MERIDIAN GROUP

Weekly *Report*

13/01/2025

TLP: WHITE

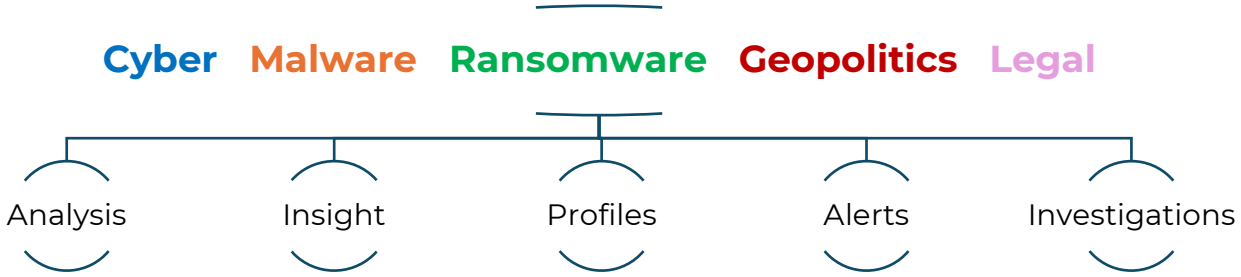
MERIDIAN S.R.L

Viale Erminio Spalla, 9-00142 Roma (RM) | +39 06 99 70 66 80 | P.IVA/CF 13693001003 | meridiangroup@legalmail.it | info@meridian-group.eu | www.meridian-group.eu |

Summary

Methodologies and Resources

The Cyber Intelligence (CI) team uses the following methods and resources for news analysis and for acquiring information useful in containing cyber-attacks.



The CI Team, through this weekly report, aims to provide timely and accurate analysis regarding the aforementioned areas, enabling readers to stay informed about the latest news concerning new vulnerabilities, potential threats, and changes in the geopolitical landscape.

The daily news analysis on the Kitsune platform is essential for CI analysts to monitor and understand emerging risks in the various categories mentioned above, thus allowing them to prevent or mitigate potential threats to customer security.

GEOPOLITICS

Russia orders Yandex to obscure maps and images of strategic refinery

AN UNPRECEDENTED COURT RULING MANDATES THE TECH GIANT TO REMOVE INFORMATION ABOUT A SENSITIVE OIL FACILITY TARGETED BY REPEATED UKRAINIAN ATTACKS.

A Russian court has ordered Yandex, the country's leading technology company, to remove maps and images of one of Russia's largest oil refineries. The decision was prompted by repeated Ukrainian drone attacks on the facility.

According to the state-run TASS news agency, this marks the first ruling requiring Yandex to eliminate information about strategic facilities tied to the defense industry. Yandex, often referred to as the "Google of Russia", operates the nation's most widely used search engine, along with services such as maps, email, transportation, and e-commerce.

The refinery in question was not identified in official documents, but independent sources believe it to be the state-owned Rosneft facility in Ryazan. During the ongoing conflict in Ukraine, Rosneft has supplied materials to Russian armed forces and has been targeted by four Ukrainian attacks over the past year, resulting in structural damage and injuries to employees.

A government agency initiated the legal action against Yandex after discovering that detailed maps and images of the refinery were publicly accessible. When direct negotiations with Yandex failed, the agency sought judicial intervention.

The court ruling requires Yandex to remove or obscure images of workshops, compression stations, storage tanks, and other sensitive areas of the facility. The court stated that the public availability of such information "compromises national defense capabilities" and "delays the delivery of materials" to the armed forces. Yandex was also fined as part of the ruling.

The issue of disclosing strategic imagery affects both Russia and Ukraine. Last November, Ukraine accused Google of exposing its military sites in an online map update. Ukrainian officials emphasized the risks of revealing sensitive information, such as the locations of air defense systems.

Google Ukraine responded by stating that the satellite images in question were over a year old and already publicly available. "We avoid publishing recent images of conflict zones," the company said.

