CERT-EU

Cyber Brief (April 2025)

May 2, 2025 - Version: 1

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 311 open source reports for this Cyber Brief[1].
- **Policy, cooperation, and law enforcement.** The FBI sought help to identify Chinese hackers breaching telecoms. The US launched a program to shield sensitive data from foreign threats. Trump dismissed the NSA director following advice from a far-right activist, per Washington Post. China tacitly admitted cyberattacks on US critical infrastructure, framed as a response to US support for Taiwan. It also restricted rare earth exports and banned Chinese firms from engaging with US defence contractors.
- **Cyberespionage and prepositioning.** French, German, and Dutch authorities have linked recent cyberattacks to Russian state-backed actors, including cyberespionage against diplomatic and research institutions, and sabotage attempts on critical infrastructure. A Member of the European Parliament revealed being targeted by Iran-linked hackers in cyberespionage attempt. North Korea-linked DPRK IT Workers campaign expands globally with a focus on Europe. Still in Europe, new cases of mercenary spyware were reported, targeting journalists and activists. On the global level researchers observed the suspected Chinese UNC5221 threat actor actively exploiting critical Ivanti Connect Secure vulnerability, while a Chinese APT group targeted Russian government. Additionally, China accused US intelligence of targeting Chinese cryptographic firm. Notably, Pakistan-linked APT36 exploited Pahalgam attack theme to target Indian government.
- **Cybercrime.** The Tycoon2FA phishing kit now uses advanced evasion techniques, while a Cloudflare phishing campaign leverages Telegram to filter victim IPs. Lazarus continues targeting cryptocurrency platforms with fake job interviews, and the Cookie-Bite proof-of-concept shows how Chrome extensions can bypass MFA. Meanwhile, a Google DKIM flaw is being exploited for nearly undetectable phishing attacks.
- **Data exposure and leaks.** Notable cases of data leaks affected four sectors, namely public administration, telecommunications, technology and transport.
- **Disruption and destruction.** Chinese authorities accused the US NSA of launching cyberattacks during the 2025 Asian Winter Games in Harbin with the aim to disrupt critical systems and steal sensitive information.

- **Information operation.** Czech Prime Minister social media account was compromised to post false messages, including about a Russian attack on Czech soldiers. Lithuania warned of Russian and Belarusian hybrid activity towards Belarusian diaspora. Japanese media reported on China using AI in information operations targeting Taiwan.
- **Hacktivism.** In Europe, Russia-linked supposed hacktivists targeted various entities in Europe, including Finnish election-related organisations and Dutch organisations, while a coalition of hacktivists dubbed "Holy League" targets British military with DDoS attacks.

Europe

Cyber policy and law enforcement

Czech government sanctioned Russian GRU officer
On April 2, the Czech government added journalist Natalia Sudlianková and GRU officer Alexei Shavrov to its sanctions list for ties to Russian military intelligence. Both are accused of supporting Russian-state influence campaigns and information operations in Czechia. Sudlianková was ordered to leave the country within 30 days. `russia` `sanctions` link

Operation Endgame brings down Smokeloader customers
On April 9, Europol announced that Operation Endgame, a cooperation initiative between Europol, several EU countries' police, the US, and Eurojust, that led to the takedown of the biggest malware droppers in May 2024, conducted a new sweeping operation against Smokeloader pay-per-install botnet in early 2025. This led to arrests, house searches, and arrest warrants of customers of this botnet. `takedown` `arrests` link

Six cybercriminals arrested in Spain for AI scam
On April 7, Spain's Policía Nacional announced their arrest of six individuals belonging to a criminal organisation that scammed over 19 million euros out of victims worldwide. They created fake ads featuring well-known national figures through artificial intelligence, recommending that people invest in products; the victims were chosen via algorithms. `arrests` link

Cyberespionage and prepositioning

French authorities attribute APT28 cyberespionage campaign to Russian state interests
On April 29, the French cybersecurity agency ANSSI reported that APT28, a Russian-linked threat group, had targeted the French government, diplomatic, and research sectors between 2021 and 2024. These cyberattacks aimed to gather intelligence and are part of broader operations affecting Europe, Ukraine, and North America. The attacks continue amid Russia's ongoing war against Ukraine. ANSSI and its partners identified multiple infection chains used in these campaigns. `russia` `diplomacy` `research` link

