Issue 98 | January 2025

NTT DATA

Radar

The cybersecurity magazine

Strengthening the supply chain: cybersecurity for third-party risk management

By María Pilar Torres Bruna

One of the challenges faced by an organisation or a CISO when defining a cybersecurity strategy is determining the perimeter to protect. Migrating parts of the organisation to the cloud has blurred a once well-defined perimeter, and remote working has further amplified this perception. A third key factor in the cybersecurity of our organisations is our third parties. Some of these are critical to our business operations, and their systems integrate with ours to varying degrees. How can we ensure that they do not become a new attack vector for us?

Third-Party Security refers to managing the risks associated with vendors, partners, and any external entity that has access to an organisation's critical systems, data, or resources. To achieve proper risk management, several roles, in addition to the CISO, must recognise its importance and define or implement the necessary controls. Departments such as procurement, business, or specialised areas like legal, must incorporate security controls into their services and treat them as non-negotiable.

Contractual agreements establish the security foundations that the service-buying company needs to protect its information and business. They also help clearly define the responsibilities and expectations of both parties regarding data protection and risk management. Furthermore, contractual agreements facilitate the management of the relationship with vendors, ensuring that an adequate level of information security is maintained over time. This should be verified through regular audits of the third party.

Finally, it is essential to establish a periodic review and update of contracts to adapt to new risks and regulatory changes. Similarly, ensuring that vendors understand the minimum-security standards they will be required to meet allows them to scale their services more precisely.

Why is this particularly important now? Supply chain attacks are expected to become one of the major threats in 2025, with the number of identified attacks rising significantly. This increase will be particularly evident in critical infrastructure, industrial sectors, and cloud environments, with the emergence of native worms specifically developed for such ecosystems.

Currently, there is already a significant number of attacks on organisations that occur through third parties. Large companies often make substantial investments in cybersecurity, making it increasingly difficult to exploit a direct attack vector. However, their providers or partners may be smaller companies with potentially lower investments in cybersecurity. In such cases, attackers may target one of these companies and, once inside, escalate their access to reach the primary target.

For these reasons, we wanted to start the year by focusing on cybersecurity in the supply chain. The NTT DATA team hopes you find this topic insightful and wishes all our readers a happy 2025.

Maria Pilar Torres Bruna
Cybersecurity Director

The growing threat of data breaches in a digitised world

Cyberchronicles by José Cianci

The evolution of technology has turned information into the most valuable asset of the digital age, making it an attractive target for cybercriminals. These attackers use techniques such as phishing, vishing, and smishing, leveraging seemingly legitimate data—often sourced from previously leaked or sold information on the dark web—to deceive victims, gain financial benefits, or establish an attack vector against the security or reputation of their target.

The protection of confidentiality, one of the pillars of information security, is essential to prevent incidents of this nature. Such events not only impact the organisations responsible but also compromise the individual privacy of users. It is a demonstration of how cyberattacks can erode trust in the handling and safeguarding of personal data, as well as compliance with data protection policies and laws in each country. These incidents jeopardise the economic security of millions of people and the reputation and financial stability of organisations, which may face potential legal sanctions and damage to their public image. This underscores the importance of strengthening protective measures and ensuring regulatory compliance to safeguard data confidentiality.

Following recent incidents, on 1 December 2024, Spain's Tax Agency was allegedly targeted by a ransomware attack carried out by a hacker group self-identified as *Trinity*. The cybercriminals claim to have stolen 560 gigabytes of private and confidential data and are demanding $38 million in cryptocurrency as extortion to prevent the information's publication. Despite the Tax Agency stating that no security breaches or irregularities have occurred in their systems, concerns about the security of taxpayer data have heightened, and questions have been raised about the capabilities of public institutions to withstand cyberattacks.

Double extortion attacks—where data is both encrypted and sensitive information is published—show an upward trend in Spain. Authorities are investigating the case, and cybersecurity measures will be reinforced to prevent future attacks.

At the end of October 2024, Interbank, one of Peru's leading banking institutions, faced a severe data breach that exposed the information of three million customers. This incident, caused by unauthorised access to sensitive data such as account balances, credit card numbers, and API credentials, triggered a wave of panic among users, sparking fears about the security of their savings and leading to an unprecedented bank run. Investigations point to possible internal failures and the involvement of foreign cybercriminals, exposing the lack of a robust cybersecurity infrastructure.

By May 2024, Landmark Admin, a company providing administrative services to major insurers in the United States, suffered a cyberattack that exposed the personal information of over 800,000 individuals. The attackers gained access to sensitive data, including Social Security numbers, driver’s licences, passports, banking details, medical information, and insurance policy details. Although the company detected suspicious activity on 13 May and took measures to protect its systems, the attackers managed to infiltrate again on 17 June. In response, Landmark Admin has implemented stronger data encryption protocols and other security enhancements to its infrastructure, restored the compromised systems, and is working with authorities to investigate the attack.