MALWARE

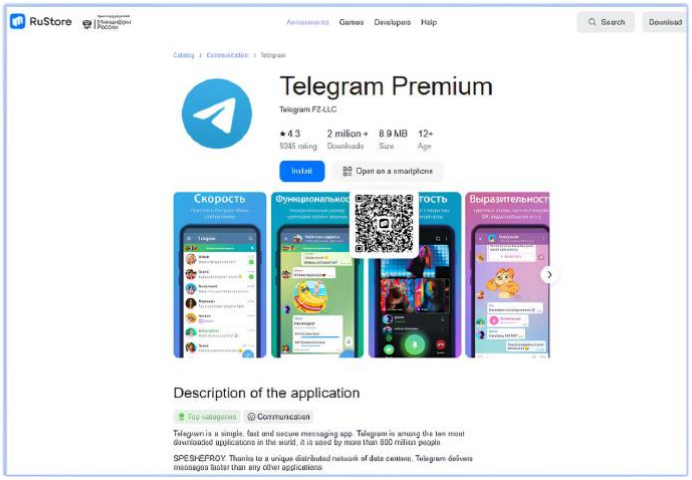
FireScam: the Android malware Masquerading as Telegram Premium to steal sensitive data

A SOPHISTICATED CYBERATTACK LEVERAGES PHISHING SITES AND MALICIOUS PERMISSIONS TO STEAL CREDENTIALS, MONITOR ACTIVITY, AND MAINTAIN REMOTE CONTROL OVER INFECTED DEVICES.

A sophisticated Android malware, dubbed FireScam, has been identified masquerading as a premium version of the Telegram messaging app. Its goal is to steal sensitive data and maintain persistent remote control over compromised devices. FireScam spreads through a phishing site hosted on GitHub.io, which imitates RuStore, a popular Russian app store operated by tech giant VK.

The attack begins with the download of an APK file named GetAppsRu.apk, provided via the phishing site rustore-apk.github[.]io. Once installed, the APK acts as a "dropper," delivering the primary payload designed to steal sensitive data such as notifications, messages, and app-related information, which are sent to an endpoint on Firebase Realtime Database.

The dropper app requests numerous permissions, including the ability to write to external storage and install, update, or delete apps on Android 8 or later. Notably, it exploits the ENFORCE_UPDATE_OWNERSHIP permission, allowing it to designate itself as the owner of updates. This blocks legitimate updates from other sources, ensuring the malware's persistence on the device.



FireScam employs obfuscation and anti-analysis techniques to evade detection. Once installed, it monitors notifications, user activity, clipboard content, and e-commerce transactions, collecting data of interest. It can also download and analyze images from specified URLs.

When the "Telegram Premium" app is launched, the malware requests additional permissions to access contacts, call logs, and SMS messages. It then displays a login page from Telegram's official website via a WebView to steal user credentials, initiating data collection regardless of whether the victim logs in or not.

The malware registers a service to receive Firebase Cloud Messaging (FCM) notifications, enabling operators to issue remote commands and maintain covert access to the device. Simultaneously, it establishes a WebSocket connection with a command-and-control (C2) server to exfiltrate data and coordinate further actions.

Additionally, the phishing domain hosted another malicious artifact called **CDEK**, likely referencing a Russian package tracking and logistics service. However, this component could not be fully analyzed during the investigation.

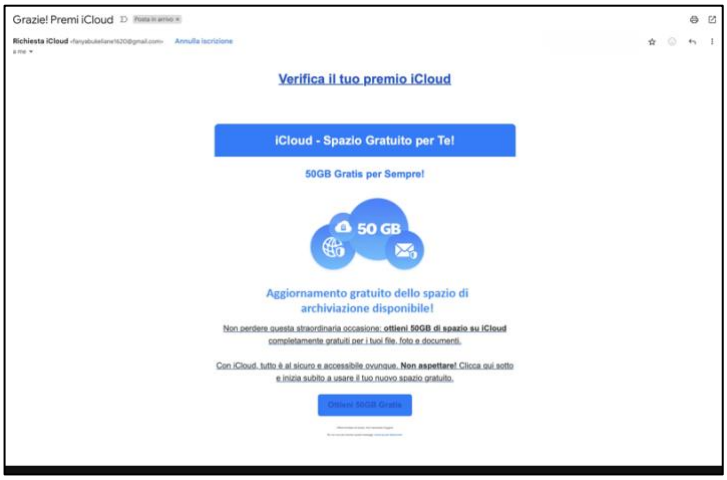
The identity of FireScam's operators, how users are directed to these sites, or whether techniques like SMS phishing or malvertising campaigns are employed remains unclear.

