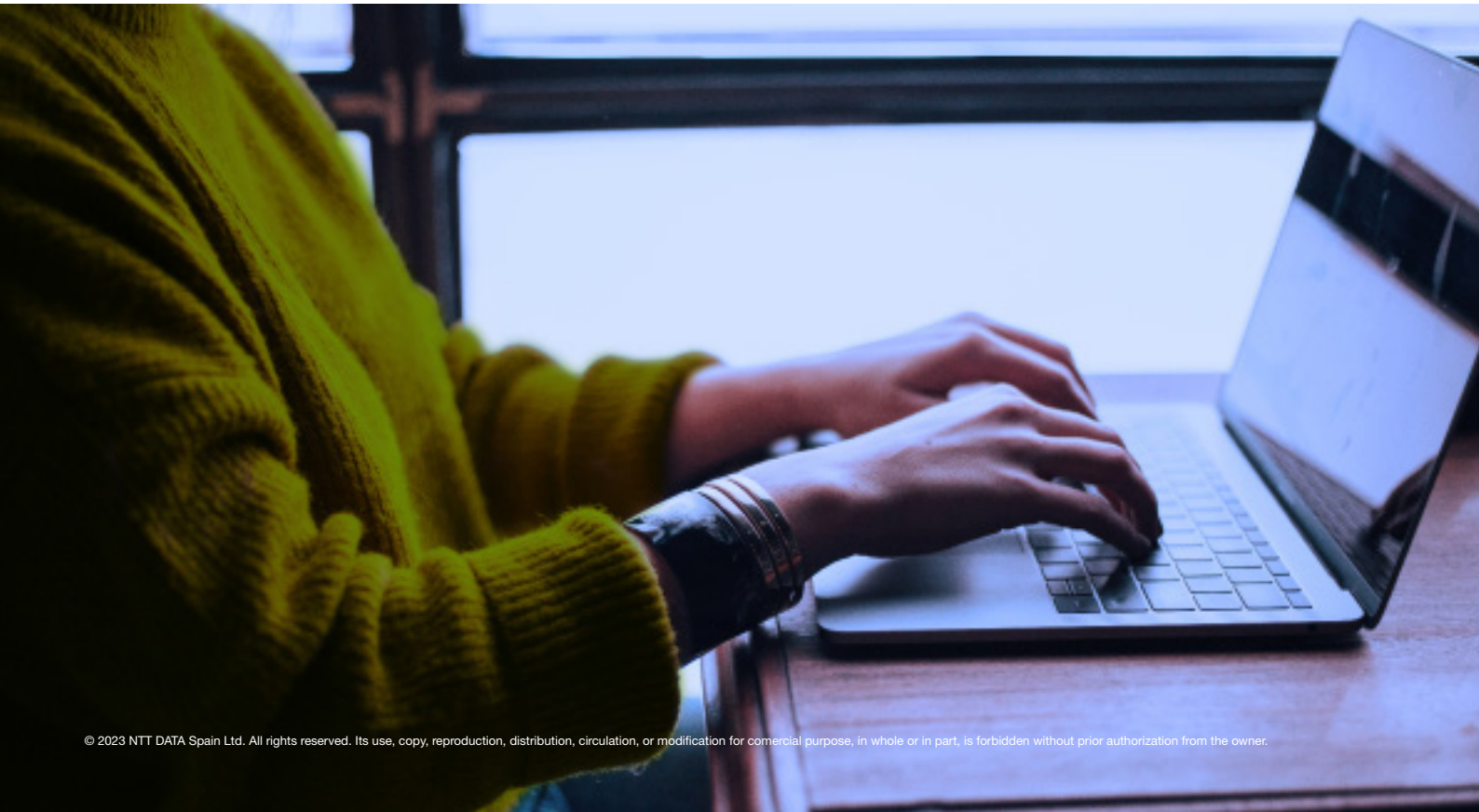
AI does not work alone, it needs a “co-pilot”, people. Why does a machine need to have a human behind it? For safeguarding.

