Cyber Security Brief (January 2024)

February 2, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 476 open source reports for this Cyber Security Brief.
- Relating to cyber policy and law enforcement, EU's chief diplomat warned that global elections are prime targets for disinformation campaigns and several cybercriminals involved in malware development and operation or darknet forum administration were arrested, sentenced or sanctioned.
- On the cyberespionage front, in Europe, there were reporting of activity by likely Chinese, Russian and Turkish threat actors. In the rest of the world, two major breaches against prominent technology companies were attributed to the Russia-linked APT29 threat actor. There were also new reports on the cybersurveillance tool Pegasus usage.
- Relating to cybercrime, a city in Spain, refused to pay a ransomware group, despite having the municipal operation disrupted and the Conti ransomware operation reappeared. In Europe, for January, the top most active ransomware operations have been Lockbit, 8Base, Hunters International, MedusaLocker, Akira, and BlackBasta; the most targeted sectors have been manufacturing, construction & engineering, retail, legal & professional services, and hospitality.
- There were disruptive attacks on Ukrainian state organisations, including in the energy and railway sectors. In the rest of the world, a cyberattack affected a global fintech firm.
- As regards data exposure and leaks, significant incidents affected citizens' data in Brazil, and entities in the defence, technology, telecommunication and social media sectors. A new dataset, dubbed Naz.API, containing millions of stolen credentials appeared.
- On the hacktivism front, in Europe, groups of Russian, Iranian or Belarusian origins claimed attacks.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in January 2024.

Europe

Cyber policy and law enforcement

EU chief diplomat Josep Borrell warns of elections targeted by disinformation
On January 23, EU's chief diplomat Josep Borrell warned that global elections are prime targets for disinformation campaigns, especially from countries like Russia. He presented the EU's second annual disinformation report, which examined over 750 attacks between December 2022 and November 2023. These attacks involved tactics such as spreading false stories and harassing legitimate sources, using 4.000 channels like websites and social media platforms, often with pre-planning for election interference. `Warning` , `Elections`

Combined police operation disrupts the Grandoreiro banking malware
On January 30, the Federal Police of Brazil, supported by ESET, Interpol, the National Police of Spain, and Caixa Bank, disrupted the Grandoreiro banking malware operation and announced five arrests connected to it. This malware has been targeting Spanish-speaking countries, including Spain, since 2017, causing around 120.000.000 US dollars in losses. `Take down` , `Arrests`

Spanish Police arrest the leader of vishing scheme
On January 12, 2024, the Spanish National Police arrested the leader of a criminal organisation involved in voice phishing scams that targeted US-based individuals and businesses since at least 2021. The group used fake identities and forged banking cards to steal up to 5 million euros, which they moved to Spanish bank accounts, converted into cryptocurrencies, and sent to businesses in the UK, Panama, and Lithuania owned by the criminal network. `Arrests`

Cyberespionage

New China-aligned APT group Blackwood
On January 24, the cybersecurity firm ESET disclosed a previously unknown China-linked threat group called Blackwood, active since 2018. Blackwood uses a sophisticated implant named NSPX30, delivered through adversary-in-the-middle attacks on legitimate software updates. NSPX30 can evade Chinese antivirus software and targets Chinese and Japanese entities in the manufacturing, trading, and engineering sectors, as well as individuals in China, Japan, and the UK. `Chinese threat actor`

Ukraine thwarts Russian surveillance hacking in Kyiv
Ukraine's Security Service (SBU) discovered and neutralised two surveillance cameras in residential buildings in Kyiv, which were hacked by Russian intelligence to spy on air defence forces and critical infrastructure. The state-sponsored hackers used these cameras to monitor strategic areas, including critical facilities and a parking lot. `Russian threat actor`

Turkish cyberespionage group's recent focus on the Netherlands
The security company Hunt & Hackett reported on January 5 about Sea Turtle, a Türkiye-based, likely state-sponsored cyberespionage group. In 2023 Sea Turtle conducted multiple campaigns in the Netherlands. The group is generally targeting government bodies, telecommunication companies, and Kurdish groups in Europe and the Middle East. Their primary tactics include DNS hijacking and sensitive data theft, aligning with Turkish strategic interests. `Turkish threat actor`