CYBER

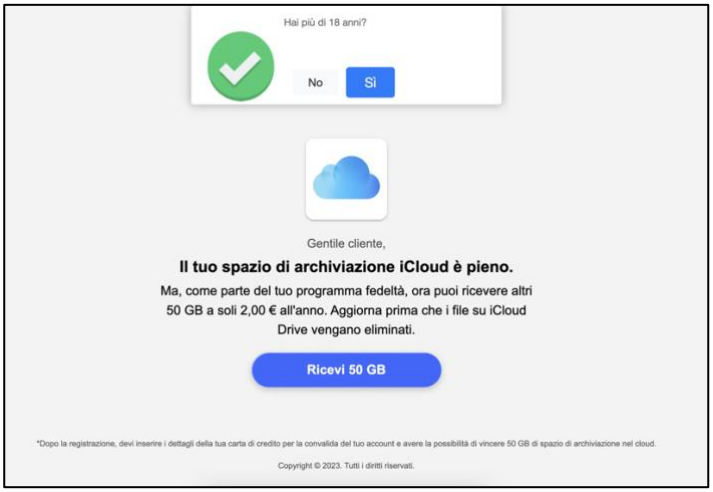
New phishing campaign targeting iCloud

FRAUDULENT EMAILS PROMISE FREE STORAGE TO TRICK VICTIMS INTO SHARING PERSONAL INFORMATION AND CREDIT CARD DETAILS

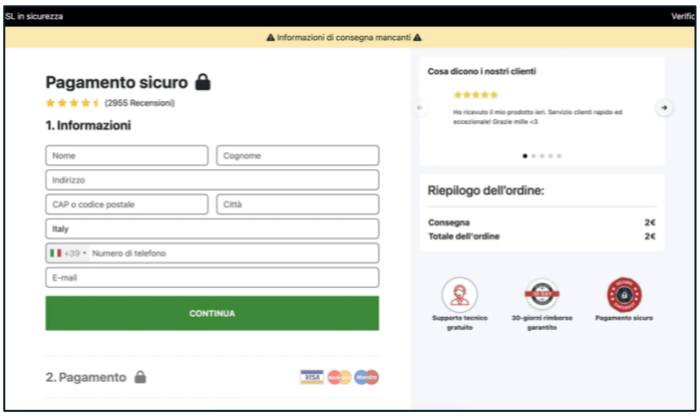
A sophisticated phishing campaign themed around the iCloud service has recently been identified. This campaign aims to fraudulently obtain personal information from potential victims, including credit card details. Delivered through email, the campaign lures users with the promise of a reward: free additional storage space on Apple's iCloud service.

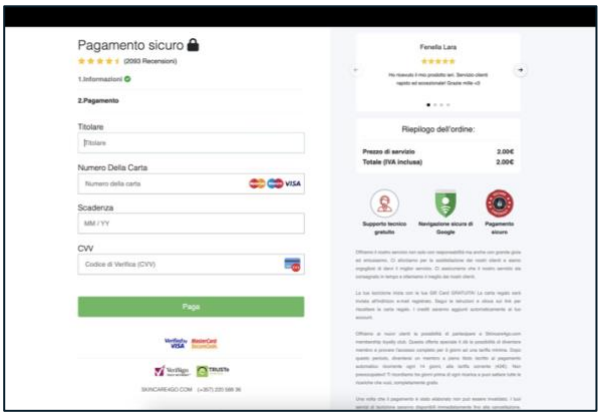


The hyperlink included in the email directs users to a specially crafted portal that promotes the possibility of acquiring 50 GB of additional storage for just €2 per year—an obvious inconsistency compared to the claims made in the email.