Additionally, the company has offered those affected 12 months of free credit monitoring and identity theft protection services, along with further guidance to prevent fraud. Although the company has not identified the group responsible for the attack nor has it been attributed to any known ransomware collective, this incident highlights the risks and challenges faced by companies handling sensitive information.

At the start of 2024, Telefónica began investigating a potential data breach affecting 120,000 customers and employees. According to preliminary investigations, the compromised information includes names, addresses, email addresses, and phone numbers, although sensitive data such as bank accounts or passwords have not been identified. The company detected the alleged breach in March 2024, and the data was reportedly offered for sale on online forums by cybercriminals, who claimed they had no use for it and decided to sell it. The breach could be related to vulnerabilities in an external provider.

Telefónica is working to confirm the authenticity of the information and take corrective measures. This incident adds to the company's cybersecurity history, including a global attack in 2017 and another in 2022 that affected parts of its infrastructure and router configurations.

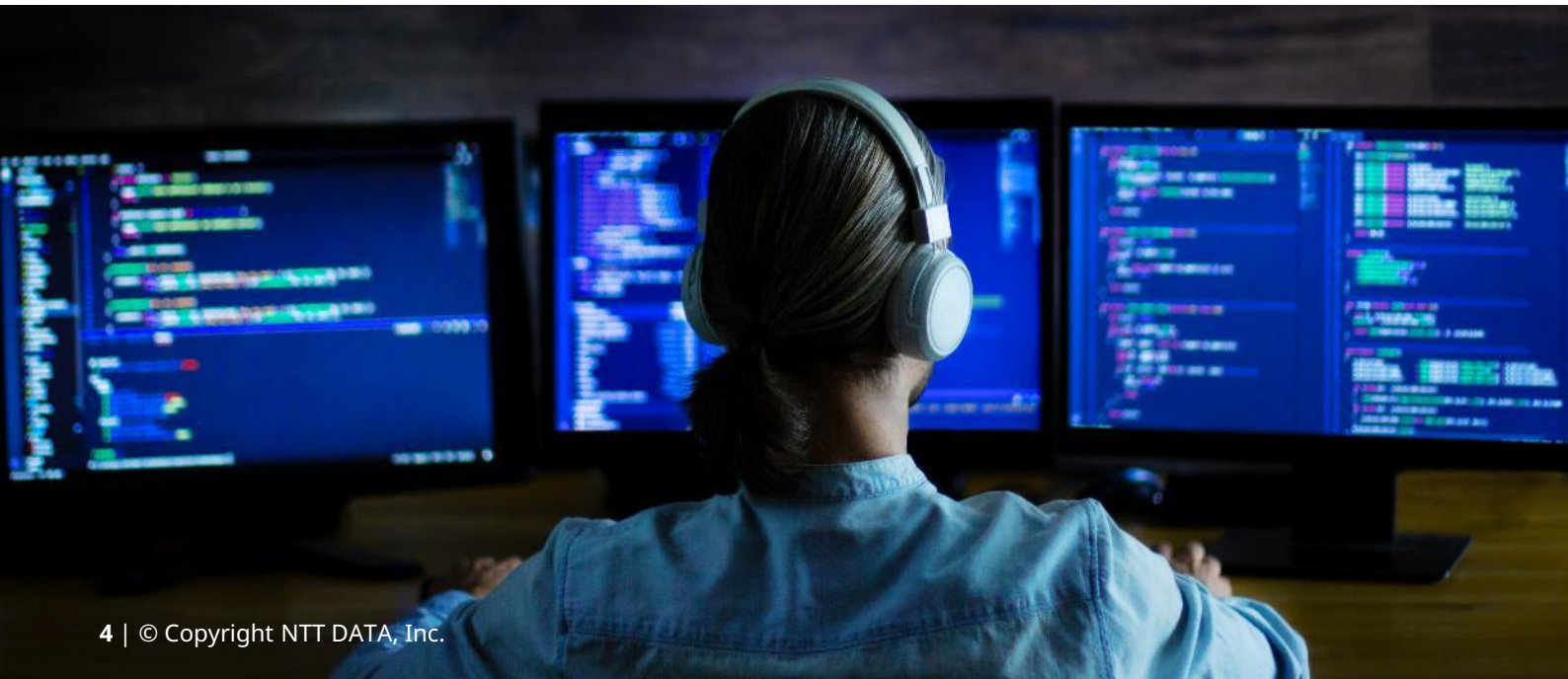
Finally, a massive incident occurred last year, when more than 760,000 records from employees of major companies such as Bank of America, Koch, Nokia, JLL, Xerox, Morgan Stanley, and Bridgewater were leaked online, exposing sensitive information that could have serious consequences. The data, which includes names, email addresses, phone numbers, job titles, and even the names of top executives, originated from a massive hack the previous year, where a group of cybercriminals linked to the Russian Cl0p gang exploited a zero-day vulnerability in MOVEit file transfer software to steal information from thousands of organisations.

The attack affected nearly 100 million people and 2,800 companies, and the information now leaked is considered valuable by cybercriminals, as it allows them to carry out social engineering attacks such as phishing or identity theft, with access to detailed organisational data.

