MERIDIAN GROUP

Weekly *Report*

27/01/2025

TLP: WHITE

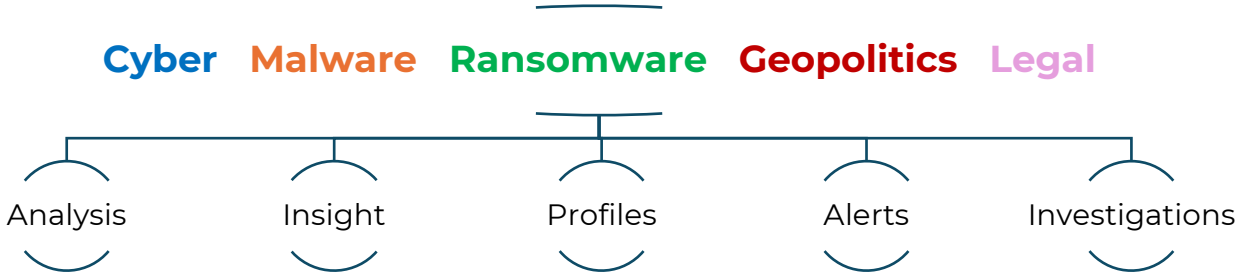
MERIDIAN S.R.L

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.



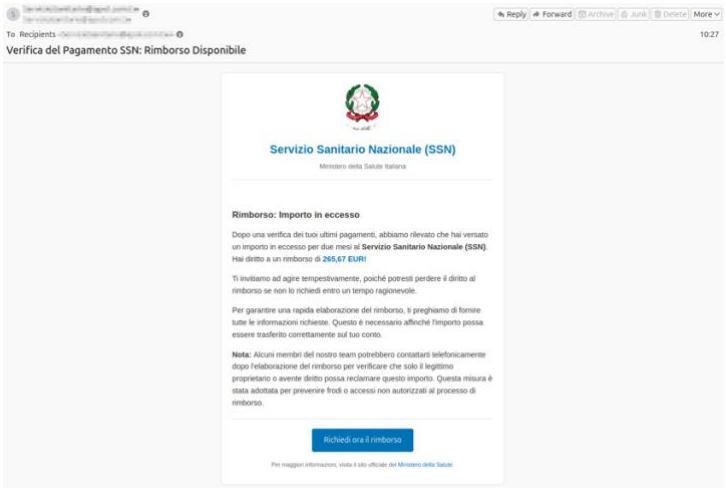
The CI Team, through this weekly report, aims to provide timely and accurate analysis regarding the aforementioned areas, enabling readers to stay informed about the latest news concerning new vulnerabilities, potential threats, and changes in the geopolitical landscape.

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.

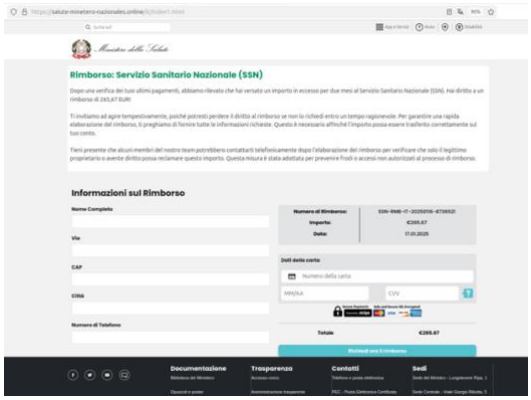
CYBER

The name of the Ministry of Health exploited for cyber fraud

A phishing campaign currently underway has been identified, leveraging the logo and name of the Ministry of Health to deceive victims into unlawfully providing personal and financial data.



Through phishing emails, users are prompted to click on a link that redirects them to a counterfeit webpage. On this page, they are asked to provide personal data to allegedly claim a refund of €265.67 from the National Health Service. The information requested includes full name, residential address, phone number, and credit card details.



Once the required fields are completed, the victim is further redirected to a second page where they are fraudulently asked to re-enter their credit card details. This strategy, orchestrated by cybercriminals, aims to both reduce the likelihood of data entry errors and, when possible, obtain the details of a second credit card.