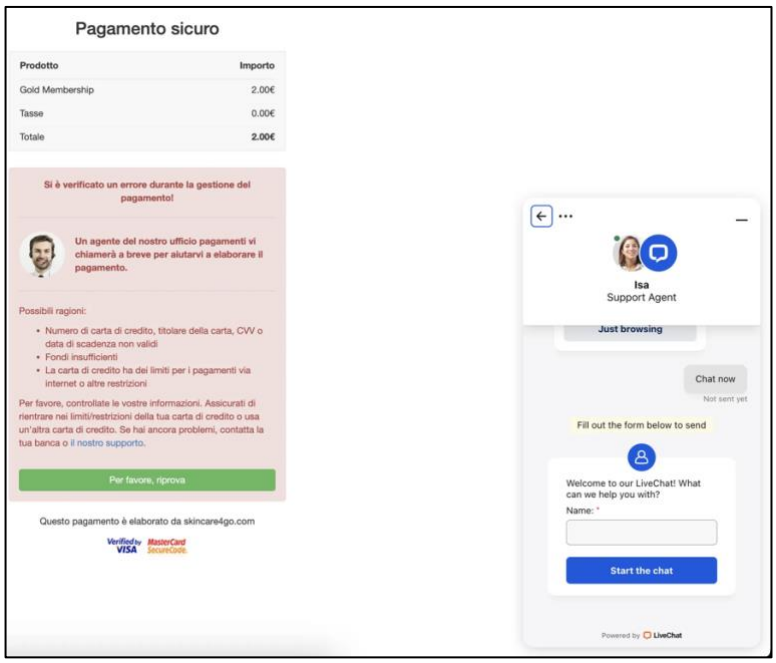


By clicking the "Receive 50 GB" button, victims are prompted to provide sensitive information, such as personal details and credit card information, in a manner similar to the activities described in the report AL01/250103/CSIRT-ITA.





Once the data is entered, the fraudulent site displays a payment failure screen, accompanied by an explanatory message regarding the alleged reasons for the unsuccessful transaction. This screen also includes a support chat feature, managed by a bot. By interacting with this functionality, the system requests a description of the issue encountered, subsequently urging the victim to use additional payment cards and redirecting them to alternative payment portals set up to perpetuate the scam.



GEOPOLITICS

Strengthening alliance between Russia and North Korea: risk of advanced military technology exchange

MOSCOW MAY PROVIDE PYONGYANG WITH SATELLITE AND SPACE TECHNOLOGIES IN EXCHANGE FOR TROOPS AND WEAPONRY AMID GROWING CONCERNS OVER NORTH KOREA'S NUCLEAR PROGRAM

Russia may soon share advanced satellite technologies with North Korea following the latter's deployment of troops to support Moscow's offensive in Ukraine, U.S. Secretary of State Antony Blinken stated on Monday, January 6.

"North Korea is already receiving military equipment and training from Russia. We now believe Moscow intends to share advanced space and satellite technologies with Pyongyang"

The Secretary of State is currently in South Korea for his final diplomatic tour before the inauguration of President-elect Donald Trump. His remarks come as North Korea recently tested a medium-range ballistic missile, which reportedly crashed into waters off the eastern coast of the Korean Peninsula, according to South Korean officials.

Blinken also warned that Russia might formally recognize North Korea's nuclear program, departing from its longstanding commitment to the denuclearization of the Korean Peninsula.

The United States has expressed concern over the growing alliance between Pyongyang and Moscow. Last June, President Vladimir Putin and North Korean leader Kim Jong Un signed a significant defense agreement. Putin's visit to North Korea was seen as an effort to secure Kim's support at a time when Russia is struggling to replenish its weapon stockpiles and is facing severe losses in Ukraine. Since then, ammunition and missiles are believed to have been transferred from North Korea to Russia, though both nations deny such exchanges. According to Ukrainian and Western sources, North Korean soldiers are also reportedly fighting alongside Russian forces.

There are additional concerns that Moscow is violating international sanctions by aiding North Korea in developing its military satellite program.

South Korean Defense Minister Kim Yong Hyun further revealed that North Korea has requested Russian technologies for tactical nuclear weapons, intercontinental ballistic missiles (ICBMs), reconnaissance satellites, and nuclear-powered submarines in exchange for providing military support on the battlefield.

CYBER LEGAL

Google accused: privacy violation and data collection without consent

A SAN FRANCISCO JUDGE APPROVES CLASS ACTION AGAINST GOOGLE FOR ALLEGED UNAUTHORIZED COLLECTION OF PERSONAL DATA, HIGHLIGHTING AMBIGUITIES IN ITS POLICIES. THE 2025 TRIAL COULD HAVE MAJOR IMPACTS ON THE TECH INDUSTRY.

A federal judge in San Francisco has ruled that Google must face a class action lawsuit over alleged unauthorized collection of personal data from users' smartphones, even when location tracking is disabled. Chief Judge Richard Seeborg dismissed the company's attempt to have the case thrown out, paving the way for a potential jury trial scheduled for August 18, 2025.

The plaintiffs allege that despite public statements from the company claiming that users could disable location tracking, Google continued to record browsing history and background activities. This behavior, they argue, violates users' reasonable expectations of privacy and is exacerbated by Google's deliberate obfuscation of these practices in its privacy policies. The lawsuit specifically cites the California Invasion of Privacy Act (CIPA) and other state laws prohibiting the collection of personal data without explicit consent.