Likely cyberespionage threat actor exploiting zero-days in Ivanti's Connect Secure VPN
According to a report by Volexity, two zero-day vulnerabilities in Ivanti's Connect Secure VPN and

Policy Secure network access control appliances are currently being widely exploited. These vulnerabilities, CVE-2023-46805 and CVE-2024-21887, were first used in attacks in December and have escalated since January 11. The victims include organisations of varying sizes globally, including Fortune 500 companies across different industries. `Unattributed threat actor`

Cybercrime

Majorca's Calvià city hit by 11M ransomware attack

On January 16, the Calvià City Council in Majorca was targeted by a ransomware attack, which disrupted municipal services. The city refused to pay the 11 million US dollars ransom demand. `Spain` , `Public administration`

Disruption

Several Ukrainian state-run bodies report cyber attacks

On January 25, several major Ukrainian state organisations, including the energy company Naftogaz, the national postal service Ukrposhta, Ukrtransbezpeka, a convention centre, and the ticket sales system for Ukrainian state railways, reported cyber attacks on their IT systems. These attacks were attributed to Russian intelligence by a government source. Other victims in the finance and banking sectors were also affected but not disclosed officially. `Ukraine` , `Energy` , `Transport` , `Postal service` , `Finance`

Information operations

Fake messages alleging Ukrainian ceasefire with Russia

On January 29, Ukraine's Cyber Police issued a warning regarding an information operation by pro-Russia influence actors spreading disinformation, although they did not specify how the messages were being disseminated. The message disseminated, with the intent of discrediting the country's leadership, alleged that the Office of the President of Ukraine had agreed to a ceasefire with Russia. `Russian threat actor` , `Ukraine`

Germany uncovers Russian disinformation campaign on X

Experts commissioned by the German foreign ministry monitored X, between December 20, 2023, and January 20, 2024. They uncovered more than 50.000 fake user accounts that made over one million tweets in German conducting pro-Russian disinformation campaigns. The accounts also often provided links to fake news stories. `Russian threat actor` , `Germany`

Data exposure and leaks

Ukrainian group claims the leak of Russian banks customer info

KibOrg, a Ukrainian group of journalists and IT specialists, released, on January 8, what they claimed was the full customer database of Russia's largest commercial bank, Alfa-Bank, containing personal details of over 30 million clients dating back to 2004. Alfa-Bank denied and dismissed the data leak as misinformation. KibOrg declared that it will continue its efforts to expose Russian activities and fight misinformation in cyberspace. `Russia` , `Banking`

Swiss air force data exposed after cyberattack on US security firm

The US security firm Ultra Intelligence & Communications, which serves clients like the Swiss Air Force and NATO, suffered a cyberattack by the BlackCat ransomware group, leading to a leak of about 30 GB of sensitive documents on the dark web. The breach did not affect the operational

systems of the Swiss armed forces, but exposed contracts and communications technology purchases for encrypted Swiss Air Force communications. `Switzerland`, `Defence`

Hacktivism

Iran-nexus group claims credit for attack on Albania's Parliament
In late December 2023, Albania's Parliament faced a cyberattack, suspected to be carried out by Iranian hackers. The Iran-linked group Banished Kitten claimed responsibility for the activity, likely in retaliation for Albania hosting the Iranian opposition group MEK. The attack also targeted telecom companies and an Albanian airline, with threats to leak stolen data and wipe data from servers. `Albania`, `Parliament`

NoName targets Finland government ahead of presidential election
On January 25, pro-Russian hacktivist group NoName057(16) (a.k.a. NoName) claimed DDoS attacks against the websites of three Finnish government entities and one Finnish presidential candidate ahead of the January 28, 2024, Finnish presidential election. As proof of successful disruptions, the hacktivist group provided a link via their Telegram channel to a web performance-monitoring tool and a screenshot allegedly showing the unresponsive websites. `Finland`