German intelligence looking into likely Russia-linked cyberattack targeting research organisation
On April 8, Germany's Federal Office for Information Security (BSI) and the Federal Office for the Protection of the Constitution (BfV) announced they were investigating a cyberattack targeting the German Association for East European Studies (DGO), an organisation specialised in international relations. Threat actors breached DGO at the end of March and accessed their e-mails. German intelligence officials say that they suspect the threat actors are Russia-linked, possibly APT29. `russia` link

Russian hackers target Dutch critical infrastructure in first known sabotage attempt
On April 22, the Dutch Military Intelligence Agency (MIVD) revealed that Russian hackers

attempted to sabotage the digital control system of a Dutch public facility last year, marking the first known cyberattack on the Netherlands' critical infrastructure. The agency warned of growing threats from both Russia and China, highlighting Russia's sabotage efforts in the North Sea and increasing cyber operations against European nations supporting Ukraine. `russia` link

Russia-linked threat actors target Microsoft OAuth workflows
On April 22, Volexity published a blog post on Russia-linked phishing campaigns abusing Microsoft OAuth 2.0 authentication workflows to target entities with ties to Ukraine. The threat actors, tracked as UTA0352 and UTA0355, impersonate European officials and use platforms like Signal and WhatsApp to lure victims into sharing Microsoft authorisation codes. `public administration` `russia` link

Russia-linked Gamaredon targeted a foreign military mission in Ukraine with removable drives delivering GammaSteel
Russia-linked threat actor Gamaredon targeted a foreign military mission of a Western country based in Ukraine with GammaSteel malware. Initial access was gained through infected removable drives. The infection chain involves PowerShell scripts for obfuscation and services like write.as and cURL with Tor for data exfiltration. `russia` link

MEP Hannah Neumann targeted by Iran-linked hackers in cyberespionage attempt
On April 23, European Parliament member Hannah Neumann revealed that her office was targeted by a Tehran-linked cyberespionage operation. Hackers impersonated trusted contacts to deliver malware to her laptop. The attack, attributed to Iranian group APT42, was blocked before any data was stolen. Neumann, chair of the EU-Iran delegation, believes the attempt aimed to intimidate her due to her critical stance on Iran's regime. `iran` link

Chinese mobile interconnect providers pose surveillance risks
On April 17, iVerify, a cybersecurity company, highlighted that China's state-owned mobile interconnect providers are integral to global mobile traffic, routing data for over 60 operators across 35 countries, including in Europe. iVerify emphasised the risk for man-in-the-middle attacks by such Chinese mobile interconnect providers, which could intercept traffic whenever traffic is routed using outdated, unencrypted protocols like SS7 and Diameter. `china` `telecommunications` link

North Korea-linked DPRK IT Workers campaign expands globally with a focus on Europe
On April 1, Google Cloud reported that North Korea-linked DPRK IT Workers campaign has expanded. While the United States remains a key target, over the past months, DPRK IT workers have encountered challenges in seeking and maintaining employment in the country. Google assesses that the campaign has expanded globally, with a notable focus on Europe. The IT Worker reportedly actively sought employment with multiple organisations within Europe, particularly those within the defence industrial base and government sectors. `north korea` link

Two Serbian journalists targeted with Pegasus spyware in February 2025
On March 28, Amnesty International reported that two journalists from the Balkan Investigative Reporting Network (BIRN), an award-winning Serbian network of investigative journalists, were targeted with NSO Group's Pegasus spyware. According to Amnesty International investigation's investigation, the intrusion happened in February 2025. This is the third time in two years that Amnesty International's Security Lab has found NSO Group's Pegasus spyware being used against civil society in Serbia. `psoa` link

EU country WhatsApp users among victims of 2019 NSO spyware campaign
On April 9, the online news outlet TechCrunch published an article about court documents revealing locations of WhatsApp victims targeted by NSO spyware in 2019. At the time, more than 100 human rights activists, journalists, and civil society members were targeted, with a

total of around 1400 victims. It now appears that among the victims, there were users in Spain, the Netherlands, Hungary, France, and the United Kingdom. `psoa` link