Google, for its part, has argued that its data collection practices comply with the law and that users were adequately informed through its privacy policies. The company also claimed that the data collection was aimed at improving services such as personalized recommendations and real-time maps and emphasized that the plaintiffs had not demonstrated tangible harm resulting from these practices. However, Judge Seeborg rejected these arguments, stating that Google's privacy policies could be seen as ambiguous and misleading by an average user. According to the judge, a reasonable

user might find the collection of personal data without explicit consent, or in contradiction to the company's statements, to be "highly offensive".

Seeborg's decision opens the door to a trial that could have significant implications not only for Google but for the entire tech industry. In recent years, Google has faced numerous legal controversies related to privacy, including a class action over user tracking in Chrome's "Incognito" mode. The allegations against Google are part of a broader trend of increased scrutiny on the data collection practices of large tech companies, driven in part by the enactment of laws such as the California Consumer Privacy Act (CCPA). These regulations are pushing companies to reevaluate their policies to avoid financial penalties and reputational damage.

The trial scheduled for 2025 could represent a turning point, with the potential to set an important precedent for future privacy cases. If the plaintiffs succeed in proving that Google systematically violated users' privacy rights, the company may be forced to pay significant damages and make substantial changes to its tracking policies. Additionally, an unfavorable ruling could have repercussions far beyond California, influencing privacy regulation at both national and international levels.

CYBER LEGAL

The EU Court sets a precedent: Commission penalized for personal data breach

THE EU GENERAL COURT HAS RULED AGAINST THE EUROPEAN COMMISSION FOR VIOLATING GDPR, ORDERING COMPENSATION OF €400 FOR AN UNLAWFUL DATA TRANSFER TO META. THE JUDGMENT REAFFIRMS THAT EU INSTITUTIONS MUST FULLY COMPLY WITH DATA PROTECTION REGULATIONS.

For the first time in history, the General Court of the European Union has declared that the European Commission violated its own data protection laws, requiring it to compensate a German citizen with €400. This case marks a significant step in strengthening data protection and accountability, even for European institutions.

The issue arose from the European Commission's use of the "Login with Facebook" feature on one of its platforms. A German citizen utilized this option to register for an EU-organized conference. However, the use of this feature resulted in the user's IP address being transferred to Meta Platforms, Facebook's parent company, headquartered in the United States.

This transfer occurred without adequate safeguards for the protection of the user's personal data, a clear violation of the General Data Protection Regulation (GDPR). The user decided to bring the matter before the General Court of the European Union, arguing that the Commission had failed to adhere to the rules it is tasked with enforcing.

The GDPR, in effect since 2018, is considered one of the world's most stringent frameworks for personal data protection. It mandates compliance by all institutions, Member States, and businesses operating within the European Union. Some of the GDPR's core principles include: purpose limitation, requiring personal data to be collected only for specific, clearly defined objectives; data minimization, ensuring only strictly necessary information is collected; and regulation of cross-border transfers, prohibiting data movement outside the European Economic Area without adequate safeguards, such as standard contractual clauses.

In this case, the European Commission did not implement sufficient measures to ensure that the data transfer to Meta Platforms complied with these principles. The court's decision emphasizes that European institutions must fully respect the GDPR.

The ruling sets a dual precedent. On one hand, it confirms that the GDPR applies to EU institutions, including the European Commission and its agencies. On the other, it underscores the importance of safeguarding the personal data of European citizens when transferred to third countries.

The court considered the breach to be relatively minor, as indicated by the €400 compensation, but nonetheless stressed the need for greater diligence by European institutions. Moreover, this decision could encourage other citizens to take legal action in similar cases.

The General Court's ruling comes at a time of increasing focus on personal data protection and cross-border information transfers. The European Court of Justice had already determined in the 2020 Schrems II decision that the Privacy Shield—an agreement regulating data transfers between the EU and the US—failed to provide sufficient privacy guarantees for European users.

This case reinforces the notion that European institutions must serve as models of compliance with the laws they promote. To prevent future legal issues, it is likely that the Commission and other institutions will review their internal processes to ensure full adherence to the GDPR.

The fine imposed on the European Commission marks a pivotal moment in strengthening the legal framework for personal data protection within the European Union. The ruling not only ensures greater protection for citizens but also sends a clear message: no one, not even the highest EU institutions, is above the law.