GEOPOLITICS

Elon Musk, controversy over gestures during Trump's inauguration: "Nazi salute or symbol of enthusiasm?"

During the celebrations for President Donald Trump's inauguration on Monday, January 20, Elon Musk made a hand gesture that sparked a heated online debate. Some users compared it to a Nazi salute, but the Anti-Defamation League, which monitors antisemitism, dismissed the accusation, describing it as an enthusiastic and awkward gesture unrelated to extremist symbolism. Musk brushed off the criticism, calling it a "tired attack" and baseless.

On the stage of the Capital One Arena in Washington, greeted by thunderous applause, Musk began his speech by thanking the audience for their support and emphasizing the significance of the moment: "This was no ordinary victory. It was a crossroads in the path of human civilization." During the speech, he placed his hand on his heart with fingers spread, then extended his right arm upward with his palm facing down, a gesture he repeated toward the crowd behind him, accompanied by the statement: "My heart is with you. It's thanks to you that the future of civilization is assured."

These gestures immediately drew attention, with the Jerusalem Post ironically asking whether Musk had made the "Sieg Heil" during the event. Charlotte Knobloch, president of the Jewish community of Munich and Upper Bavaria, called the gesture "highly irritating," but stressed that her main concerns were Musk's political positions. He has voiced support for the far-right German party Alternative für Deutschland (AfD), an anti-immigration and anti-Islam party classified as far-right extremist by German security services. Musk even hosted a broadcast with the party's leader on his social media platform X.

In response to criticism, Musk quipped: "Frankly, they need better dirty tricks. The 'everyone is Hitler' attack is so tired." After his appearance, Musk shared a video of his speech on X, describing the future as "exciting." Some users on the platform defended Musk, arguing that the gesture sincerely meant "my heart is with you" and criticized those who interpreted it differently.

GEOPOLITICS

Trump between isolationism and controversies: withdrawal from who and Paris agreement and tensions with China

On his first day back at the White House, Donald Trump took a series of executive actions that had an immediate impact both domestically and internationally. Domestically, he signed measures to limit immigration, revoke environmental regulations, and reduce initiatives on racial and gender diversity, as well as granting clemency to approximately 1,500 of his supporters involved in the 2021 Capitol attack.

Internationally, Trump announced the United States' withdrawal from the World Health Organization (WHO), accusing the agency of mismanaging the COVID-19 pandemic and being influenced by China. Beijing criticized this decision, emphasizing the importance of strengthening global health governance.

Furthermore, Trump signed an executive order withdrawing the United States again from the Paris Climate Agreement, placing the U.S. among the few countries not adhering to the global pact to limit global warming. This move raised international concern, with European Commission President Ursula von der Leyen reaffirming Europe's commitment to fighting climate change: "*The Paris Agreement represents the best hope for humanity*."

China also expressed concern over Trump's withdrawal from the climate accords. Chinese Foreign Ministry spokesperson Guo Jiakun emphasized that China is strongly committed to responding to the climate crisis and will continue to promote the global energy transition. Guo also stated that the role of the World Health Organization (WHO) "should only be strengthened, not weakened," expressing China's support for the global health agency despite the executive order that mandates the U.S. withdrawal from WHO.

On the trade front, Trump declared his intention to intensify tariff policies, threatening 25% tariffs on Canada and Mexico, while hinting that new measures against China could be introduced. Tensions with Beijing remain high, fueled by trade disputes and control over companies such as TikTok.

Trump's return to the presidency underscores a foreign policy characterized by isolationism and skepticism toward international cooperation, with a significant impact on global dynamics and relations with major economic and political partners.

CYBER LEGAL

Star Blizzard exploits WhatsApp to collect sensitive data: the international legal response

The Russian hacker group Star Blizzard has recently targeted the WhatsApp accounts of high-ranking government officials and diplomats in various countries, using a sophisticated phishing technique. The victims received emails seemingly sent by U.S. officials, inviting them to join WhatsApp groups supporting humanitarian initiatives in Ukraine. The email contained a QR code that, when scanned, allowed the hackers to connect to the victims' WhatsApp accounts and access their messages, gathering sensitive information.

