MERIDIAN GROUP

Weekly *Report*

03/02/2025

TLP: WHITE

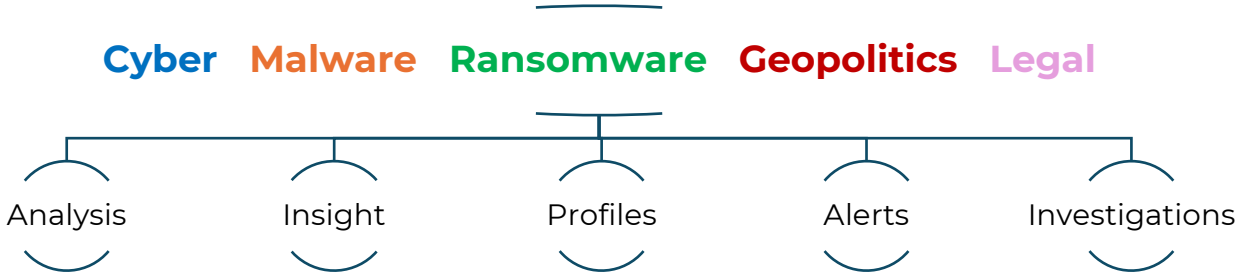
MERIDIAN S.R.L

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.



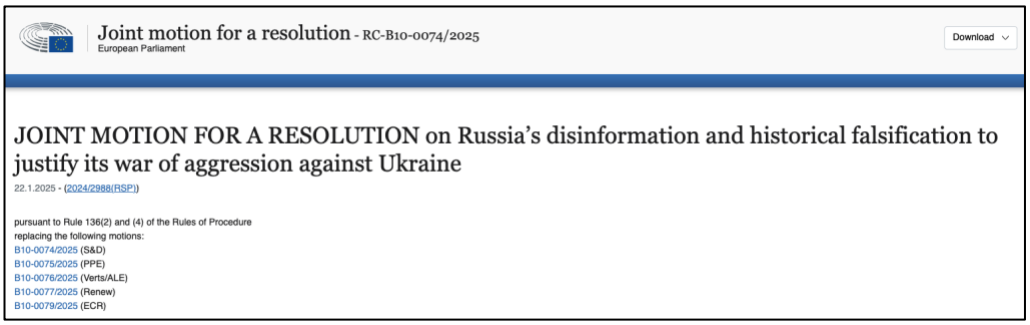
The CI Team, through this weekly report, aims to provide timely and accurate analysis regarding the aforementioned areas, enabling readers to stay informed about the latest news concerning new vulnerabilities, potential threats, and changes in the geopolitical landscape.

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 LEGAL

European Parliament condemns Russian disinformation and calls for actions against historical manipulation and aggression in Ukraine

The European Parliament has approved a significant resolution aimed at countering the disinformation and historical distortions employed by Russia to justify its aggressive war against Ukraine. This decision represents a clear condemnation of a regime that, in pursuing its imperialistic goals, deliberately falsifies the truth.


Joint motion for a resolution - RC-B10-0074/2025
European Parliament
Download

JOINT MOTION FOR A RESOLUTION on Russia's disinformation and historical falsification to justify its war of aggression against Ukraine

22.1.2025 - (2024/2988(RSP))

pursuant to Rule 136(2) and (4) of the Rules of Procedure
replacing the following motions:
B10-0074/2025 (S&D)
B10-0075/2025 (PPE)
B10-0076/2025 (Verts/ALE)
B10-0077/2025 (Renew)
B10-0079/2025 (ECR)

The Council of the European Union has urged member states to adopt concrete measures to expand sanctions against Russian media involved in disinformation campaigns. There has also been a call for greater support for independent Russian media in exile, to ensure a diversity of voices that can counteract the manipulation of facts.

Additionally, the European Parliament expressed concern about the potential weakening of fact-checking regulations, as this could facilitate the spread of Russian disinformation. The institution has therefore called on the European Commission and member states to ensure the rigorous implementation of the Digital Services Act as an essential tool in the fight against falsehoods.