Apple warns users, including a journalist and an activist in Europe, of spyware targeting
On April 29, Apple notified users in 100 countries that they may have been targeted with government spyware, including Italian journalist Ciro Pellegrino and Dutch activist Eva Vlaardingerbroek. The alerts follow similar warnings by Apple and other tech firms, amid investigations into mercenary spyware allegedly sold to governments and used against journalists, activists, and NGOs. `psoa` link

Suspected data breach in Finnish Foreign Ministry's remote access service
On March 27, the Finnish Ministry for Foreign Affairs detected suspicious activity in its remote access service, raising concerns about a possible data breach. In response, the Ministry swiftly disabled the service and launched an internal investigation. The incident was reported to the National Bureau of Investigation and cybersecurity authorities for further analysis. The Ministry emphasised its commitment to securing its systems and mitigating any potential risks. link

Polish political party targeted ahead of Polish Presidential elections
On April 2, Poland's Prime Minister Donald Tusk posted on X that his political party had been the target of a cyberattack and suggested it had Eastern origins. Donald Tusk said his Civic Platform party's computer system was targeted, ahead of the upcoming presidential election. The head of Tusk's office later told Polish media that the cyberattack consisted of an attempt to take control of computers of employees of the Civic Platform office and the election staff. link

Cybercrime

NTLM exploit CVE-2025-24054 actively abused via malicious .library-ms files
On April 16, Check Point reported active exploitation of CVE-2025-24054, an NTLM hash disclosure vulnerability triggered by malicious .library-ms files. Despite Microsoft's patch on March 11, attackers began leveraging the flaw by March 19, targeting entities in Poland and Romania via malspam campaigns. The exploit requires minimal user interaction, such as right-clicking or navigating to a folder, and resembles the earlier CVE-2024-43451 vulnerability. link

Disruption and destruction

Cyberattack disrupts Spanish water supplier Aigües de Mataró
On April 23, a cyberattack hit Spanish water supplier Aigües de Mataró, affecting corporate systems and its website but leaving water supply and quality controls intact. Aigües de Mataró stated that the attack could inconvenience its subscribers who became unable to access corporate services, and might experience delays for billing and other administrative procedures. The nature of the attack remains unconfirmed. link

Information operations

Czech Prime Minister Petr Fiala social media account compromised
On April 8, hackers breached Czech Prime Minister Petr Fiala's X (formerly Twitter) account, posting false messages, including about a Russian attack on Czech soldiers. The malicious activity aimed to mislead followers and potentially damage the Prime Minister's reputation. `russia` `social media` link

Lithuania State Security warns of Russian and Belarusian hybrid activity towards Belarusian diaspora

On April 23, the State Security Department of Lithuania publicly reported about hybrid attacks planned by Russian and Belarusian intelligence services against Belarusian diaspora living in Lithuania. The attacks involved information operation components such as videos allegedly filmed by Litvinist groups and directed against Lithuania being spread on social networks. The goal of the attacks would reportedly be to incite ethnic tension and increase the sense of insecurity in Lithuania. `russia` link

Data exposure and leaks

Major data leak under investigation at Dutch ministries
On April 10, a significant data leak affecting multiple Dutch ministries, including Economic Affairs and Climate and Green Growth, came to light. Dutch authorities have not confirmed if any personal data was accessed or stolen. The Interior Ministry is leading the investigation, and the Dutch Data Protection Authority has been notified, though the full scope and impact remain unclear. `public administration` link

Samsung Germany data breach exposes 270.000 customer support records
On April 14, German media revealed that on March 30, data from Samsung Germany was compromised in a data breach of their logistics provider, Spectos, exposing a support database containing customer data. The breach led to the theft of 270.000 customer support records, now listed on Have I Been Pwned, including emails, names, purchases, and tracking numbers, which could be misused for phishing, although access to core systems was reportedly blocked and direct identity theft risks remain low. `technology` link

Europcar GitLab breach exposes data of up to 200,000 customers
In March 2025, a hacker gained access to Europcar Mobility Group's private GitLab repositories, stealing 37 GB of data including source code, SQL backups, and configuration files. The breach may impact up to 200 000 customers, with exposed names and email addresses from Europcar's Goldcar and Ubeeqo brands. Europcar confirmed the GitLab breach, notified authorities, and is contacting affected users. No passwords or payment information were reportedly compromised. `transport` link