Pro-Ukraine hacktivist group Blackjack targets Russian ISP
The pro-Ukraine hacktivist group Blackjack; has claimed, on January 10, a cyberattack against the Russian internet service provider M9com, in retaliation for the attack on Ukraine's largest telecom service provider, Kyivstar, which took place on December 12, 2023. The claimed activity involved disrupting M9com's services, stealing confidential data, and deleting significant amounts of data. `Russia`, `ISP`

Belarusian hacktivist group disrupts state news agency
On January 2, Belarusian hacktivists, known as the Belarusian Cyber-Partisans, claimed responsibility for shutting down BelTA, the country's largest state-owned media outlet, during the New Year's weekend. They reportedly wiped the main website servers, backups, and other network components, citing retaliation against President Alexander Lukashenko's propaganda efforts. `Belarus`

Anonymous Sudan launches cyber attack on UK in response to Yemen airstrikes
On January 12, the hacktivist group Anonymous Sudan claimed responsibility for a cyberattack against the UK, alleging it was in response to the UK's support of Israel and the air attacks in Yemen. The attack targeted the London Internet Exchange (LINX), impacting some services. There was no independent verification of the group's claims. `UK`

Hack wiped 2 petabytes of data from Russian research centre
On January 26, pro-Ukrainian hacktivists reportedly breached the Russian Center for Space Hydrometeorology, linked to Russia's space agency, Roscosmos. The centre supports various sectors, including the military, civil aviation, agriculture, and maritime industries. Ukrainian authorities claim that the hacktivists destroyed 280 servers at the research centre, resulting in the loss of 2 petabytes of data, but they did not confirm their direct involvement in the attacks. `Russia`

Russia-linked NoName targets Lithuania and Ukraine
On January 10 and 11, the pro-Russian hacktivist group NoName claimed DDoS attacks on several European websites, including Ukrainian and Lithuanian financial services, telecommunications, transportation, and logistics entities. These attacks coincided with Ukrainian President Zelensky's visit to Lithuania and the country's announcement of a 200 million euro military aid package for Ukraine. `Ukraine`, `Lithuania`

World

Cyber policy and law enforcement

The FBI disrupted KV Botnet used by China-linked Volt Typhoon
On January 31, the FBI announced in a press conference that they disrupted the KV Botnet used by China-linked threat actor Volt Typhoon, namely used to hijack small office/home offices (SOHO) in the United States to ultimately target critical infrastructure. `Take down`

Russian TrickBot malware developer sent to prison
On January 25, a Russian national was sentenced to five years and four months in a US prison for his role in creating and distributing the Trickbot malware. Trickbot evolved from a banking credential theft tool in 2015 to a modular cybercrime tool used by groups like Ryuk and Conti for infiltrating corporate networks and conducting attacks worldwide. `Sentence`

US court convicts BreachForums administrator
On January 19, a US court convicted a US individual for numerous cybercrimes. The individual is reportedly one of the administrators of BreachForums, one of the most prolific cybercrime forums. The individual received a penalty of supervised release spanning 20 years. `Sentence`

Crackdown on xDedic cybercrime marketplace
The US Department of Justice issued charges against 19 individuals linked to the xDedic dark web cybercrime marketplace, responsible for over 68 million US dollars in fraudulent activities. The marketplace has been involved in selling stolen credentials and personal information. The international operation, involving multiple countries, dismantled the marketplace that operated globally with over 700.000 compromised servers. `Charges`

US, UK, Australia sanction REvil hacker
On January 23, Australia, the US, and the UK imposed sanctions on the Russian national Aleksandr Gennadievich Ermakov for his involvement in the 2022 hack of Medibank, a prominent Australian health insurance provider, and the REvil ransomware group. The Medibank hack in October 2022 affected around 10 million individuals, leading to data theft and disruptions. `Sanctions`

US Department of Energy to invest in clean energy cybersecurity innovations
On January 17, the US Department of Energy (DOE) called for submissions for innovative cybersecurity tools to secure clean energy infrastructure. The DOE plans to offer grants of up to 3 million US dollars across approximately 10 awards, totalling an investment of 30 million US dollars. `Innovation`