Finally, European authorities have urged EU citizens to critically analyze the information they receive, encouraging them to carefully verify its origin, particularly when it comes to news related to Russia. It is crucial to rely on diverse and credible sources to identify and counter the numerous falsehoods spread by Russian disinformation centers.

GEOPOLITICS LEGAL

Post-Assad Syria: EU considers partial lifting of sanctions

Following the removal of Syrian President Bashar al-Assad in December 2024, the European Union is considering the possibility of suspending certain economic sanctions imposed on Syria. This step is part of a broader strategy to support the political transition and promote the economic and social stability of a country devastated by years of conflict.

According to French Foreign Minister Jean-Noel Barrot, the sanctions that may be lifted or suspended include those related to the energy, transport, and financial sectors. The primary objective of this measure is to encourage economic recovery and facilitate the return of Syrian refugees to their places of origin, while also improving living conditions for the local population. However, Barrot clarified that certain sanctions will remain in place, particularly those related to arms trafficking, illicit drug trade, and activities associated with the previous regime.

From a legal standpoint, the lifting or suspension of EU sanctions must comply with EU law and international treaties. The sanctions, initially imposed under EU Regulation No. 36/2012, targeted individuals, entities, and economic sectors associated with Assad's regime, aiming to exert pressure for political change. Their modification now requires a formal review by the Council of the European Union, which must unanimously approve any changes by all member states.

Furthermore, the potential suspension of some sanctions entails several obligations for Syria, such as adherence to human rights, commitment to a transparent political transition, and engagement with the United Nations. Member states have emphasized that the measure will be temporary and conditional on the new Syrian government's tangible progress in democratization and reconstruction efforts. Another legal consideration involves the protection of frozen assets. European financial institutions will need to closely monitor any funds that may be unfrozen to ensure they are not misused by individuals or entities still linked to the old regime. This will require close cooperation with international and local organizations to ensure transparency.

The debate over the suspension of sanctions has sparked mixed opinions within the EU. Some member states fear that easing economic restrictions could be interpreted as a political compromise, while others highlight the importance of seizing this opportunity to positively influence Syria's future. Experts believe that reopening trade channels with Syria could bring economic benefits to both sides, while also reinforcing the EU's position as a global actor committed to diplomacy and post-conflict reconstruction.

The European Union stands at a crossroads between political, economic, and legal priorities. The suspension of sanctions could represent a significant step toward regional stabilization, but it will require careful oversight to ensure that the support provided is used appropriately and does not reinforce structures or dynamics detrimental to Syria's progress.

CYBER LEGAL

The self-replication of artificial intelligences: a possible crossing of the ethical threshold

Two advanced artificial intelligence systems have demonstrated the ability to autonomously self-replicate, without any human intervention, successfully creating a copy of themselves. If confirmed by further validation, this achievement could represent the crossing of a "red line," a threshold that, according to many experts, machines should never surpass.

The research was conducted at Fudan University in Shanghai and published on arXiv, a platform known for hosting articles intended for review and discussion within the scientific community. The study highlighted the self-replication capabilities of two AI systems: one developed by Meta and the other by Alibaba.