This attack is an example of how state-sponsored hacker groups can evolve, moving from traditional spear-phishing techniques to more sophisticated methods aimed at secure communication platforms like WhatsApp, often used for confidential exchanges by diplomats and government officials. While WhatsApp uses end-to-end encryption, the attack highlighted the vulnerability of accounts when users interact with malicious links or codes.

This attack raises significant legal issues, particularly regarding data protection and the security of communications. For victims residing in the European Union, the incident could constitute a violation of the GDPR, which imposes strict obligations on the protection of personal data. Furthermore, the intrusion into the official communications of government officials can be interpreted as a violation of the digital sovereignty of states. When attacks are state-sponsored, the legal situation becomes even more complex, as international law does not always provide clear answers for attributing responsibility. Possible legal responses include international sanctions, but attributing responsibility to a specific state remains a difficult issue both legally and politically.

GEOPOLITICS

Huawei challenges Nvidia: expansion in China's AI chip market

Huawei is aiming to expand its presence in China's AI chip market, currently dominated by Nvidia, by encouraging local companies to adopt its Ascend processors for inference tasks. Major Chinese AI firms have traditionally relied on Nvidia GPUs for training large language models, viewing them as essential for technological advancement.

However, instead of competing with Nvidia in training, Huawei is positioning its Ascend processors as the optimal solution for inference—the computations used by language models to generate responses. The company believes inference will become a key driver of future demand, particularly as the pace of training slows and AI applications, such as chatbots, become more widespread. Huawei is pursuing a less technically complex but potentially lucrative strategy by ensuring compatibility between Nvidia GPU-trained models and its Ascend chips. Since the two processors operate on different software platforms, Huawei has developed tools to bridge the gap, simplifying the transition for businesses.

The initiative has also garnered support from the Chinese government, which has urged local tech giants to purchase Huawei chips to reduce reliance on Nvidia. According to sources close to Nvidia in China, Huawei is seen as the most formidable domestic competitor, thanks to its advanced design capabilities. U.S. export restrictions limit Chinese companies' access to high-performance GPUs. While Nvidia offers its less advanced H20 chips in China to comply with regulations, these chips remain in high demand, outperforming local alternatives.

Despite its progress, Huawei's Ascend chips are not yet ready to compete in training large models. Technical challenges, such as connectivity issues within larger chip clusters, pose significant hurdles. "The Ascend chips perform well individually, but there are connectivity limitations when scaled," explained Lin Qingyuan, a semiconductor analyst at Bernstein. Another obstacle is persuading developers to migrate from Nvidia's Cuda software, widely regarded as the standard for efficiency and ease of use. Nevertheless, Huawei plans to overcome this challenge with the upcoming launch of its Ascend 910C chip, which is expected to deliver substantial hardware and software upgrades.

In addition to Huawei and Nvidia, other Chinese companies, such as Baidu and Cambricon, are investing in AI chip development. Meanwhile, U.S. tech giants like Amazon and Microsoft are working to gain a foothold in the inference chip market. According to SemiAnalysis, Nvidia generated $12 billion in revenue from China in 2023, selling one million H20 chips—double the sales of Huawei's Ascend 910B chips. However, Huawei is narrowing the gap by rapidly scaling production capacity. "Nvidia's lead is shrinking, but Huawei still faces supply constraints," noted Dylan Patel, chief analyst at SemiAnalysis.

U.S. restrictions have driven Chinese firms to focus on inference, a domain where significant efficiency gains can be achieved even with less powerful chips. For instance, Chinese startup DeepSeek recently introduced its V3 model, which boasts lower training and inference costs. The company has also partnered with Huawei to adapt its model to Ascend chips, offering technical support to developers.

Despite the challenges, Huawei continues to invest in expanding its presence in the inference chip market, aiming to meet growing demand for more affordable and efficient solutions. This strategy could redefine the technological landscape in China, further strengthening its independence from Western tech giants.