Each of these cases highlights not only the growing threat of data breaches but also the vulnerability to increasingly sophisticated attacks. Cybercriminals, by exploiting security flaws in organisations, not only steal information but also undermine public trust and compromise the economic stability of the victims.

This scenario underscores the urgent need to strengthen cybersecurity policies, adopt more advanced technologies, and promote education for customers and employees about cyber risks. Data protection is not only a legal obligation but a strategic necessity to mitigate risks and ensure that trust and security are not compromised.

José Cianci Pacheco
Cybersecurity Junior Engineer



The importance of providers and the supply chain in cybersecurity

Article by Julissa Calderón

Cybersecurity when it comes to providers and the supply chain is an aspect that has gained importance within companies in the areas of cyber defence and cyber resilience. In recent years, attacks caused by the exposure of information through third parties have increased. Cybercriminals today view trusted providers as an important means to reach their final target and seek attack vectors that allow them to breach data or put the organisation at risk. For this reason, it is crucial for companies to be prepared through security in their relationships with providers.

Will there be any company that does not rely on third-party subcontracted services?

While companies handle the core processes of their businesses, they often need specialised providers for specific services/products to support and integrate them into their value chain. Of course, not all providers support critical processes of the company, but some do, and for this reason, they even become strategic partners.

What company does not share business information within the framework of the contract with its providers?

Providers may provide goods or services and depending on the terms of their contract and scope, they need to access information about the company. In certain cases, beyond just knowing the information, they may need to work with it, which implies a different level of access. In the technological field, some third parties need access to the company's network and even information systems to perform their tasks. Therefore, it is essential that security measures for providers are established, followed, and monitored by the organisation to ensure that the measures applied are similar to or even better than those determined within the company itself.

Do all companies have security policies in place, shared with their providers, that protect the information and the environment in which it is shared?

Not all organisations make efforts to establish security and cybersecurity conditions in their agreements with providers. In some cases, they only include general clauses in contracts to safeguard confidentiality, integrity, and continuity of information within the framework of the product or service. However, despite the risks, many companies lack adequate cybersecurity measures that are controlled and monitored.

What considerations should be made regarding cybersecurity measures?

1. Regarding cybersecurity, it is important to identify those providers that, due to the services they provide, meet any of the following criteria:
    - Providers that support critical business processes.
    - Providers that access the company's information assets
    - Providers that are custodians of information assets.

    Identifying these providers is the first step to establish and apply security measures according to their participation and involvement in the company's security and cybersecurity.
2. It is important to establish information security and cybersecurity measures that providers must comply with throughout the entire lifecycle: during contracting, deployment of service or operation, and contract closure.

For this, it is important to integrate these specifications with the procurement and purchasing processes, as well as with legal aspects that are analysed as part of the contracts. It is relevant to take into account the following key aspects:

- Access limits.
- Establish secure communication channels.
- Connection device security.
- Cyber incident response plans.

3. Apply information security and cybersecurity risk analysis to those providers as needed. It is recommended to start with providers that support critical processes and/or are related to the company's most important information assets.
4. Monitor the compliance of the measures applied by the providers, whether technical, legal, or organisational in relation to cybersecurity, in order to have clarity about their compliance and make recommendations if necessary.
5. Raise awareness among providers regarding their participation and the importance of their role in safeguarding cybersecurity and information security.

There are several international frameworks and standards that establish guidelines to improve protection in relationships with providers. For example, the ISO 27001:2022 standard incorporates certain control aspects to ensure security in the different layers of Information and Communications Technology. Likewise, NIST SP 800-161r1 contains specifications for managing cybersecurity risks in the supply chain.

Cyber threats are constantly evolving, so it is crucial for companies to stay alert and take proactive measures to protect their supply chains from cybersecurity risks.

Julissa Calderón Loayza
Cybersecurity Expert Associate

Strengthening application security programs through Generative Artificial Intelligence

Article by Martín Bedoya

Application security has been on the rise since the software industry discovered that shifting software assurance to the left is more efficient in the long run than simply running tests. Application security refers to practices and tools designed to protect the software development process from threats, ensuring that controls are included from the outset to protect confidentiality, integrity, and availability.

An application security program is implemented by integrating controls into the software lifecycle, using automated tools, training teams, and constantly monitoring to detect and mitigate vulnerabilities. The strategy depends on each organisation, its risk appetite, development process, and the allocated budget.

Implementing an application security program is a challenge for organisations due to the lack of specialised resources, resistance to change, and the need to balance security with delivery timelines. In terms of governance, two strategies are commonly employed in an application security program: On one hand, security professionals are integrated into development teams to support assurance activities. This approach is highly effective but costly to maintain and scale.

On the other hand, specific security capabilities are often provided, which are activated on demand by development teams. This model, while cheaper and more scalable, loses agility and shifts some security activities to the team members themselves. Regardless of the strategy implemented, application security programs can be optimised using artificial intelligence.

Generative artificial intelligence offers the possibility to optimise security activities at each phase of the software lifecycle by automating threat detection, improving the accuracy of risk assessments, identifying vulnerabilities, suggesting balanced remediations, and, of course, reducing security professionals' bias.