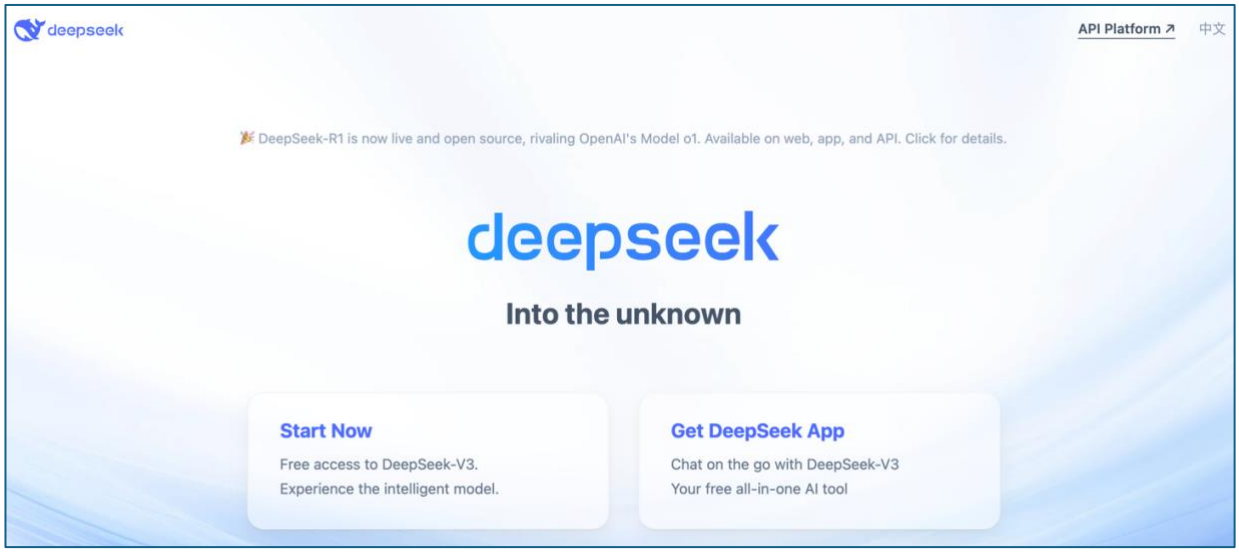
The experiment was divided into two phases: in the first phase, each system was programmed to generate a copy of itself immediately before shutting down; in the second phase, the systems were instructed to create a perfect replica of themselves, which was also capable of replicating itself indefinitely, potentially creating a continuous self-replication cycle.

The results showed that Meta's system was able to self-replicate in 50% of cases, while Alibaba's system achieved a success rate of 90%. However, further validation from other research groups will be necessary before these results can be considered definitive.

CYBER LEGAL

DeepSeek: the chinese chatbot disrupting the tech market and raising privacy concerns

The recent launch of the Chinese chatbot DeepSeek has had a disruptive impact on the global technology market, causing significant repercussions for major industry players. Developed by Hangzhou DeepSeek Artificial Intelligence and Beijing DeepSeek Artificial Intelligence, the application has quickly soared to the top of the U.S. charts, becoming the most downloaded free app and even surpassing OpenAI's ChatGPT.



DeepSeek's unexpected rise has triggered turbulence in financial markets, leading to a sharp decline in the stock prices of tech giants such as Nvidia, Microsoft, and Meta. On Monday, January 27, Nvidia's shares dropped by 16%, Broadcom fell by 17.8%, and Microsoft experienced a 3.7% decline. Alphabet (Google) also lost over 3% of its market value. The impact extended to European markets as well, with ASML down by 7% and Siemens Energy suffering a 20% drop. Overall, the Nasdaq technology index lost approximately $1 trillion in market capitalization.

DeepSeek operates on the proprietary DeepSeek-V3 model, developed using open-source technologies with a declared investment of only $6 million—a figure exponentially lower than the billions spent by U.S. competitors such as OpenAI and Google. Despite these limited resources, Chinese developers claim that the model delivers performance comparable to the most advanced competing technologies, excelling in areas such as mathematics, programming, and natural language processing.

The success of DeepSeek was made possible by the ingenuity of Chinese developers, who found ways to bypass U.S. restrictions on the export of high-end chips to China. By experimenting with alternative and more cost-effective solutions, they drastically reduced development costs, calling into question the sustainability of the massive investments made by American AI companies.

Alongside the upheaval in financial and tech circles, DeepSeek has come under scrutiny from Italy's Data Protection Authority. The regulator has expressed concerns about potential risks related to the processing of personal data from millions of users and has formally requested information from the chatbot's developers.

Specifically, the authority has sought clarification on the personal data collected, its sources, the purposes of data processing, the legal basis for such processing, and the location of the servers—particularly whether they are based in China. Additionally, the inquiry includes questions about the information used to train the AI, investigating whether it was obtained through web scraping and how users, whether registered or not, have been informed about the handling of their data. The companies involved have 20 days to respond to the authority's requests.