CYBER GEOPOLITICS

Elon Musk, the AfD, and european concerns: political interference and digital regulation

ELON MUSK'S LIVE STREAM ON X WITH THE LEADER OF THE GERMAN FAR-RIGHT SPARKS DEBATE ON ELECTORAL INTERFERENCE, BIG TECH, AND THE URGENCY OF A EUROPEAN RESPONSE VIA THE DIGITAL SERVICES ACT

Elon Musk's decision to host Alice Weidel, leader of the far-right German party Alternative für Deutschland (AfD), in a live stream scheduled for January 10 has ignited a heated debate in Germany and across the European Union. This event, taking place in a politically sensitive context with Germany's parliamentary elections scheduled for February 23, raises concerns over potential electoral interference and the role of major digital platforms in European politics.

The AfD, classified as a far-right extremist party by Germany's security services, is known for its anti-immigration and anti-Islamic positions. Recently, it has seen a rise in polls, reaching 21.5% support and securing second place behind the conservatives. Musk, who has openly praised the party's economic policies, is accused of legitimizing the AfD and removing some of the stigma surrounding it. His actions, along with his critical remarks about Chancellor Olaf Scholz and President Frank-Walter Steinmeier, have further polarized the political debate.

The live stream with Weidel will be closely monitored by German authorities and the European Commission, who will assess potential violations of the Digital Services Act (DSA) and campaign finance regulations. The DSA, designed to

balance freedom of expression with the prevention of hate speech and political interference, could become central to Europe's response to Musk's activities.

Meanwhile, France and Spain have urged the EU to take a firmer stance against political interference. French Foreign Minister Jean-Noel Barrot has called on the Commission to strengthen the enforcement of the DSA, while Spanish Prime Minister Pedro Sanchez accused Musk of undermining European democracy. Musk's statements in favor of populist parties and his criticisms of European leaders, including UK Prime Minister Keir Starmer, have raised questions about the line between free speech and undue influence.

The European Commission, while reiterating that Musk is free to express himself, emphasized that any activity must comply with legal boundaries. A meeting of the DSA board, scheduled for January 24, will examine possible responses to these developments, aiming to strike a balance between transparency, platform regulation, and the protection of the democratic process in Europe.

The January 10 event thus represents a crucial test for German politics, the role of big tech, and the EU's ability to safeguard its electoral integrity in an era of growing external influences.

CYBER

CERT-AGID: support for clamAV format in the IoC feed

A NEW FEATURE TO ENHANCE CYBERSECURITY, MEETING THE NEEDS OF THE ACADEMIC AND INSTITUTIONAL COMMUNITY

Starting today, the CERT-AGID IoC Feed supports the ClamAV format, the renowned open-source antivirus widely used in academic, institutional, and corporate environments. This new feature has been implemented in response to a specific request from the system administrators of GARR universities, who highlighted the need to enhance the existing feed with an additional format that is customizable and easy to use, thereby improving the security level of managed systems.

Thanks to this integration, it is now possible to directly utilize the Indicators of Compromise (IoC) disseminated by CERT-AGID to detect suspicious files in systems protected by ClamAV. Moreover, signature management is transparent and highly flexible, as detailed in the official technical documentation.

Public administrations already accredited to the IoC Feed can immediately take advantage of the new ClamAV format by simply adding the parameter `type=clamav` to the provided URL:

<URL_received>&type=clamav

The service will return a text file formatted according to the `.hsb` standard used by ClamAV, omitting the file size and replacing it with the wildcard character `*`. To ensure backward compatibility, the minimum functional level required is ClamAV version 73.

```
9a510395868bb9ffe02004ef6010738facba10ab65da2d70f6719a430537c525:*:FormBook:73
d97e22f94b96aa4eddbe315fe64f8379:*:Lumma:73
8dd9c8238f9a2da51c476fa09c68e8cf1316422c:*:Rhadamanthys:73
33162044ddd087dc5636406f8efa9ed9d3bb636b9f66f78a452235aae4ecce42:*:Irata:73
153635d66bd01a944dcd4661cec41896:*:KoiStealer:73
4be7ce58752d3d6c689441487d24933166c3decc:*:AsyncRat:73
81abb1776a5da5c7844a18f50a4f254eed232c6164b62e2a5fd69d4494c4b943:*:njRAT:73
a462535dd4c7d80f9b474eb2a67117563a9fcc8d73fc0592b7753fdf4191f758:*:FormBook:73
79a2a731aea9ede92ef449b25e910647:*:AgentTesla:73
ba889042212f5499eaac3dc6ed5862df:*:FormBook:73
34a8890e4998418150c23488eae537640fa236f0:*:Remcos:73
b21c95ebf34440ad8da30f6e4fe25badb871d61a:*:Rhadamanthys:73
116887b2ac34a05784dca6f2cac7cc03:*:Rhadamanthys:73
02c53e42858c9c99b5aef5552972954f26885209f9bf30b825403433ff28e513:*:Rhadamanthys:73
215ff81b6f3a50e48d9f5acfb89f5ea3a1afd59dddbb0666f7ce97a922f60326:*:KoiStealer:73
654c0c7e931356faa0396f064994dc50:*:FormBook:73
a99182cf7c27dda2a192598210339eb96f0612a6:*:Rhadamanthys:73
dc767ae22ec2c3aa37aac0fb59b96ea54eeb08d5:*:AsyncRat:73
dbcdba774b5330c06fde116ef1d1184f307d65ca:*:Rhadamanthys:73
0826938525ff0f4f400488819d1e7dc7:*:SpyNote:73
23f0f232c72231ee39a7df5d87bc1721:*:Rhadamanthys:73
4d63883ce64474b643f30b2e3e3876710a92a861c52a1a452c4d86955d1b5f1e:*:FormBook:73
31f30a8b7270e00247b64c28cab661f23660c398d0da80b953e6587d58e4a429:*:FormBook:73
755fb54225dd285b06c369a2f5e58082:*:Remcos:73
2079cc699607e1946c94d546ecf70609:*:Rhadamanthys:73
df7ffd20940c227dac2b37a2646e819cad5a52dd:*:Rhadamanthys:73
c16e7b591755e996a4fafb382453c7c8cfafc966:*:Rhadamanthys:73
95865bf569deef3fa8a68a642cf078e1572a03d4:*:QnodeService:73
517ec3bee4730f2b57b1e5d576d0f92749c32d6678ac7695670c7c2b4d86ae06:*:Lumma:73
ff82fd4a86eb8c8b36ff276a0078d6e1dd981b1b:*:Irata:73
e3439125d29714a7c9f8f4e8a36c2d0ffc4d5acd926589a4caf255c2b808758a:*:Rhadamanthys:73
```

CYBER LEGAL

Scandal at ICAO: unauthorized disclosure of recruitment information

UN AGENCY ICAO INVESTIGATES PERSONAL DATA BREACH LINKED TO RECRUITMENT, FACING LEGAL AND REPUTATIONAL IMPLICATIONS. THE ORGANIZATION COLLABORATES WITH INTERNATIONAL AUTHORITIES AND TAKES MEASURES TO ENHANCE CYBERSECURITY AND PREVENT FUTURE INCIDENTS.

The International Civil Aviation Organization (ICAO), a United Nations agency based in Montreal, is currently investigating an alleged leak of sensitive data related to personnel recruitment. According to sources close to the matter, the investigation focuses on the potential unauthorized disclosure of candidates' personal information, which may include identifying details, professional experience, and other confidential data collected during the selection process.

The alleged breach of personal data raises significant legal concerns, particularly regarding international data protection regulations. In this context, ICAO, despite its status as a UN agency, must ensure compliance with applicable regulations, such as the European Union's General Data Protection Regulation (GDPR) when the data of European citizens are involved, along with other relevant national or regional laws.

The data breach could entail legal liability for ICAO, as the agency has both ethical and legal obligations to safeguard the personal data it collects and processes. Moreover, if the breach is found to have resulted from negligence or failure to implement adequate security measures, the organization's liability could be further compounded. Consequences may include administrative penalties, depending on the applicable jurisdiction, as well as remedies for affected individuals who may pursue legal action for damages, especially if the data leak caused material or moral harm. Reputational and diplomatic impacts could also be substantial, as ICAO operates under the oversight of multiple member states, which might demand greater transparency and actions to prevent future incidents.

ICAO has announced the launch of an internal investigation to determine the extent of the breach, its causes, and to identify those responsible. The organization emphasized that, if individual accountability is established, strict disciplinary measures may be taken in accordance with internal regulations and international conventions. Additionally, ICAO has confirmed it has already informed the relevant authorities in affected countries, facilitating transnational cooperation to address potential legal issues.