We cannot deny that we are in the eye of a perfect storm between technology and innovation, as we have at our disposal the necessary means to run tools such as ChatGPT, and, in addition, the ideal conditions are being created for these processes to be efficient and for AI decisions to be relevant and involve adequate data protection.

The intersections between artificial intelligence and data protection regulations are evident. An example of this is its privacy policy, which does not clarify how it processes and protects personal data to generate content. What is clear is that it does use it.

The chat is fed by a massive number of texts collected on the internet (blogs, articles, public forums, websites...) so, if our data is on any of the mentioned sites: ChatGPT has access to it.

Not to mention everything it learns from our nuances, for instance, the way we ask when we chat with it. Is it analysing us? Is it generating a profile without our consent? Is it transparent with the users?



That is why data protection is especially relevant with this type of learning-based systems and we must not forget the basics to make them secure applications for the user.

There are four essential cornerstones according to data protection regulations:

- Data subjects' rights
- Principles of data processing (the rules of the game)
- Proactive accountability measures (risk-based approach)
- Supervisory authorities

The most obvious solution is to establish the privacy system by design. Acting as a hinge element between the design phase of the AI system and the deployment phase. In the end, the core factor is how we confer the AI system.

In many cases, if we do not execute the system properly from the design stage so that it complies with Data Protection regulations at a later stage, once they make decisions, nothing can be done. When the system is already in the market, if the privacy element has not been implemented from the design phase, that AI system may not be adequately compliant with Data Protection regulations.

What are the design phase and the deployment phase? Let us take a look at them.

SYSTEM DESIGN PHASE

- Project Scope
- Data collection
- Algorithm selection
- Model development
- Model training
- Model evaluation

SYSTEM DEPLOYMENT PHASE

- Different organisation (develops/implements)
- Integration in the environment
- Inferences made from the model
- Decision making
- Model monitoring

The first thing to do when starting a project is to set the scope, the 5Ws (what, who, where, why, when), to be clear about the roadmap. For an AI to work as we want it to, it needs a large amount of data so that it can learn.

Once we have this concoction under control, we develop, train, and evaluate the generated models.

It sounds simple, but this is where one of the four cornerstones of data protection comes into play, for if we take a closer look at these two words, "data collection", many of the principles of data protection come into conflict with each other.

To make it clearer, let us set an example. If we put AI to work and feed it with massive data, the principle of data minimisation will undoubtedly be affected.

Obviously, we need a multitude of databases to come into play so that the data is as up to date as possible, and the variables are sufficiently representative. If it generates inferences, the data could be inaccurate, and we do not want that to happen... That is the accuracy principle.

How can we correctly execute programs implementing Privacy by Design from the point of view of the DPD? Solutions of this type must be designed in compliance with the regulatory framework from the outset. We can do this with a proper justification of the variables chosen for the phases of the process, establishing the purposes of the processing, what is to be achieved, and analysing the data protection objectives.

This is done so that when the different teams enter the project's deployment phase (developers, QA, integrators, etc.), they can move within these pre-established margins and be able to comply with the regulations.

TRENDS

Self-governed identity: the new identity management model in cybersecurity

Self-Sovereign Identity (SSI) is a model of digital identity management that removes authentication from a single, central, sovereign authority. In contrast to traditional models where governments and companies are the custodians of our data, a self-governed identity system is based on the individual's ability to manage and share their information securely and selectively. In other words, the roles are swapped, and the focus is on models where the user decides what they can and cannot see about us.

In order to achieve identity self-management, we will have to rely on the use of these three basic pillars:

- **Blockchain:** digital and decentralised recording of information, using cryptography within a blockchain in which, due to the way it is structured, it will prevent it from being successfully modified by third parties.
- **Decentralised identifiers (DIDs):** a unique code for each individual that allows a unique identification, as well as managing what information is to be accessed from the wallet (application or device that allows the storage and management of cryptocurrencies and digital assets), in which the information is collected for identification purposes. To do this, a secure connection is made between two parties using a pair of public keys and one or more private keys.
- **Verifiable credentials (VCs):** identities are encrypted and secured so that they can be verified by any organisation quickly and efficiently, without having to consult your personal data directly.