Hacktivism

Russia-linked supposed hacktivists target Finnish election-related organisations
On April 8, according to Finnish newspaper Yle, Russia-linked supposed hacktivists NoName057(16) claimed responsibility for several DDoS attacks that targeted almost all Finnish parliamentary parties, as well as several organisations and websites of individuals. Election-related websites were among the targets. The group claims the attacks respond to President Stubb's proposed Ukraine ceasefire. `russia` `election` link

Pro-Russia hacktivists target Dutch public organisations in DDoS attacks
On April 30, pro-Russia threat actor NoName057(16) disrupted Dutch public and private services with ongoing DDoS attacks, targeting websites across several provinces and municipalities. The group claimed retribution for military aid to Ukraine. Despite service disruptions, Dutch officials confirmed no internal systems were compromised. The cybercrime actor continues its campaign through its DDoSia platform. `russia` link

Coalition of hacktivists Holy League targets British military with DDoS attacks
On April 7, several media outlets reported on the Holy League, a coalition of around 90 pro-Russian and pro-Palestinian hacktivist groups, launching weekly DDoS attacks on British military

and infrastructure agencies. Their mission is to conduct cyberwarfare against the allies of Ukraine and Israel. `defence` link

World

Cyber policy and law enforcement

FBI seeks public help to identify Salt Typhoon hackers behind telecom breaches
On April 24, the FBI requested public assistance and announced a reward of up to 10 million US dollars for information to identify the Salt Typhoon hackers, a Chinese cyberespionage group responsible for breaches in U.S. and global telecom networks. These hackers gained access to sensitive data, including private communications of US officials, and are still targeting telecom providers worldwide, with ongoing investigations and potential sanctions on related Chinese firms. `china` `united states` link

US implements a national security programme to protect Americans' sensitive data from foreign adversaries
On April 11, the US Department of Justice began implementing a national security program under Executive Order 14117 to prevent foreign adversaries like China, Russia, and Iran from accessing Americans' sensitive personal and government-related data. The initiative aims to counter threats such as espionage and AI-enabled surveillance by restricting data transactions and enforcing new compliance measures. `artificial intelligence` `united states` link

Trump fires NSA Director on advice from Laura Loomer, per Washington Post
On April 2, Gen. Timothy Haugh was dismissed as Director of the US National Security Agency (NSA), reportedly following advice from far-right activist Laura Loomer, according to The Washington Post. Loomer had urged President Trump to remove officials she deemed insufficiently loyal. The decision has drawn criticism from top Democrats, who expressed concerns about national security implications. `united states` link

China tacitly acknowledges cyber activity targeting US infrastructure
On 10 April, the Wall Street Journal reported that during a confidential meeting in Geneva in December 2024, Chinese officials indirectly signalled that Beijing had supported cyber intrusions against US critical infrastructure. The activity, reportedly linked to Volt Typhoon, was framed as a response to US support for Taiwan. US officials interpreted the remarks as a strategic warning amid escalating tensions. `china` link

China restricts exports of rare earth minerals
On 13 April, the New York Times reported that China imposed new export restrictions on rare earth minerals and magnets, requiring special licenses. These materials are crucial for semiconductor production. Additionally, China's Ministry of Commerce, alongside the General Administration of Customs, reportedly banned Chinese firms from engaging with several American companies, notably military contractors. `china` link

Cyberespionage and prepositioning

Suspected Chinese UNC5221 threat actor actively exploiting critical Ivanti Connect Secure vulnerability
On April 3, Ivanti disclosed CVE-2025-22457, a critical buffer overflow vulnerability in Ivanti Connect Secure VPN appliances, enabling remote code execution. Mandiant and Ivanti reported active exploitation since mid-March by UNC5221, a suspected China-nexus espionage group,

deploying custom malware. A patch was released on February 11, 2025; users are urged to upgrade immediately. `china` link