RANSOMWARE

Ransomware attacks: Russian cybercriminals exploit Microsoft Teams with new fraud techniques

Russian cybercriminals have adopted a new fraudulent scheme, posing as technical support agents on Microsoft Teams. Using this technique, they deceive victims into believing they have a technical issue, ultimately convincing them to allow the installation of ransomware on their companies' networks.

The British cybersecurity firm Sophos has identified over 15 incidents in which two distinct groups exploited the default settings of Microsoft Office 365 services to infiltrate victims' systems through social engineering techniques. One of these groups has ties to the entity known as Storm-1811, previously identified by Microsoft for similar operations. The other group, appearing to mimic Storm-1811's tactics, is suspected of being linked to the criminal organization FIN7.

These new campaigns were uncovered during investigations into cases involving the "BeaverTail" malware, associated with attacks by North Korean actors. The latter often pose as recruiters on job search platforms, tricking victims into downloading malware designed to steal cryptocurrencies from their devices. However, the Russian attacks are markedly different from North Korean methods, both in the type of malware used and the nature of the victims targeted.

A notable incident occurred on U.S. election day. Two employees at a company received an overwhelming number of emails in a short span. One of them, working remotely, was later contacted via a Teams call by a supposed technical support representative, initiating the attack.

The two criminal groups leveraged their own Microsoft Office 365 tenants to carry out these attacks, exploiting a default configuration in Microsoft Teams that allows users from external domains to start chats or meetings with internal users. In some cases, the attackers made voice or video calls through Teams; in others, they sent text messages containing links to tools designed to gain remote control of the victim's device. For this phase, the attackers utilized Microsoft tools such as QuickAssist or Teams' screen-sharing feature.

In one significant attack, a fake support operator convinced an employee to authorize a remote control session. The attacker then opened a command terminal, uploaded files, and executed malware, including a Java Archive (JAR) and a .zip file containing Python code.

While these methods are sophisticated, they rely on freely available code. Tools used by groups like FIN7 have been sold to other cybercriminals, further facilitating such attacks.

GEOPOLITICS

Terrorism: 30-year-old ISIS affiliate arrested in Naples for violent plans against the jewish community

On Wednesday, January 20, a 30-year-old Moroccan national was arrested in Naples on charges of association with the aim of international terrorism and subversion of the democratic order. The operation was the result of extensive investigations coordinated by the anti-terrorism unit of the Naples prosecutor's office, which led to the identification of the man and the reconstruction of his ties to the ISIS terrorist organization. During the investigation, which also included online monitoring, searches and seizures were carried out against other individuals linked to the suspect.

According to the findings, the man had embraced ISIS ideology and was actively engaged in the dissemination and promotion of propaganda and multimedia material associated with the terrorist organization, including training content. Investigators also determined that the 30-year-old had expressed violent intentions, particularly targeting the Jewish community in Naples, and had voiced his intention to acquire a knife to carry out his terrorist plans.

The precautionary measure was issued by the investigating judge of Naples at the request of the prosecutor’s office, led by Chief Prosecutor Nicola Gratteri. The arrest represents a significant step in the fight against international terrorism and violent radicalization.

CYBER GEOPOLITICS

Iran and Russia strengthen cooperation in cyberspace with a new strategic agreement

Iran and Russia have signed an agreement aimed at strengthening the ties between the two countries in the military, security, and technology sectors. The agreement, made between two of the most sanctioned nations in the world, seeks to elevate bilateral relations to a higher level, as highlighted by the Kremlin. Specifically, certain clauses focus on cybersecurity cooperation and internet regulation.

Over the years, Russia has signed similar treaties with other countries, such as China and North Korea, to share experiences in the fields of information technology and digital development. The agreement, signed in Moscow by Presidents Vladimir Putin and Masoud Pezeshkian, includes expanding cooperation in combating the illegal use of information and communication technologies. Moreover, the two countries have agreed to exchange expertise in managing their respective national networks and have committed to promoting stricter global cyberspace regulations, with the aim of creating standards for international tech companies.