The use of the wallet in these SSI models allows the management of the information shared by the individual to fall entirely on them. Moreover, it allows this action to be conducted wherever and whenever, using a unique identifier for this purpose. This in turn will prevent their identity from disappearing if it is deleted by the body that manages it or if it is not valid in any context other than the one in which it is collected by the responsible entity.

Within this approach we find the concept known as the "trust triangle", composed of holder (user who generates the decentralised identifier in the wallet), issuer (authority issuing the verifiable credentials) and verifier (party in charge of verifying the credential).

An example of use would be an application for a university degree, where the holder is asked to show their ID in the wallet to prove that they have the required bachelor's degree (whose issuer would be an educational institution). By sharing this information, a secure connection is established between the university and the user. Only the necessary information is disclosed, while maintaining the privacy of other personal data, which is not disclosed because the user selects what can be viewed. The university (verifier) verifies the authenticity of the data using the digital identity and associated public key stored in the blockchain.

This approach to identity management is more secure and efficient than traditional methods, avoiding centralisation and the risks of credential theft. The user has the power to decide who accesses their information, reducing the risk of privilege escalation and unauthorised tracking. Together, Self-Governed Identity and Verifiable Credentials represent a significant advance in protecting digital identity and privacy in an increasingly digitised environment.

VULNERABILITIES

Citrix

CVE-2023-3519;-3466;-3467
Date: 18-07-2023

Description. Three vulnerabilities affecting Citrix products (NetScaler ADC and Citrix Gateway) have been published. One of them is of critical severity (CVE-2023-3519) and the other two of high severity (CVE-2023-3466 and CVE-3467). The critical vulnerability (CVE-2023-3519) exploits a bug that allows code injection and thus remote code execution by attackers. In order to exploit this vulnerability, the device needs to be configured as a Gateway. One of the high severity vulnerabilities (CVE-2023-3466) consists in the possibility of executing Cross-Site Scripting attacks due to the lack of validation of the input data. Successful exploitation of this vulnerability requires the attacker to send a URL to the victim. The latest high vulnerability (CVE-2023-3467) exploits inadequate privilege management, allowing privilege escalation within the vulnerable product.

Link: https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/12672-ccn-cert-av-08-23-actualizacion-de-seguridad-en-productos-citrix.html

https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Affected Products: The affected products are the following:

- NetScaler ADC and NetScaler Gateway 13.1 prior to 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 prior to 13.0-91.13
- NetScaler ADC 13.1-FIPS prior to 13.1-37.159
- NetScaler ADC 12.1-FIPS prior to 12.1-55.297
- NetScaler ADC 12.1-NDcPP prior to 12.1-55.297

Solution: The solution proposed by the manufacturer is to update to the following versions:

- NetScaler ADC and NetScaler Gateway 13.1-49.13 and later versions
- NetScaler ADC and NetScaler Gateway 13.0-91.13 and versions later than 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.159 and versions later than 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.297 and versions later than 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.297 and versions later than 12.1-NDcPP

Ivanti EPM

CVE-2023-35082
Date: 03-08-2023

Description. Last July, a number of vulnerabilities relating to Ivanti EPMM were published. These vulnerabilities were fixed with a series of security patches. However, a group of cybersecurity researchers have discovered a way to bypass the security measures applied by the manufacturer, exposing the vulnerabilities once again. The new critical vulnerability (CVE-2023-35082) arises from the same location as the previous vulnerability (CVE-2023-35078) and could potentially allow an attacker to access users' personally identifiable information and make limited changes to their personal information. Specifically, an attacker with access to different API paths could access personally identifiable information (PII) such as names, phone numbers and other mobile device details for users on a vulnerable system.

Link: https://thehackernews.com/2023/08/researchers-discover-bypass-for.html
https://www.bleepingcomputer.com/news/security/ivanti-discloses-new-critical-auth-bypass-bug-in-mobileiron-core/

Affected Products: The vulnerability affects all supported versions (11.4, 11.10, 11.9, 11.8 and earlier).

Solutions: We are currently waiting for the manufacturer to release new patches to fix these vulnerabilities permanently.