Cyberespionage

Russia-linked APT29 breached Microsoft between November 2023 and January 2024
On January 19, Microsoft revealed that on January 12, 2024, the Russian state-sponsored threat actor APT29 (aka Midnight Blizzard) breached some of its corporate e-mail accounts, leading to data theft. This intrusion took place in November 2023 when the threat actor executed a password spray attack to gain access to a legacy non-production test tenant account. On January 26, Microsoft confirmed that the threat actor also breached other organisations as part of this malicious campaign. `Russian threat actor` , `Technology`

HPE: Russia-linked APT29 breached security team's e-mail accounts
On January 24, Hewlett Packard Enterprise (HPE) disclosed that suspected Russian hackers of the group APT29 had breached their Microsoft Office 365 e-mail system, stealing data from their

cybersecurity team and other departments. HPE learned of the breach on December 12, 2023, when it was revealed that the attackers had accessed their cloud-based e-mail system in May 2023 and also infiltrated their SharePoint server to steal files. `Russian threat actor`, `Technology`

DPRK-linked group experimenting with CTI reports as decoys
On January 22, security researchers at SentinelLabs disclosed a campaign by ScarCruft (aka APT37), which is believed to be linked to North Korea. The targets included South Korean academics focused on North Korean affairs and a North Korea-focused news organisation. ScarCruft tested the use of a technical threat research report as a decoy, possibly also targeting cybersecurity professionals. `North Korea threat actor`

India targeting high-profile journalists with spyware
Amnesty International and the Washington Post reported on December 28, 2023, that the Indian government targeted two prominent journalists, Siddharth Varadarajan and Anand Mangnale, using Pegasus spyware. Both received intrusion attempts on their Apple devices in late October 2023. Varadarajan was leading protests, while Mangnale was working on an article about a major Indian conglomerate. The intrusions used the BLASTPASS exploit chain, exploiting vulnerabilities to send malicious images via PassKit attachments. `Indian threat actor`

Advocacy group claims Togo-based journalists' phones infected with Pegasus
On January 23, the Reporters without Borders (RSF) advocacy group claimed to have identified traces of NSO Group's Pegasus spyware on the phones of two Togo-based journalists. The journalists were previously held in pre-trial detention in November 2023 due to their reporting. RSF's investigation began on December 18 and concluded on January 16, 2024. `PSOAs`

Cybercrime

VexTrio: brokering malware for 60+ affiliates
On January 23, security company Infoblox uncovered VexTrio, an entity involved in a large criminal affiliate program. VexTrio, characterised as the Uber of cybercrime, operates a traffic distribution system (TDS) network with over 70.000 domains, assisting at least 60 affiliates. VexTrio uses victim information from browser settings and cached data to redirect victims to an affiliate's malicious content based on predefined profiles. `Malware brokerage`

ThreeAM likely associated to reorganised Conti activities
On January 19, security researchers at Intrinsec revealed that ThreeAM, a cybercrime actor, likely works under the wing of the reorganised Conti syndicate (Conti's former TEAM 2, now known as Royal). `Malware`

US Securities and Exchange Commission's X account compromised through SIM swap attack
On January 22, the US Securities and Exchange Commission (SEC) confirmed that their X account suffered a compromise on January 9. An unauthorised party obtained control of the SEC cell phone number associated with the account in an apparent "SIM swap" attack. `Social media`

Data exposure and leaks

Brazilian population's personal data exposed
On January 10, an Elasticsearch cluster containing personal data of over 223 million Brazilians, was found publicly accessible online, potentially exposing the entire population to identity theft and cybercrimes. The leaked information included personal and taxpayer data. `Citizens`

Hacker alleges to have stolen a Malaysian customer database with nearly 20 million user data

On January 24, a user in a forum claimed a data leak containing nearly 200 million entries with data from nearly 20 million effective users from a Malaysian telecommunications company. The company has responded by saying they received a ransom note but that the data is dated. `Telecommunications`

Leak of 26 billion records: Dropbox, LinkedIn, Twitter named

On January 22, security researchers announced they have discovered a supermassive leak. It contains data from numerous previous breaches, comprising of 12 TB of information, spanning over 26 billion records. The leak, which contains LinkedIn, Twitter, Weibo, Tencent, and other platforms' user data, is almost certainly the largest ever discovered. `Social media`