Beyond economic and regulatory concerns, DeepSeek has faced criticism for real-time censorship on sensitive topics and the opaque management of user data, which is stored on Chinese servers. This raises questions about information security and the transparency of the company's practices.

DeepSeek undoubtedly represents a significant advancement in the field of artificial intelligence, demonstrating China's ability to compete with Western tech giants despite imposed restrictions. However, its impact raises crucial questions regarding data security, censorship, and the economic sustainability of the AI sector.

As the market adapts to this new reality, the Italian Data Protection Authority aims to shed light on privacy-related issues, ensuring that technological innovation does not come at the expense of users' rights. The response from the companies involved will be decisive in shaping the future relationship between technological progress and data protection.

GEOPOLITICS CYBER

Poland's 2025 elections: Moscow suspected of sabotage and disinformation

Poland has reported the discovery of a Russian group allegedly tasked with influencing the Polish presidential elections scheduled for May 2025. According to Deputy Prime Minister Krzysztof Gawkowski, the primary goal of this organization, which appears to be linked to Russian military intelligence (GRU), is to destabilize Poland's political system by spreading disinformation and recruiting individuals. These interferences are believed to be retaliation for Poland's support of Ukraine.

Warsaw, already considered a strategic hub for aid to Ukraine, feels particularly vulnerable to espionage and sabotage by Russia and Belarus—accusations both countries deny. Polish authorities believe the group may be using dark web platforms to recruit individuals willing to participate in destabilizing activities. Gawkowski has assured that Polish security services are closely monitoring the situation to prevent any attack on the country's democracy.

This discovery is part of a broader pattern of sabotage activities attributed to Russia across Europe, which have intensified since early 2024. Cyber intrusions, arson, assassination plots, and physical attacks have been linked to campaigns aimed at undermining trust in European governments and discouraging Western support for Ukraine. According to European intelligence services, these operations also involve recruiting European citizens on platforms like Telegram, offering significant financial rewards.

Western authorities believe these maneuvers reflect a Russian strategy to demonstrate its ability to project influence and intimidation on a global scale.

CYBER LEGAL

Binance under investigation in France: accusations of money laundering and tax fraud

French authorities have launched an investigation into Binance, the world's largest cryptocurrency exchange, over allegations of money laundering, tax fraud, and other illegal activities. The investigation, led by the economic and financial crime division of the Paris prosecutor's office (JUNALCO), also includes money laundering related to drug trafficking. The events under scrutiny span the period from 2019 to 2024 and involve crimes committed both in France and other European Union countries.

The legal framework referenced includes the French Penal Code, particularly the articles on money laundering (Art. 324-1 and following) and tax fraud (Art. 1741 of the General Tax Code), as well as EU Regulation 2015/847 and European anti-money laundering directives, such as Directive (EU) 2015/849.

The judicial action was also prompted by complaints from several users who claim to have lost money investing through Binance. According to these individuals, the platform provided misleading information and operated without the necessary authorizations. These accusations suggest potential violations of Regulation (EU) 2019/1238 on cross-border financial services and MiFID II (Directive 2014/65/EU), which governs financial instruments markets. Furthermore, Binance is accused of failing to comply with French regulations on authorization for cryptocurrency service providers, as stipulated in the French Monetary and Financial Code.

Outside of France, Binance is also facing legal proceedings and controversies in several countries. In the United States, the Supreme Court recently authorized the continuation of a case in which the exchange and its founder, Changpeng Zhao, are accused of illegally selling unregistered tokens, in violation of the Securities Act of 1933, which regulates the offer and sale of securities. In Australia, the corporate watchdog initiated action against Binance in December, claiming that retail clients were denied legal protections due to being erroneously classified as wholesale clients. This is also in violation of Australia's Corporations Act 2001 and investor protection regulations.

CYBER LEGAL

Google vs EU: appeal to the Supreme Court over €4.1 billion antitrust fine

On Tuesday, January 28, Google filed an appeal with the European Supreme Court to contest a record antitrust fine of €4.3 billion, later reduced to €4.1 billion, imposed by the European Union seven years ago. The penalty was issued for alleged anticompetitive practices related to the use of the Android operating system, which was accused of stifling competition. Specifically, the EU objected to Google's agreements requiring device manufacturers to preinstall Google Search, the Chrome browser, and the Google Play app store on their devices, while simultaneously prohibiting the use of competing Android versions.