PATCHES

Oracle

Date: 19-07-2023

Description. Oracle has released a series of updates to fix 508 vulnerabilities, including a total of 76 critical updates and 183 unique CVEs. Some of the products with the most critical vulnerabilities and patches are listed below: The Oracle Construction and Engineering product has a total of 147 patches and, in addition, 115 unauthenticated remote exploits. Some of the CVEs for which this product's patches apply are CVE-2023-1370, CVE-2023-24998 and CVE-2022-48285, among others. The Oracle Fusion Middleware product has 60 new security patches and 40 of these vulnerabilities can be exploited remotely without authentication. Some of the related CVEs are CVE-2022-42920, CVE-2022-45047, CVE-2023-25690, CVE-2021-42575 and CVE-2022-41853. The Oracle MySQL product has received 24 new security updates. Of these vulnerabilities, 11 of them can be exploited remotely without authentication. The CVE with the highest criticality that has been fixed with the security updates is CVE-2023-20862.

Link:
https://www.ccn-cert.cni.es/component/vulnerabilidades/view/34497.html
https://www.oracle.com/security-alerts/cpujul2023.html

Affected products: In total there are 32 different Oracle products affected.

Update: Apply the patches recommended by Oracle depending on the product concerned.

Atlassian

Date: 18-07-2023

Description. Atlassian has released several security patches for its products. These patches fix three high severity vulnerabilities. These vulnerabilities could allow an attacker to perform the following actions: Remote code execution. This vulnerability allows an authenticated attacker to execute arbitrary code with high confidentiality impact, high integrity impact, high availability impact and no user interaction (CVE-2023-22505). Remote code execution that allows an authenticated attacker to execute arbitrary code with high confidentiality impact, high integrity impact, high availability impact and no user interaction (CVE-2023-22508). Remote code injection and execution allows an authenticated attacker to modify the actions performed by a system call and execute arbitrary code that has a high impact on confidentiality, a high impact on integrity, a high impact on availability and no user interaction (CVE-2023-22506).

Link: https://www.cisa.gov/news-events/alerts/2023/07/21/atlassian-releases-security-updates
https://confluence.atlassian.com/security/security-bulletin-july-18-2023-1251417643.html

Affected products: Some of the affected products include the following:
- Confluence Data Center & Server.
- Bamboo.

Update: Apply the patches and updates published on the manufacturer's official website for each of the affected products.

EVENTS

Cybersecurity in the health sector

19 September 2023 |

Security event to be held in Madrid both on-site and virtually, with the aim of intertwining the fields of knowledge of health and cybersecurity, in order to strengthen the collaboration of all the figures involved in the protection of information in the field of health. During the congress, different challenges that the digitalisation of healthcare will bring with it from the cybersecurity point of view will be discussed, such as the application of regulations, the problem of remotely connected medical devices and the strengthening of resilience in the sector.

Link: https://ciberseguridadtips.com/congreso-de-ciberseguridad-en-el-sector-salud/

Cyber Security and Cloud Expo

26 - 27 September 2023 |

The event will take place on 26-27 September in Amsterdam and will feature CISO conferences and discussions on current cybersecurity issues in cloud environments, risk management, cyber resilience, privacy and regulation, identity management, among other topics.