Through the use of generative artificial intelligence, security professionals evaluate user stories to identify potential risks, prioritise them, and recommend mitigation measures, thus optimising security planning from the earliest stages of development. This process allows for an increase in the number of user stories evaluated by each professional, substantially improving the capacity of application security programs.

Furthermore, generative artificial intelligence enables the industrialisation of threat models based on user stories or software diagrams, reducing the business understanding required and significantly decreasing the time spent by consultants to identify potential threats. In the long run, this allows for addressing a higher demand from development teams.

Finally, static source code analysis based on generative artificial intelligence enables the identification of insecure patterns in the code that may not be detected by traditional tools. It also provides detailed explanations and offers recommendations to correct vulnerabilities, reducing technical debt and improving time to market.

One of the major challenges of application security programs is reducing bias. Professionals with defensive training tend to secure software through controls, while those with offensive experience tend to focus on attacks. Artificial intelligence helps reduce this bias, provided the interaction between the professional and the generative model is effectively structured.

Artificial intelligence has become an essential tool for strengthening application security, offering capabilities to automate complex processes and reduce human errors. In a world where applications are growing in volume and complexity, it is crucial to address emerging threats quickly and accurately. Integrating artificial intelligence into the software lifecycle assurance will allow organisations to cover a larger application ecosystem and improve their security posture.

Martín Bedoya Rodríguez
Cybersecurity Expert Engineer

Cyber-insurance as a shortcut to supply chain attacks

Trends by Jose Cárdenas

The complexity of supply chain security lies in the interconnection and dependence on multiple actors, technologies, and locations that make up modern supply chains. This complexity is heightened by globalisation, as components originate from various regions, each with differing cybersecurity regulations and potential geopolitical risks. This necessitates robust approaches, such as the use of cyber-insurance to mitigate the financial and operational consequences of an attack.

Agencies like Cybersecurity Ventures estimate that the global annual cost of software supply chain attacks for businesses will reach an astonishing $138 billion by 2031, up from $60 billion in 2025 and $46 billion recorded in 2023. With these projections, it seems cybercriminals may be outpacing major corporations in terms of profits… while we, once again, bear the consequences.

Cyber-insurance

Given the rapidly increasing impact costs projected for the coming years, the need to invest in cyber-insurance alongside efforts to secure corporate systems is becoming more pressing. Various companies now offer cyber-insurance as part of their service portfolios, aiming to provide businesses with relief and peace of mind by reducing the impact of cyberattacks such as ransomware or DDoS incidents. However, the terms of cyber-insurance are evolving as the number of victims continues to rise.

Higher premiums

The rise in cyber-insurance premiums reflects the increasing complexity of cyberattacks. Insurers have adjusted premiums to account for the higher costs associated with these incidents.

However, this increase in cost and coverage has compelled companies to demonstrate that they have robust security measures in place, such as multi-factor authentication and ransomware protection, to qualify for competitive terms.

Increase in cyber-insurance Exclusions

While cyber-insurance policies can provide extensive coverage, certain incidents are often excluded, such as:

- **Social Engineering**: Since social engineering attacks like phishing manipulate individuals into compromising cybersecurity from within, cyber policies do not always cover these losses.
- **State-Sponsored Attacks**: Many cyber policies classify these attacks as acts of war and exclude them from coverage.
- **Cyber-attacks Exploiting Known Vulnerabilities**: If attackers exploit a vulnerability that the company was aware of but failed to address, many cyber policies will deny the claim.

Cyber-insurance segmentation

The segmentation of cyber-insurance has become a key trend due to the diversity of risks faced by different sectors. Instead of offering generic policies, insurers are tailoring their products to the specific needs of each industry, such as healthcare, banking or e-commerce. For example, companies in the healthcare sector require protection against the theft of medical data, while technology organisations need coverage for the loss of intellectual property.

This approach enables insurers to provide more precise and effective coverage aligned with the particular risks of each client, which also helps optimise premium costs.