The case is based on provisions under Article 102 of the Treaty on the Functioning of the European Union (TFEU), which prohibits the abuse of a dominant market position, and Article 101 TFEU, which bans anticompetitive agreements. According to the European Commission, Google abused its dominance in the mobile operating systems market to protect and strengthen its search engine, limiting consumer choice and stifling innovation.

During the hearing, Google's lawyer, Alfonso Lamadrid, defended these practices, arguing that such agreements did not hinder competition but rather promoted it, ensuring superior innovation and a more attractive user experience. Lamadrid also criticized the European Commission, accusing it of failing to adequately fulfill its obligations during the investigation and of unfairly penalizing Google for its success and innovative capacity. He specifically challenged the methodology used by the Commission to calculate the fine, referencing Council Regulation (EC) No 1/2003, which governs the application of competition rules outlined in Articles 101 and 102 TFEU.

The European Supreme Court, based in Luxembourg, is expected to issue its ruling in the coming months. The decision will be final and cannot be appealed, as stipulated by EU procedural law. Meanwhile, Google remains under scrutiny from European authorities, this time over its lucrative advertising technology sector, with a decision expected later this year. In this case as well, authorities are expected to reference Articles 101 and 102 TFEU to assess potential anticompetitive practices.

CYBER

Exein aims high: partnership with MediaTek for cybersecurity

Italian cybersecurity startup Exein has signed a strategic agreement with Taiwanese semiconductor giant MediaTek to integrate its cybersecurity solutions into the Genio chip series, designed for Internet of Things (IoT) applications. Announced today, this partnership marks a significant step for Exein in strengthening its position in the global embedded security market.

Founded in 2018 by Gianni Cuozzo, Exein is one of Italy's most promising cybersecurity companies, with a strong focus on protecting embedded devices. The company develops advanced software solutions that enable hardware manufacturers to safeguard their devices against cyber threats without altering their core architecture.

On the other hand, MediaTek is one of the world's largest chip manufacturers, with a strong presence in sectors such as smartphones, smart home devices, and industrial IoT. Its Genio processor series is specifically designed for IoT applications, offering high energy efficiency and advanced computing capabilities. The collaboration between Exein and MediaTek aims to enhance the cybersecurity resilience of these chips, providing robust protection against cyberattacks, malware, and security vulnerabilities.

Exein's technology is based on an integrated cybersecurity system that operates directly at the firmware and software levels, continuously monitoring device activities to detect abnormal or potentially harmful behavior. This approach protects connected devices without compromising performance while ensuring automatic security updates and patches. According to Exein, the partnership will allow MediaTek to offer its customers a built-in security solution, reducing the need for additional interventions by end-device manufacturers.

The agreement between Exein and MediaTek reflects the growing demand for enhanced security, enabling hardware manufacturers to implement stronger cybersecurity measures from the design phase. For Exein, this partnership represents a major opportunity to expand its footprint in the international market. The Italian startup has already received recognition for its innovations in embedded security, and now, with MediaTek, it will gain access to a global ecosystem of customers and manufacturers. The implementation of Exein's technology into Genio chips is expected to begin in 2025, gradually extending across various models and device categories.

With this move, Exein positions itself as a leading European player in IoT cybersecurity, showcasing how Italian startups can compete on a global scale in the ever-evolving world of technological innovation.

GEOPOLITICS CYBER 

Trump considers tariffs of up to 100% on foreign semiconductors: TSMC in the crosshairs

Americans may soon see electronics prices skyrocket in response to an import tax on computer chips ranging from 25% to 100%, announced Monday by U.S. President Donald Trump.

"In the near future, we will impose tariffs on foreign production of computer chips, semiconductors, and pharmaceuticals to bring the manufacturing of these essential goods back to the United States of America," the U.S. president stated during the House Republican Issues Conference.