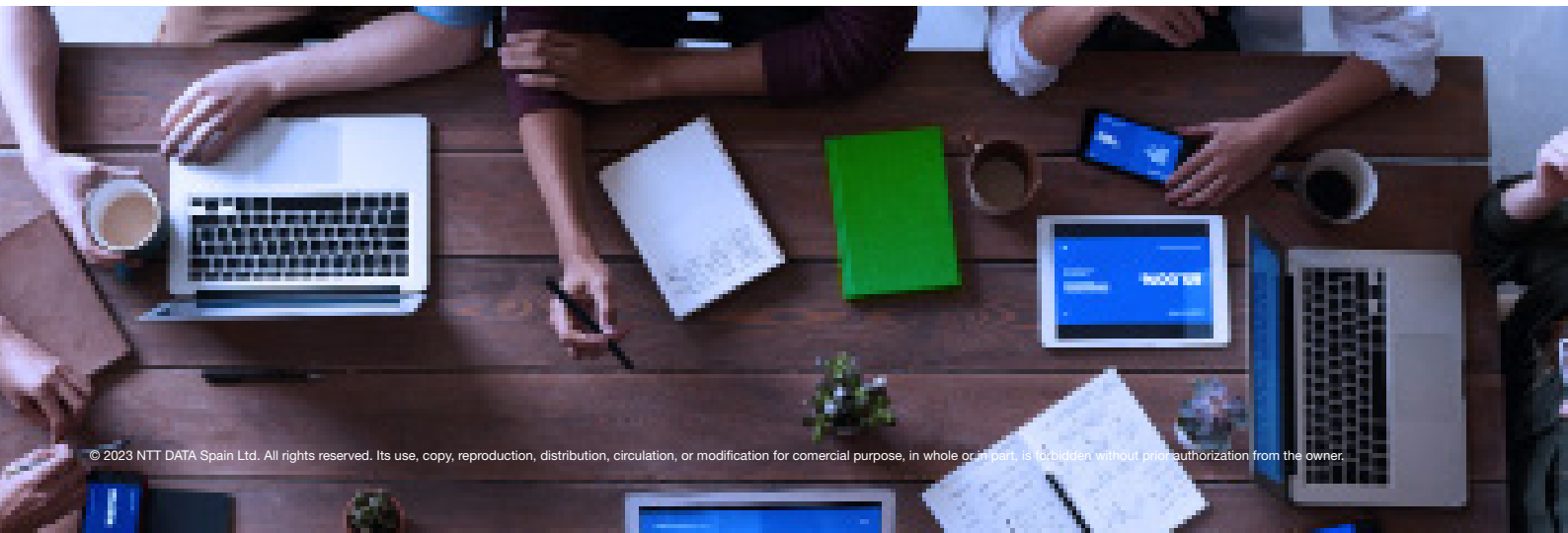
LInk: Cyber Security & Cloud Expo 2023 | Technology Conference | Amsterdam (cybersecuritycloudexpo.com)

Gartner Security & Risk Management Summit

26 - 28 September 2023 |

Gartner Summit to be held in London, focused on risk management for security professionals, which will address the possibilities of strengthening cybersecurity by aligning it with companies' business strategies, generating a more flexible and dynamic environment that enhances security capabilities in digital environments.

Link: https://www.gartner.com/en/conferences/emea/security-risk-management-uk



RESOURCES

Annual Android 0-day vulnerability report – Google

Google has published its annual report summarising the 0-day vulnerabilities detected in Android that have been used by malicious actors. Since these reports began to be published in 2014, this year has been the second with the most 0-day vulnerabilities detected. Among other conclusions, it highlights how, due to manufacturers not having security patches ready in time, vulnerabilities that have been remediated could be used as 0-day vulnerabilities against users, as they are unable to have the necessary updates on their devices.

Link: https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html

BlackLotus

BlackLotus is a UEFI Bootkit designed specifically for Windows, intended to function as an HTTP loader. This tool incorporates a built-in secure boot bypass, as well as Ring0/Kernel protection to protect against any removal attempts once it is deployed. This software consists of two main components: an Agent, which is installed on the target device, and a Web Interface, used by administrators to manage agent-installed devices. Although this attack appeared in forums last year, its source code was released this month and is now accessible to any user.