Have I Been Pwned integrates 71 million stolen e-mail addresses from Naz.API dataset

The Have I Been Pwned service has added nearly 71 million e-mail addresses from the Naz.API dataset, which consists of stolen credentials, to its data breach notification platform. This dataset contains over 1 billion lines of stolen credentials gathered from sources like credential stuffing lists and malware logs. It has been linked to security issues such as Doxxing and SIM-swapping attacks. `Credentials`

Trello API abused to link e-mail addresses to 15 million accounts

In January, the Trello API was exploited to connect e-mail addresses with 15 million user accounts. Trello is an online project management tool owned by Atlassian. This unauthorised access to e-mail information raised significant privacy and security concerns. `Technology`

iPhone apps abuse iOS push notifications to collect user data

According to a mobile researcher named Mysk, numerous iOS apps are using background processes triggered by push notifications to collect user data about devices, potentially allowing the creation of fingerprinting profiles used for tracking. The researcher claims these apps bypass Apple's background app activity restrictions and constitute a privacy risk for iPhone users. `Mobile phone`

Information operations

China disinformation campaigns targeting Taiwan's election

In the lead-up to the January 13 presidential election in Taiwan, China launched a substantial volume of cyberattacks, according to Google-owned cyber intelligence firm Mandiant. These attacks, which include phishing campaigns, and malware delivery, are focused on spreading disinformation and degrading Taiwan's institutions rather than stealing data, marking a departure from China's usual cyber tactics. `Elections`

Disruption

Global fintech firm EquiLend went offline after cyberattack

On January 22, EquiLend, a global financial technology firm in New York, experienced a cyberattack. Some systems were taken offline, and unauthorised network access was detected. The company has not disclosed if any company or customer data was compromised during the incident. `Fintech`

Significant vulnerabilities

Vulnerability in Wordpress Google Fonts Plugin

On January 2, 2024, an unauthenticated Stored Cross-Site Scripting (XSS) and directory deletion

vulnerability has been discovered in the “OMGF | GDPR/DSGVO Compliant, Faster Google Fonts. Easy.” plugin for WordPress. This vulnerability, identified as “CVE-2023-6600” (CVSS score of 8.6), may allow unauthenticated attackers to update the plugin’s settings and inject malicious scripts into affected sites. This vulnerability could affect sites that have the OMGF plugin installed and configured, which is estimated to be over 300,000 sites. See CERT-EU’s SA 2024-001.

Critical Vulnerability in Ivanti Endpoint Management Software
On January 4th, 2024, a critical remote code execution (RCE) vulnerability was fixed in Ivanti’s Endpoint Management software (EPM). This vulnerability, tracked as “CVE-2023-39336” (CVSS score : 9.6), allows unauthenticated attackers to hijack enrolled devices or the core server. Ivanti EPM is used to manage client devices across various platforms, including Windows, macOS, Chrome OS, and IoT operating systems. The vulnerability affects all supported versions of Ivanti EPM and has been resolved in version 2022 Service Update 5. The editor also states that no evidence of active exploitation was currently found. See CERT-EU’s SA 2024-002.

Critical Vulnerability in Apache OFBiz
On December 26, 2023, the Apache OFBiz project released an update addressing a critical vulnerability in Apache OFBiz. The vulnerability allows attackers to bypass authentication, which could lead to remote code execution (RCE). See CERT-EU’s SA 2024-003.

Critical Vulnerabilities in Ivanti Connect Secure
On January 10, 2024, Ivanti has released an advisory about two critical vulnerabilities in Ivanti Connect Secure (ICS) and Policy Secure gateways. These vulnerabilities, identified as CVE-2023-46805 and CVE-2024-21887, have been exploited in the wild and can allow remote attackers to execute arbitrary commands on targeted gateways. See CERT-EU’s SA 2024-004.