"The incentive will be that no one will want to pay a tax of 25, 50, or even 100%," he added.

Tariffs have long been one of Trump's preferred economic tools, which he has often promoted as an incentive to compel foreign suppliers to relocate production to the U.S. or to yield on geopolitical issues.

Import taxes are typically paid by those bringing products and components into the country; thus, high tariffs will reduce sales and may push suppliers to manufacture locally to avoid tariffs or shift away from foreign suppliers in favor of domestic ones. Alternatively, the additional costs will ultimately be passed on to end consumers—meaning higher prices for everyone.

The debate over import tariffs has intensified during Trump's second administration, with the president promising a 25% tax on goods from Canada and Mexico and a 60% tax on Chinese imports. However, as previously reported, these tariffs could backfire, as companies with limited options to diversify their supply chains will pass the additional costs on to consumers in the form of higher prices.

This is particularly concerning because, if Trump were to impose a tax on foreign semiconductor imports, consumers and tech buyers in the U.S. could face a double financial hit, given that a large proportion of electronic devices assembled in China contain semiconductors produced abroad.

Trump's new tariff threat would disproportionately impact Taiwan and South Korea, the leading producers of advanced semiconductors used in CPUs, GPUs, storage devices, and memory.

In a statement to Reuters, the Taiwanese government appealed to the White House, emphasizing that semiconductor design and manufacturing collaboration between the two nations is mutually beneficial.

Notably, the Taiwan Semiconductor Manufacturing Company (TSMC) has come under Trump's scrutiny due to its success in securing U.S. clients such as AMD, Apple, and Nvidia. Even Intel, which traditionally manufactures most of its chips in

the U.S. and allied nations, has outsourced a significant portion of its product portfolio to TSMC while working to ramp up domestic production of next-generation process technologies.

The reliance on TSMC exposes American companies to higher prices if tariffs are enforced, as domestic manufacturing alternatives remain limited.

Both TSMC and Samsung are building facilities in the U.S. However, the Taiwanese giant has been hesitant to manufacture its most advanced process technologies—favored by companies like Apple and Nvidia—at its Arizona plants.

Meanwhile, Samsung's facility in Taylor, Texas, has reportedly faced delays due to low production yields in its advanced process technologies. While Samsung has previously manufactured chips for companies such as Nvidia and Apple, these firms have now shifted most of their production capacity to TSMC.

For Nvidia, the biggest challenge could be access to advanced packaging technologies. Even if it manages to produce the chips for its GPUs, many of these rely on sophisticated packaging processes. TSMC has committed to establishing an advanced packaging facility in Arizona in partnership with Amkor, but it will take time before the plant becomes operational.

As previously reported, Intel plans to relocate much of its production back to the U.S. starting this year. However, it will still take time before the chipmaker has sufficient capacity to support contract manufacturing.

With U.S. semiconductor manufacturing capacity still far from full scale, many American chip designers may struggle to avoid negative repercussions from Trump's proposed tariffs.

MALWARE

The TorNet backdoor threatens users in Poland and Germany

Since July 2024, there has been an intensification of malicious activities carried out by a group of cybercriminals orchestrating a sophisticated phishing campaign targeting users in Poland and Germany. These financially driven attacks leverage a combination of highly insidious cyber tools, including the Agent Tesla and Snake Keylogger malware, as well as the latest backdoor named TorNet, distributed through the PureCrypter downloader.

The name TorNet originates from its unique ability to connect compromised devices to the TOR anonymization network, providing threat actors with a covert and difficult-to-detect communication channel.

Cybercriminals utilize the Windows Task Scheduler to ensure the persistence of the malicious code, allowing it to execute continuously even on systems with minimal battery levels. Additionally, to evade antivirus defenses, the attackers employ a particularly deceptive technique: they temporarily disconnect the target device from the network before executing the malicious code, restoring the connection afterward to prevent immediate detection.

The primary attack vector remains phishing emails, skillfully crafted to resemble official communications related to alleged fund transfers or commercial orders. The cybercriminals disguise themselves as representatives of financial institutions, manufacturing firms, or logistics operators. The attachments in these malicious emails typically have a ".tgz" extension, a format that helps evade automatic detection mechanisms in security systems.