Link: https://github.com/ldpreload/BlackLotus

LetsCall

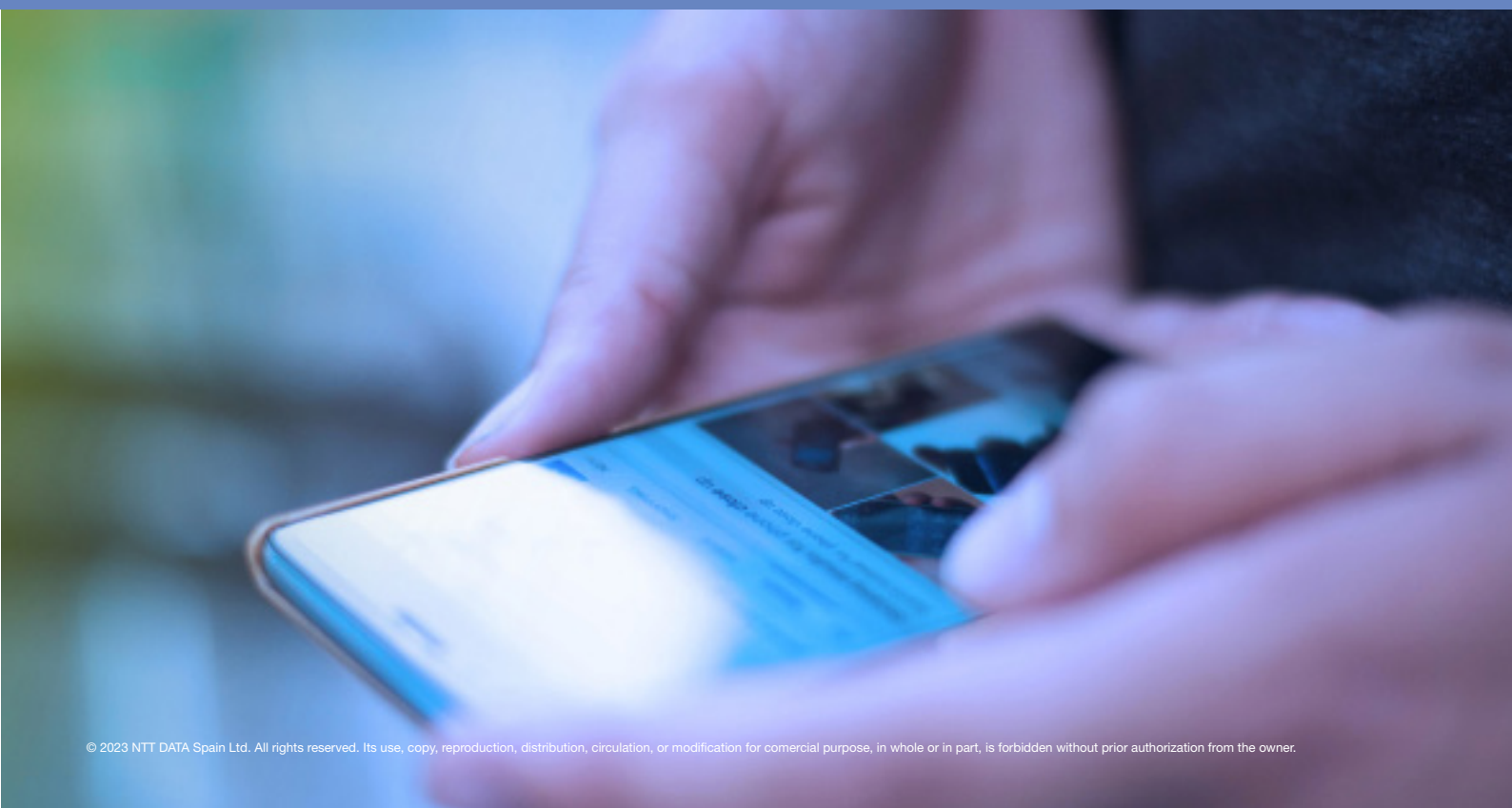
LetsCall is a new toolkit that presents an easy-to-use framework for developing and executing Vishing (Voice over IP Phishing) attacks. This is because it presents all instructions and tools that not only describe how to operate the affected devices, but also how to communicate with potential victims. This framework has already been used in places like South Korea, where this attack has manifested itself in the development of a bank robbery.

Link: https://www.threatfabric.com/blogs/letscall-new-sophisticated-vishing-toolset

WormGPT

A new tool called FraudGPT has emerged, which is currently only provided via Telegram and is the successor to the already available WormGPT. Both FraudGPT and WormGPT provide an artificial intelligence service for designing and developing malware. It provides the same service as ChatGPT but is geared towards malware creation, providing a service with no ethical restrictions or limitations. Although the new FraudGPT service is not yet available, it is already possible to purchase the predecessor tool WormGPT.

Link: https://wormgpt.co/




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