Although ICAO benefits from a certain degree of diplomatic immunity as a UN agency, this status does not exempt the organization from adhering to international data protection principles. A review of internal policies may also be necessary to align with the latest cybersecurity standards and ensure fair handling of personal data.

To prevent similar incidents in the future, ICAO has announced plans to implement a series of preventive measures, including strengthening cybersecurity infrastructure, revising protocols for processing and storing personal data, introducing mandatory training programs for staff on handling sensitive information in compliance with international laws, and collaborating with legal and technical experts to develop updated guidelines and continuously monitor the effectiveness of new policies.

The agency has also committed to ensuring transparent and regular communication with candidates, employees, and stakeholders, providing timely updates on the ongoing investigation and the actions taken.

This incident serves as a significant wake-up call for international organizations regarding the critical importance of data protection and compliance with global regulations, highlighting the vulnerabilities even within high-profile institutions.

GEOPOLITICS

Crisis in Venezuela: Maria Corina Machado Arrested and Released During Protests Against Maduro

WAVE OF NATIONWIDE PROTESTS, GOVERNMENT REPRESSION, AND ACCUSATIONS OF ELECTORAL FRAUD MARK OPPOSITION TO NICOLAS MADURO'S THIRD INAUGURATION

Maria Corina Machado, leader of the Venezuelan opposition, was arrested and later released on Thursday, January 9, after participating in a protest in Caracas marred by tensions and gunfire. Her arrest, which occurred during a wave of nationwide demonstrations against President Nicolas Maduro ahead of his third inauguration, has drawn condemnation from political allies and foreign governments. While detained, Machado was reportedly forced to record videos and announced she would provide further details.

The opposition accuses Maduro of electoral fraud and systematic repression, including the arrests of political leaders and activists, while the government defends the legitimacy of the elections and accuses dissenters of plotting

conspiracies. Edmundo Gonzalez, the opposition's presidential candidate, is widely recognized as the "true winner" of the elections and has garnered international support but risks arrest if he returns to Venezuela.

Protests have erupted across the country, involving thousands of participants and facing harsh crackdowns. Security forces have dispersed demonstrators with tear gas and mass arrests in several cities. Meanwhile, the government has organized counter-demonstrations. Venezuelans abroad have also mobilized in solidarity.

The tense atmosphere reflects a deep political, social, and economic crisis gripping Venezuela under Maduro's regime, which is backed by the military and intelligence services.

CYBER GEOPOLITICS

The American Challenge on TikTok: Balancing National Security and Digital Freedom

FRANK MCCOURT'S PROPOSAL AND THE DEBATE OVER PRIVACY AND FREEDOM OF EXPRESSION IN THE UNITED STATES

TikTok is at the center of a complex legal and political battle in the United States, with implications for national security, freedom of expression, and control over the tech market. A consortium led by entrepreneur Frank McCourt, former owner of the Los Angeles Dodgers, has put forward a proposal to acquire the U.S. operations of the Chinese-owned platform ByteDance. The deadline for the sale is set for January 19, under a law signed by President Joe Biden last April. Without a deal, TikTok faces a potential ban in the U.S.

The consortium has stated that it has the support of major U.S. investors and banks to complete the acquisition, aiming to keep the platform operational without its current algorithm and to avert a ban. McCourt emphasized his willingness to collaborate with ByteDance, President-elect Donald Trump, and the incoming administration to secure a mutually beneficial agreement.

Meanwhile, TikTok's fate is under scrutiny by the Supreme Court, which must decide whether the law mandating the sale of the platform violates the First Amendment's protections on free speech. The Department of Justice argues that TikTok poses a national security threat, citing the risk of China accessing sensitive U.S. user data or manipulating content on the platform. TikTok and ByteDance deny these allegations, calling the law an attack on free speech.

The case has divided the U.S. administration and Congress. While many Republicans support the need to limit Chinese influence, President-elect Trump has called for a suspension of the ban, describing TikTok as an important communication tool. This represents a reversal from his first term when he sought to ban the platform.

The debate over TikTok takes place against the backdrop of escalating U.S.-China tensions and raises fundamental questions about the future of digital freedom and the regulation of social media platforms. The Supreme Court's decision could have far-reaching implications, not only for TikTok but also for other apps with international ties, defining the boundary between freedom of expression and national security.