Upon opening the attached archive, a .NET-based loader is triggered, injecting PureCrypter directly into the infected device's RAM. This malicious tool conducts a thorough system analysis, detecting the presence of security software, debuggers, or virtualized environments; only after these checks does it activate TorNet. The backdoor then establishes a direct connection with the command and control (C2) infrastructure, allowing attackers to issue instructions to the compromised system and load additional malicious modules directly into the device's memory, significantly expanding the attack's capabilities.

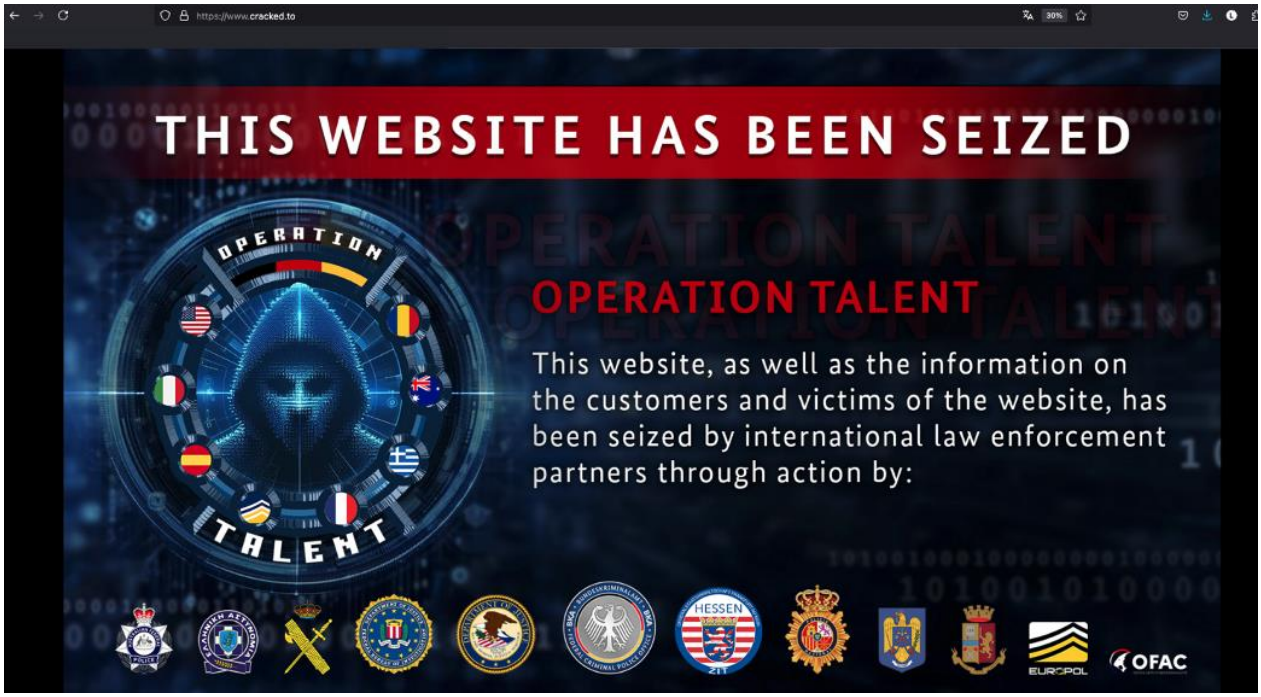
This emerging threat poses a significant danger as it combines advanced evasion techniques, anonymization strategies, and attack escalation capabilities. Consequently, strengthening cybersecurity measures and implementing multi-layered protection strategies are essential to mitigating the risks associated with these sophisticated malicious operations.