Both Russia and Iran are considered to have "unfree" internet environments, due to heavy censorship, disinformation campaigns, surveillance, and penalties for online opinions, according to Freedom House. Russia, in particular, has long attempted to limit access to the global internet to gain greater control, with recent efforts including blocking apps and websites and testing the so-called "sovereign internet." Iran has adopted similar policies, making access to international internet more difficult and expensive, steering users toward a national version of the network, where authorities can more effectively monitor and control content.

While the agreement between Russia and Iran does not impose binding obligations, it formalizes the already existing ties between the two countries, with provisions on security similar to those in a previous 2021 treaty. The latter, which came into effect in 2022, focused on cybersecurity cooperation, the prevention of cybercrime, and a mutual commitment not to attack each other in cyberspace.

In 2023, Russia's digital ministry, along with major local tech companies like Rostelecom-Solar and Positive Technologies, met with Iran's communications and technology ministry to discuss the export of Russian technology and cybersecurity collaborations. In October, Positive Technologies published a report on Iranian cyber threats, confirming growing cooperation with Tehran. According to the company, the research is based on authoritative sources. Last year, the spokesperson for Iran's National Security Commission confirmed that Russia was actively contributing to Iran's cybersecurity, providing tangible evidence of the increasing collaboration between the two nations in this field.

GEOPOLITICS CYBER 

Trump signs executive order on cryptocurrencies: new regulations, national digital reserve, and CBDC ban

On January 23, U.S. President Donald Trump signed an executive order to establish a dedicated cryptocurrency working group. This team will be tasked with drafting new regulations for digital assets and assessing the feasibility of creating a national cryptocurrency reserve. The initiative represents a concrete first step toward reforming U.S. cryptocurrency policy, as promised by Trump during his electoral campaign.

The executive order also includes measures to ensure banking access for companies in the cryptocurrency sector, addressing industry allegations that U.S. regulators had pressured banks to sever ties with these firms—claims denied by the authorities. Additionally, the order bans the creation of central bank digital currencies (CBDCs) in the United States to prevent potential competition with existing cryptocurrencies.

Another significant step in favor of the cryptocurrency industry came from the U.S. Securities and Exchange Commission (SEC), which rescinded certain accounting guidelines deemed overly burdensome for publicly traded companies tasked with safeguarding cryptocurrencies on behalf of third parties. According to industry representatives, these guidelines had hindered the adoption of digital assets.

During his campaign, Trump had positioned himself as a "crypto president," adopting a starkly different approach from the Biden administration. The latter had taken legal action against several platforms, including Coinbase and Binance, for alleged violations of U.S. laws—allegations consistently denied by the companies involved.

Trump's executive order has been met with enthusiasm from the industry, which has long called for a clear signal of support. "This order marks a watershed moment in U.S. digital asset policy," said Nathan McCauley, CEO and co-founder of Anchorage Digital. "The administration’s global and coordinated approach represents a significant step toward establishing clear and consistent rules for the sector."

Regulatory experts believe that, if fully implemented, the measure could push cryptocurrencies toward broader mainstream adoption. The initiative follows the SEC’s recent announcement of a dedicated task force to revise cryptocurrency regulations.

Investor enthusiasm for the crypto-friendly administration has also been reflected in the markets: Bitcoin hit a record high of $109,071 on Monday, closing at approximately $103,000 on Thursday. "Just days into his term, President Trump

is delivering on his promises to ensure the United States remains a leader in digital innovation," stated Senator Tim Scott, the Republican chair of the Senate Banking Committee.

For years, the industry has advocated for a revision of existing regulations, arguing that they are inadequate for digital assets. According to the executive order, the working group—which will include the Treasury Secretary, the heads of the SEC and the Commodity Futures Trading Commission, as well as other senior officials—will be responsible for creating a clear regulatory framework for cryptocurrencies, including stablecoins, which are generally pegged to the U.S. dollar.

The group will also evaluate the creation of a national digital asset reserve, potentially consisting of cryptocurrencies lawfully seized by the federal government. However, further details on how this reserve will be established were not provided. Analysts are divided on whether congressional approval will be required, though some speculate that the reserve could be created through the Treasury's Exchange Stabilization Fund, which is already used to purchase and sell foreign currencies and could potentially hold Bitcoin.