Stricter insurers

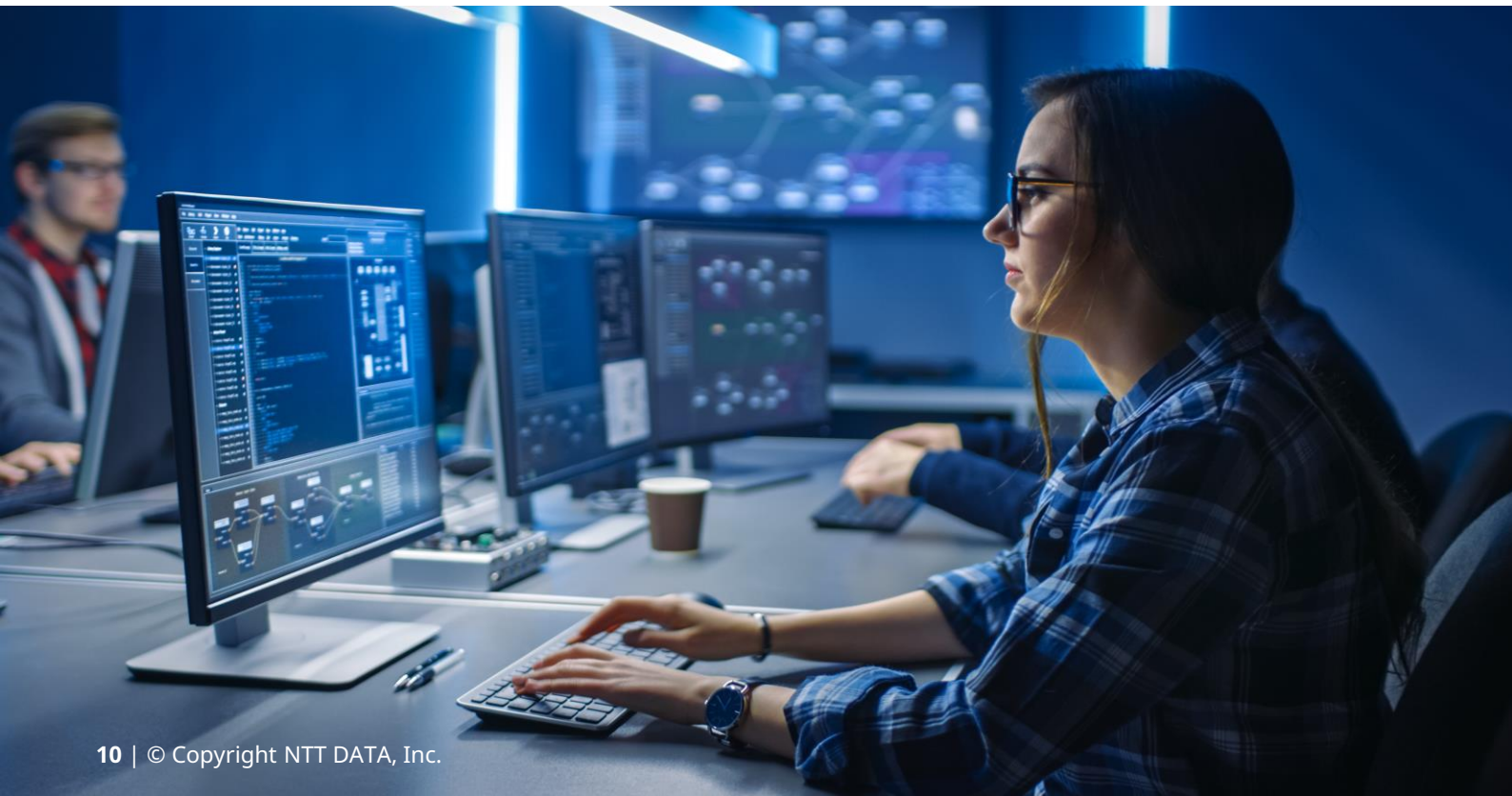
Insurers are implementing stricter requirements. Some do not even offer an insurance quote if the company does not have security measures such as multi-factor authentication, data encryption, Zero Trust, or similar policies.

Additionally, some insurance companies are adopting a more consultative approach, providing insured businesses and owners with access to security tools and service providers to help strengthen their cybersecurity posture.

Conclusion

Organisations must adapt to an ever-changing threat environment, which involves not only having a robust security strategy but also incorporating solutions such as cyber-insurance. These insurances are becoming a key tool for reducing the financial and operational risks arising from cyberattacks, although their effectiveness depends on companies implementing the appropriate preventive measures. Furthermore, collaboration with insurers and security service providers is becoming a crucial element in strengthening organisational resilience against cyberattacks.

Jose Cárdenas Camacho
Cybersecurity Analyst



Phishing through DocuSign: malware distribution from trusted sources.

Trends by Samuel Santos and Nicolas Fernandez

At the beginning of last November, researchers at Wallarm raised the alarm about a recent phishing tactic in which cybercriminal groups were reportedly exploiting the API of the company DocuSign, a well-known platform for document signing and electronic invoice delivery.

Attackers have reportedly found a way to send emails that, originating from the legitimate platform itself, precisely mimic the invoices and notifications regularly sent.

According to sources such as Trellix, this cyberattack is particularly targeting Japan, North America, Oceania, and Central Europe, distributing a modified version of the malware known as Remcos RAT, designed for remote command execution on victims' devices.

What does the attack involve?

This scheme revolves around the mass distribution of DocuSign emails containing tampered Office documents. These files include OLE (Object Linking and Embedding) objects, which initiate part of the document loading process from an external source controlled by the attacker.

By leveraging this external document loading, cybercriminals exploit the publicly known vulnerability CVE-2017-0199 present in certain versions of the Office suite. This allows them to execute an HTA (HTML Application) file obfuscated through multiple layers of JavaScript, Visual Basic, and PowerShell code.