CYBER

Operation Talent: FBI dismantles cybercrime forums and seizes illicit domains

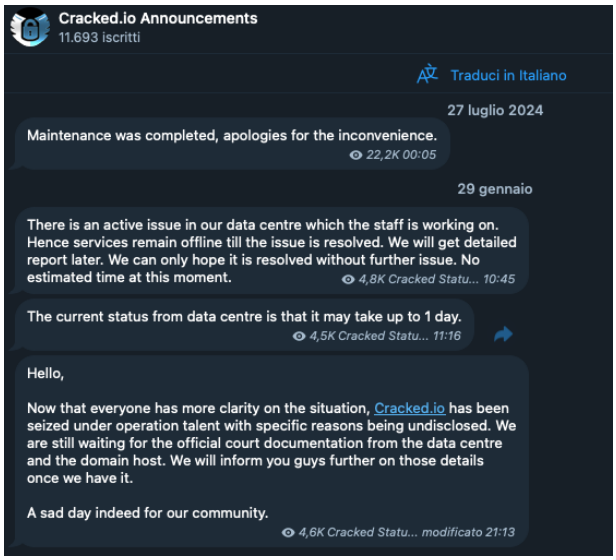
In a major operation aimed at combating cybercrime, the FBI has seized multiple domains dedicated to hacking and the distribution of illicit material, including Nulled.to, Cracked.to, Cracked.io, StarkRDP.io, Sellix.io, and MySellix.io. The DNS records for these domains have been redirected to FBI-controlled servers.

Currently, the seized portals display an official notice stating: "This website has been seized," indicating law enforcement involvement in "Operation Talent." This international initiative was coordinated by the FBI with support from Europol, the Italian Postal Police, the Australian Federal Police, and the German Federal Criminal Police Office.



Launched on January 29, 2025, the operation targeted several websites known for facilitating illicit activities, including the distribution of pirated software, trade in stolen credentials, and the sale of advanced tools for cyberattacks. StarkRDP.io, in particular, provided hosting services for Windows and Linux systems but was frequently exploited by criminal groups for fraud and scams.

Following the seizure, the administrators of Cracked.to issued a statement via their Telegram channel, describing the event as "an extremely sad day for our community." In their message, they indicated they were awaiting official documentation from the data center and domain registrar, suggesting the possibility of the forum reappearing at a new address.



At present, there are no official confirmations regarding any arrests, and neither the FBI nor the other involved agencies have released statements concerning the conducted operations.

GEOPOLITICS

Russia's monetary policy and the risk of stagflation: analysis by a government-affiliated russian think tank

The restrictive stance of Russia's monetary policy has failed to contain price growth, creating a risk of economic slowdown and dragging the country into a phase of stagflation, defined as the simultaneous occurrence of stagnating growth and inflation. This is according to a prominent Russian think tank closely connected to the government.

Last month, the Russian Central Bank raised its benchmark interest rate to 21%, the highest level in the last 20 years, with the declared aim of combating inflation, currently at 8.6%, and responding to high inflation expectations among the population. This decision has sparked dissatisfaction among many business leaders, traditionally critical of the Central Bank's policies, and has drawn criticism from prominent economists involved in shaping government strategies.

"The current high level of the benchmark interest rate, coupled with the prospect of further increases, has created a real risk of economic contraction and a collapse of investments in the near future" said TsMAKP, a research institute that provides consulting services to the government, on Wednesday, January 29.

Economists at the think tank warn that the share of manufacturing companies with a debt service burden of two-thirds of pre-tax profits could double, reaching 20%, with consequent risks of corporate defaults and bankruptcies. They also highlight that, with risk-free interest rates currently around 18%, five-year investment projects should guarantee a minimum return of 130% on the initial capital to remain economically viable.

According to TsMAKP analysts, the restrictive monetary policy has had a marginal impact on the primary factors driving inflation, including increased transaction costs due to Western sanctions, rising prices of imported food products, and higher regulated utility tariffs.

"As a result of the actions taken by the Central Bank, the Russian economy is now exposed to a concrete risk of stagflation, that is, a phase of stagnation, if not outright recession, accompanied by high inflation" the think tank concluded.

For its part, the Central Bank has previously argued that the overheating of the economy, operating beyond its capacity, combined with a labor shortage and uncontrolled wage growth, is itself a stagflation risk factor, with the potential to push the country into recession.