Critical Vulnerability in Cisco Unity Connection
On January 10, 2024, Cisco disclosed a critical vulnerability in its Unity Connection product. This vulnerability, tracked as “CVE-2024-20272” with a CVSS score of 7.3, could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. Currently, Cisco has no evidence of public proof of concept exploits for this vulnerability or active exploitation in the wild. See CERT-EU’s SA 2024-005.

High Vulnerability in FortiOS & FortiProxy
On January 9, 2024, Fortinet disclosed a high vulnerability in FortiOS & FortiProxy. This vulnerability, tracked as “CVE-2023-44250” and with a CVSS score of 8.3, could allow an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests. See CERT-EU’s SA 2024-006.

Critical Vulnerabilities in GitLab
On January 11, 2024, GitLab released a security advisory addressing several vulnerabilities, including critical ones that, if exploited, could lead to account takeover, or slack command execution. See CERT-EU’s SA 2024-007.

Critical Vulnerabilities in Junos OS
On January 10, 2024, Juniper released a security advisory addressing a critical vulnerability that, if exploited, could lead to a Denial of Service (DoS), or Remote Code Execution (RCE). While Juniper SIRT is not aware of any malicious exploitation of this vulnerability, it is recommended upgrading as soon as possible. See CERT-EU’s SA 2024-008.

Critical and High Vulnerabilities in Atlassian Products
On January 16, 2024, Atlassian released a security advisory addressing a critical vulnerability in Confluence Data Center and Confluence Server that, if exploited, could lead to Remote Code Execution (RCE) on the affected server. The editor also released a security advisory addressing 28

high-severity vulnerabilities which have been fixed in new versions of Atlassian products. See CERT-EU's SA 2024-009.

Vulnerabilities in Netscaler ADS and Netscaler Gateway
On January 16, 2024, Citrix released a security advisory addressing two vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway, specifically CVE-2023-6548 and CVE-2023-6549. These vulnerabilities have been actively exploited and require urgent patching. See CERT-EU's SA 2024-010.

Vulnerability in Wordpress POST SMTP Mailer Plugin
On January 10, 2024, an authorisation bypass vulnerability has been discovered in the "POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP" plugin for WordPress. This vulnerability, identified as CVE-2023-6875 (CVSS score of 9.8), may allow an unauthenticated attacker to reset the API key used to authenticate to the mailer and view logs, including password reset e-mails on WordPress sites that use this plugin. See CERT-EU's SA 2024-11.

Vulnerability in Chrome
On January 16, 2024, Google has released an advisory addressing a zero-day vulnerability identified as CVE-2024-0519, which affects the V8 engine in Google Chromium. This vulnerability allows for out-of-bounds memory access, potentially leading to heap corruption through a crafted HTML page. It has been reported that this vulnerability is being actively exploited. See CERT-EU's SA 2024-12.

Zero-Day Vulnerability in Apple Products
On January 22, 20024, Apple issued updates for a zero-day vulnerability identified as CVE-2024-23222. This vulnerability affects iOS, iPadOS, macOS and tvOS devices and is currently being exploited in the wild. The updates also contain fixes for other vulnerabilities affecting Apple products. It is recommended updating as soon as possible. See CERT-EU's SA 2024-13.

Critical Remote Code Execution Vulnerability in Jenkins
On January 24, 2024, Jenkins issued fixes for several vulnerabilities, including CVE-2024-23897, a critical vulnerability that could allow an attacker to achieve remote code execution. The advisory published provides detailed information on various attack scenarios, exploitation pathways, descriptions of the fixes, and potential workarounds for those unable to immediately apply the security updates. Multiple proof-of-concept (PoC) exploits for CVE-2024-23897 are now available. See CERT-EU's SA 2024-14.

Remote Code Execution Vulnerability in Cisco Products
On January 24, 2024, Cisco disclosed a critical vulnerability in multiple the Unified Communications and Contact Center Solutions products. This vulnerability, tracked as CVE-2024-20253 with a CVSS score of 9.9, could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. Currently, Cisco has no evidence of public proof of concept exploits for this vulnerability or active exploitation in the wild. See CERT-EU's SA 2024-15.

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories/`

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.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and it's clients.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
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.