Chinese APT IronHusky targets Russian government with upgraded MysterySnail malware
On April 17, Kaspersky reported that Chinese-speaking IronHusky hackers are targeting Russian and Mongolian government organisations using upgraded MysterySnail RAT malware. The updated implant, observed in recent attacks, is deployed via malicious MMC scripts disguised as Word documents, which download second-stage payloads and establish persistence on compromised systems. `china` `russia` link

China accuses US intelligence of targeting Chinese cryptographic firm
On April 28, China's National CSIRT (CNCERT) reported on a 2024 cyberespionage operation where a US intelligence agency targeted a leading Chinese provider of commercial cryptographic products, stealing customer data and code project files. CNCERT stated that the US-linked threat actor operated mainly during US working hours and used high-level cyberespionage tactics. This publication was likely intended as a response to recent public reporting on China's Volt Typhoon campaign. `china` `united states` link

Trojanised Alpine Quest app used to spy on Russian military operations
On April 21, researchers at Russian mobile antivirus company Doctor Web uncovered a new Android spyware campaign hiding inside trojanised versions of the Alpine Quest mapping app, often used by Russian soldiers for war zone planning. The malicious app, promoted as a cracked Pro version, steals sensitive data such as geolocation, contacts, and files - demonstrating how mobile surveillance is now being deployed on both sides of the conflict for military intelligence. `defence` `russia` link

Threat actor Sapphire Werewolf targets likely Russian energy companies with updated Amethyst stealer
On April 9, BI.ZONE Threat Intelligence reported on the threat actor Sapphire Werewolf and its enhanced Amethyst stealer to target energy companies, distributing it via phishing e-mails disguised as HR memos in Russian. The updated malware includes advanced virtual environment checks and uses Triple DES encryption for string protection. It collects credentials from browsers and applications, sending system data to specific addresses. The malware also executes a decoy PDF and checks for virtual machine indicators. `energy` `russia` link

Lazarus targets South Korean organisations in Operation SyncHole
On April 24, Kaspersky reported that between November 2024 and February 2025, the North Korean Lazarus group launched a campaign named Operation SyncHole targeting at least six organisations in South Korea. These organisations span industries such as software, IT, finance, semiconductor manufacturing, and telecommunications. The operation exploited vulnerabilities in South Korean software to execute watering hole attacks and install various forms of malware. `finance` `north korea` `technology` `telecommunications` link

Kimsuky APT group exploits RDP and MS Office flaws in global cyberespionage campaign
On April 14, researchers from AhnLab Security Intelligence Center (ASEC) revealed that the North Korean-linked Kimsuky group is actively exploiting RDP and Microsoft Office vulnerabilities—specifically BlueKeep (CVE-2019-0708) and CVE-2017-11882—in a global cyberespionage campaign known as Larva-24005. The attackers deploy custom malware like MySpy, RDPWrap, and keyloggers to maintain persistent access and exfiltrate sensitive data from targeted sectors across South Korea, the U.S., China, Japan, and more. `north korea` link

APT36 exploits Pahalgam attack theme to target Indian government with Crimson RAT
On April 30, cybersecurity firm Seqrite reported that Pakistan-linked APT36 used Pahalgam attack-themed decoy documents to target Indian government entities. The campaign employed Crimson RAT malware delivered via malicious Excel files with embedded macros. These files

extracted and executed the malware while displaying legitimate-looking documents. The operation shared infrastructure with SideCopy, indicating coordination between the groups. `india` `pakistan` link

Apple patches two exploited zero-days in targeted iPhone attacks
On April 16, Apple released emergency updates to fix two zero-days—CVE-2025-31200 in CoreAudio and CVE-2025-31201 in RPAC—used in targeted iPhone attacks. The flaws affected multiple Apple platforms and enabled remote code execution and PAC bypass. Apple and Google's threat team discovered the issues. Users are urged to update devices despite the attacks being highly targeted. link

ClickFix: State-sponsored actors exploit new phishing technique across key sectors
On April 17, Proofpoint reported that state-sponsored actors, including TA571, TA578, UAC-0050, and Storm-1865, have increasingly adopted the "ClickFix" phishing technique. This method deceives users into executing malicious PowerShell commands via fake error messages or CAPTCHA prompts, leading to malware infections such as DanaBot, Lumma Stealer, and AsyncRAT. Targets include sectors like transportation, logistics, and hospitality, with campaigns impersonating services like Booking.com and Microsoft SharePoint. link