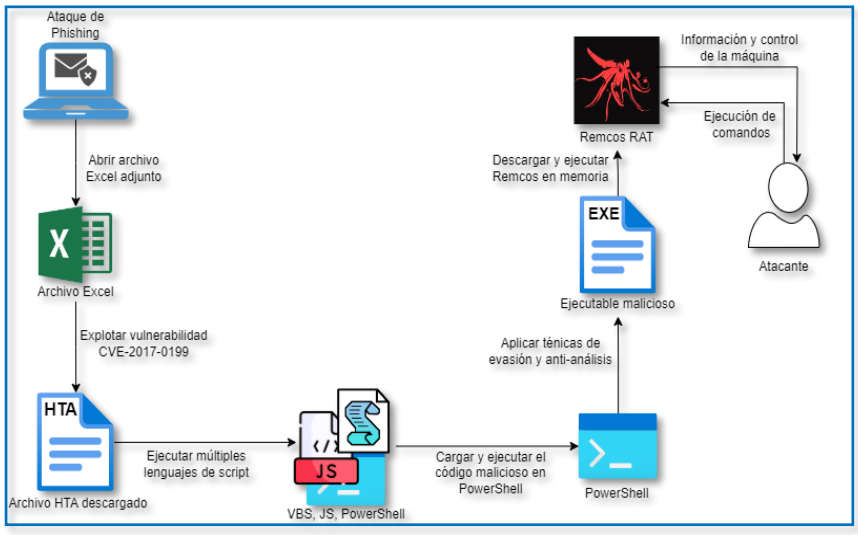
The ultimate goal of this code is to execute a PowerShell console, which, using various evasion techniques, will run a variant of the malicious software known as Remcos RAT, allowing cybercriminals to connect to the victim's machine via a Command & Control server.

From that server, the attackers can control the infected device, execute commands, move laterally or vertically within the network, and extract sensitive information.

Why is this attack effective?

The strength of this attack vector lies in the abuse of the legitimate DocuSign API, marking an evolution in traditional phishing. Rather than deceiving the user through malicious servers and emails with a false appearance of legitimacy, attackers now exploit trusted platforms as their attack vectors, deceiving their targets with communications that appear entirely authentic.

By sending emails through DocuSign, cybercriminals manage to make their messages appear legitimate to security filters, bypassing traditional defences.



This allows them to bypass traditional phishing detection mechanisms and increase the email open rate, as the recipient recognises DocuSign as a trusted source.

Conclusion

The use of the DocuSign API to carry out phishing attacks highlights the constant innovation of these types of actions, exploiting trusted platforms to execute highly effective malware campaigns. This attack, which takes advantage of old vulnerabilities in commonly used software, underscores the importance of understanding and staying vigilant against threats in an increasingly complex cybersecurity environment.

Nicolas Fernandez
Cybersecurity Analyst

Samuel Santos
Cybersecurity Analyst

Vulnerabilities

Critical vulnerability in the Java AsyncHttpClient (AHC) library

Date: December 2, 2024
CVE: CVE-2024-53990

CVSS: 9.2

CRITICAL

Description

The AsyncHttpClient (AHC) library allows Java applications to execute HTTP requests and manage responses asynchronously in a straightforward manner.

However, a vulnerability CVE-2024-53990 has been discovered, where the automatic CookieStore can overwrite explicitly defined cookies if they match by name. In multi-user environments, this could lead to the incorrect usage of these cookies, potentially causing authentication issues or data exfiltration.

Solution

Backend developers using third-party authentication and token renewal may experience authentication failures and session management issues due to the unintended overwriting of cookies.

Therefore, the vendor recommends updating to version 3.0.1 as soon as possible.

Affected Products

This vulnerability affects the following version:

- Version 3.0.0 of the AHC library.

References

- incibe.es
- github.com

Vulnerabilities

Critical DoS vulnerability at NASA

Date: December 5, 2024
CVE: CVE-2024-54130

CVSS: 9.2

CRITICAL

Description

NASA has discovered a new vulnerability in its Interplanetary Overlay Network (ION), a model of networks designed to support delays and disruptions (DTN).

The critical vulnerability CVE-2024-54130 causes the node to stop responding to incoming packets, triggering a denial of service (DoS) scenario. This occurs when a packet arrives with an endpoint identifier (EID) whose value is set to dtn:none.

As a result, space communications and data exchanges could be affected.

Solution

To mitigate the vulnerability, it is recommended to follow these steps:

- Update to version 4.1.3s or later of ION-DTN-BPv7.
- If immediate updating is not possible, implement access controls to reduce exposure.
- Analyse the systems to identify any unusual behaviour.
- Consider implementing a system to block or clean packets with unexpected EIDs.
- Develop and maintain an action plan in case of successful exploitation.

Affected Products

The vulnerability affects the following versions:

- Versions prior to 4.1.3s of ION-DTN-BPv7.

References

- incibe.es
- nvd.nist.gov
- github.com

Security patches for Veeam Service Provider Console (VSPC)

Date: December 3, 2024
CVE: CVE-2024-42448 and 1 more

Critical

Description

Veeam has released updates to mitigate two vulnerabilities (1 critical and 1 high) in VSPC, a remote BaaS and DRaaS platform that manages backups:

- CVE-2024-42448: A critical vulnerability (9.9) that allowed an administrative agent to execute remote code, potentially leading to subsequent attacks.
- CVE-2024-42449: An administrative agent could extract NTLM hashes and delete files from the VSPC service account.