Brazil allegedly conducts cyberespionage towards Paraguay amid energy trade negotiations
On March 31, UOL, a Brazilian media entity, alleged that the Brazilian Intelligence Agency (ABIN) conducted a cyberespionage campaign in 2024 against the Paraguayan government to obtain sensitive information regarding energy trade negotiations. The negotiations specifically pertained to tariffs on the Itaipu hydroelectric plant. link

Cybercrime

Tycoon2FA phishing kit adopts new evasion techniques
On April 10, Trustwave reported that the Tycoon2FA phishing kit has incorporated new evasion tactics, including obfuscated JavaScript using invisible Unicode characters, custom HTML5 CAPTCHA challenges, and anti-debugging scripts. These enhancements aim to bypass security measures and hinder analysis. The kit continues to target Microsoft 365 users, emphasising the need for robust detection strategies against evolving phishing threats. link

Phishing campaign impersonates Cloudflare services and uses Telegram to filter victim IPs
On April 1, researchers at hunt.io reported that they had tracked a phishing campaign which used fake Cloudflare prompts to trick users into clicking on a malicious redirect link. Further analyses revealed that the threat actors used a Russian-language Telegram channel and used Telegram in general to filter victim IPs. link

Lazarus ClickFake Interview campaign targets cryptocurrency platforms
On March 31, Sekoia reported that North Korea-linked threat actor Lazarus continued its targeting of the cryptocurrency sector through fake job interview, lately through so-called ClickFake Interviews. ClickFake Interview leverages fake job interview websites to deploy a Go backdoor on Windows and macOS environments by using the ClickFix tactic. `north korea` link

Cookie-Bite PoC shows how malicious Chrome extensions can bypass MFA and hijack cloud sessions
On April 22, Varonis Threat Labs researchers unveiled the Cookie-Bite attack, a proof-of-concept using a stealthy Chrome extension to steal Azure Entra ID session cookies and bypass MFA protections. The malicious extension monitors Microsoft login events, exfiltrates session tokens, and enables attackers to inject them for full access to services like Microsoft 365 and Teams, highlighting the severe risks posed by malicious browser extensions in cloud-based identity environments. `technology` link

Google OAuth and DKIM flaw enables nearly undetectable phishing attacks

On April 15, hackers exploited a flaw in Google's DKIM system to send phishing emails that passed authentication checks and appeared to come from no-reply@google.com, leading victims to a fake Google support portal hosted on sites.google.com. By abusing OAuth notifications and DKIM's
limited validation scope, attackers crafted highly convincing credential-stealing messages—an approach also seen targeting PayPal users through similar infrastructure abuse. `technology` link

Data exposure and leaks

SK Telecom confirms malware breach exposing sensitive USIM data

On April 22, South Korea's largest mobile operator, SK Telecom announced that malware had infiltrated its systems, exposing sensitive USIM data such as IMSI, MSISDN, and authentication keys from a cyberattack discovered on April 19. Although there's no evidence of misuse, the company reported the breach to authorities and implemented stricter USIM swap controls to prevent SIM-related fraud and enhance account protection for its 34 million subscribers. `telecommunications` link

Information operations

China using AI in information operations targeting Taiwan

On April 9, The Japan Times published an article about China conducting information operations on social media, namely Facebook and TikTok, to create internal turmoil in Taiwan. In fact, Taiwan's National Security Bureau published a report about China using AI to further these objectives, both in the generation and dissemination of messages. Their goal is to create division in the population. `artificial intelligence` `china` `japan` link

Disruption and destruction

China accuses US of cyberattacks during Asian Winter Games

On April 15, Chinese authorities accused the US NSA of launching cyberattacks during the 2025 Asian Winter Games in Harbin. The attacks allegedly targeted infrastructure in Heilongjiang province and attempted to access athletes' personal data. Three NSA agents were named, and US universities were implicated. China claims the activity aimed to disrupt critical systems and steal sensitive information. `china` link

[1] Conclusions or attributions made in this document merely reflect what publicly available sources report. They do not reflect our stance.

TLP definition

TLP	Disclosure	Message
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.

TLP	Disclosure	Message
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and its clients.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.