For both vulnerabilities, it was necessary for the agent to have authorisation on the VSPC server. This vulnerability highlights the importance of access controls.

Affected Products

The security updates affect the following versions:

- VSPC, version 8.1.0.21377.
- All 8.X versions prior to 8.1.0.21377.
- All 7.X versions.

Solution

Veeam recommends upgrading to version 8.1.0.21999 of VSPC as soon as possible.

References

- socradar.io
- qualys.com
- blog.segu-info.com

QNAP Updates to Critical SQL Injection Vulnerability

Date: December 6, 2024
CVE: CVE-2024-50387

Critical

Description

A series of updates have been released to address a critical vulnerability (CVSS: 10.0) detected in several versions of the QNAP operating system. The vulnerability in question is identified as CVE-2024-50387.

If exploited, this vulnerability could allow remote attackers to inject malicious SQL code, potentially compromising exposed databases.

These SQL code injections could undermine key security aspects such as confidentiality and integrity.

Affected Products

The products affected by this vulnerability are:

- SMB Service versions prior to 4.15.002.
- SMB Service h versions prior to h4.15.002.

Solución

It is recommended to update SMB Service to the latest version where the issue has been fixed:

- SMB Service 4.15.002 and later
- SMB Service h4.15.002 and later

References

- incibe.es
- nvd.nist.gov
- qnap.com

Events

AI Infrastructure & Architecture Summit 2025
January 13-15

The AI Infrastructure & Architecture Summit 2025 will take place from January 13 to 15, 2025, in London, United Kingdom. This event will focus on building customised AI models and scalable infrastructures for enterprise-level deployments. It will feature sessions led by experts from organisations such as Microsoft, HSBC, Citi, Wells Fargo, L'Oreal, and AstraZeneca, covering topics such as data platform modernisation, computational resource optimisation, and MLOps strategies.

Link

I Conference on Cybersecurity in the Financial Sector
22 January

The 1st Cybersecurity Conference in the Financial Sector, organised by Red Seguridad and the Borredá Foundation, will take place on January 22, 2025, in an online format (pre-recorded) with limited in-person attendance by invitation. Under the theme "DORA: Strengthening a Solid Resilience Framework," the event will analyse the impact of the DORA regulation on the continuity and quality of financial services, emphasising cybersecurity as a strategic imperative. It will feature renowned CISOs and experts from institutions such as BBVA, Mapfre, ING, and Grupo Santander.

Link

CyberSec Asia 2025
22-23 January

CyberSec Asia 2025 will take place on January 22 and 23, 2025, at the Queen Sirikit National Convention Centre (QSNCC) in Bangkok, Thailand, as part of the "CyberSec Asia x Thailand International Week 2025," organised by NCSA. This event brings together leaders in cybersecurity, data management, and cloud solutions from the CLMVT regions (Cambodia, Laos, Myanmar, Vietnam, and Thailand) and APAC. With over 5,000 attendees, 140 exhibitors, and 100 speakers, it is a key platform to explore trends, government initiatives, and growth opportunities in the industry, as well as to establish strategic connections.

Link

The AI Regulation Summit 2025
27 January

The AI Regulation Summit will be held on January 27, 2025, at the London Centre. This event will bring together international experts to discuss global regulatory approaches to artificial intelligence, including the UK's AI Bill, the EU's AI Regulation, and the US strategy on AI. Key topics such as data privacy, consumer protection, cybersecurity, intellectual property, and AI ethics will be examined. Additionally, best practices in risk management for AI system providers and users will be explored.

Link

OPEX Week: Business Transformation World Summit 2025
27-29 January

The OPEX Week: Business Transformation World Summit 2025 will take place from January 27 to 29, 2025, in Miami, celebrating its 26th edition. This event will bring together over 100 speakers, including Chief Transformation Officers from major brands such as Walmart, Goldman Sachs, McDonald's, L'Oreal, and Air Canada, who will share their insights on business transformation in the age of AI. The agenda includes 14 workshops, 16 interactive discussion groups, 4 industry-focused sessions, and an AI innovation zone.

Link

Resources

➢ NIS Investments 2024 by ENISA

The "NIS Investments 2024" report by the European Union Agency for Cybersecurity (ENISA) assesses the impact of the NIS 2 Directive on cybersecurity investments and maturity within the European Union. Based on data collected from 1,350 organisations across the 27 member states, the report provides a detailed view of the state of cybersecurity both before and after the implementation of the NIS 2 Directive. Additionally, it focuses on key metrics for critical sectors and manufacturing, offering a framework for conducting future assessments. This report is a valuable tool for policymakers and organisations seeking to align with the cybersecurity standards and objectives set at the European level.

Link

➢ Cybersecurity Snapshot: AI Security Roundup: Best Practices, Research and Insights of Tenable

The Tenable article provides an overview of best practices and new research related to artificial intelligence (AI) security. It includes analysis on how to protect AI-powered applications, mitigate risks associated with "Shadow AI," and integrate zero-trust strategies into critical infrastructures. Furthermore, it highlights innovative tools and approaches to address emerging cybersecurity threats.

Link

➢ New Personal Data Protection Law in Chile

The Constitutional Court of Chile has approved the new Personal Data Protection Law, aligning it with international standards. This law strengthens citizens' rights over their information, establishes strict obligations for organisations in its handling, and creates a specialised regulatory agency. It is a key step towards greater security and privacy in the country's digital environment.

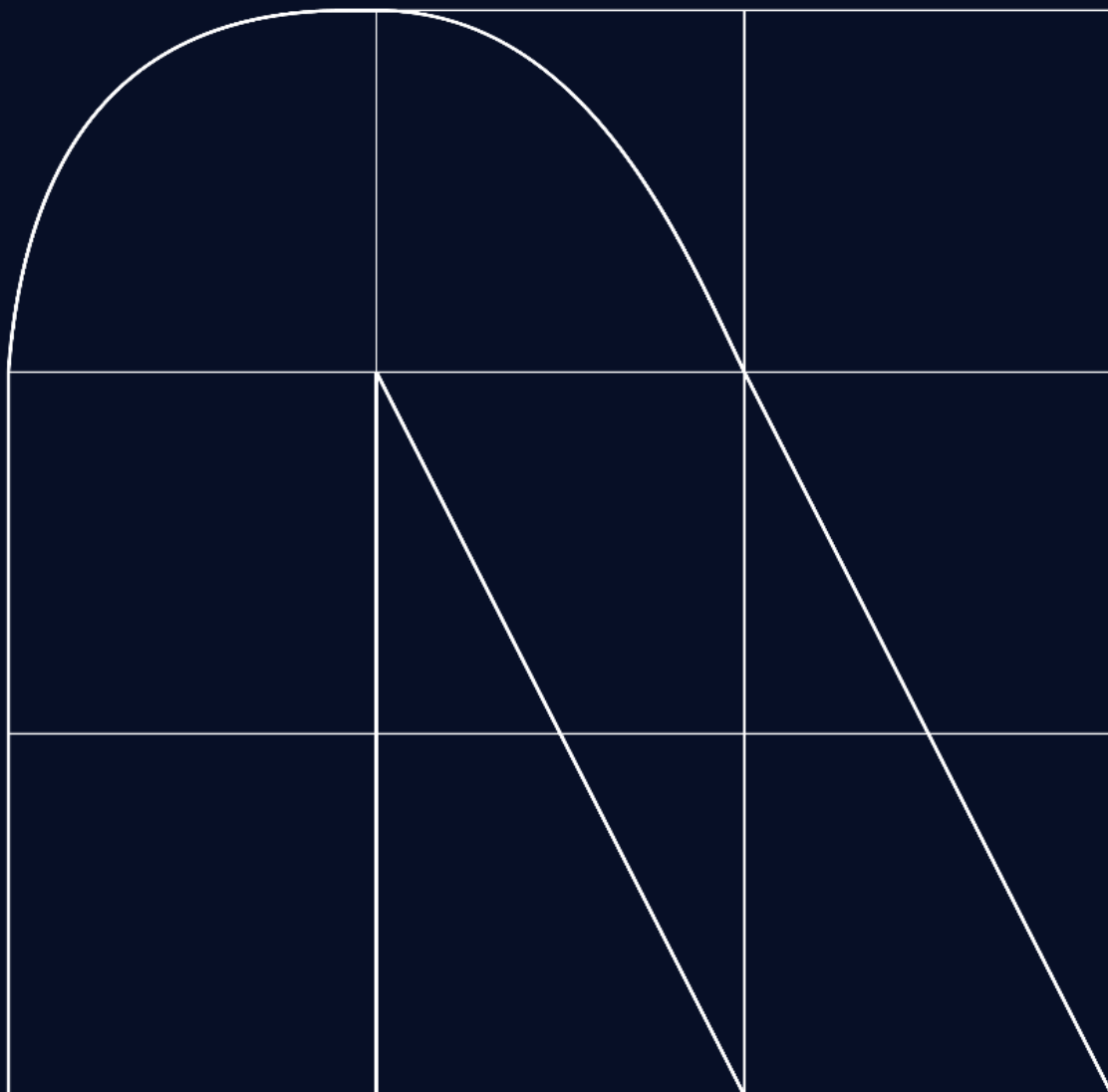
Link

➢ New Personal Data Protection Regulation in Peru

The new regulation of Law 29733, the Personal Data Protection Law, has been published in the official newspaper *El Peruano*. This regulation represents a significant advancement for Peru in the digital age, incorporating new elements such as preventive impact assessments, codes of conduct, incident reporting within 48 hours, and the right to data portability. It also strengthens the protection of minors, modernises security with international standards, and offers flexibility in territorial compliance, aligning the country with global best practices.

Link

Subscribe to RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com