10 years CERT-EU

Cyber Brief (October 2024)

November 4, 2024 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 530 open source reports for this Cyber Brief[1].
- Relating to **cyber policy and law enforcement**, in Europe, Ireland fined LinkedIn for GDPR breaches, Europol led law enforcement action against LockBit and Moldova blocked certain Russian websites ahead of its election. Elsewhere, Japan convicted a criminal who exploited AI to generate ransomware code, Turkey and Russia blocked Discord for failing to hand over requested data, Microsoft disrupted Star Blizzard infrastructure, and Google removed Kaspersky's Android security apps from the Google Play Store.
- On the **cyberespionage** front, in Europe, Russia-linked APT29 conducted a large scale information gathering campaign spoofing trusted software suppliers to deliver malicious RDP files. Additionally, a state actor was reportedly behind a data breach at the Dutch Police, North Korea-linked actors breached a German defence contractor, and GoldenJackal reportedly targeted an embassy in Belarus. Elsewhere, China-nexus threat actors reportedly targeted phones used by former President Donald Trump and his team, and the US warned of APT29 targeting vulnerable Zimbra and TeamCity servers globally.
- Relating to **cybercrime**, in Europe, the most active ransomware operations were lockbit3 and ransomhub, while the most targeted sectors were technology, manufacturing, education, construction & engineering, and healthcare.
- Relating to **information operations**, in Europe, Russia-linked threat actors targeted Moldovan entities with disinformation ahead of the elections, in the US intelligence agencies and Microsoft warned of and exposed Russian, Chinese and Iranian attempts at interference with the US Presidential elections.
- As regards **data exposure and leaks** incidents, in Europe, a French Internet Service Provider and an Italian governmental database suffered unauthorised access to some of the data they process.
- On the **hacktivism** front, in Europe, pro-Palestine and pro-Russia supposed hacktivists claimed several DDoS attacks against governmental entities, elsewhere, the US indicted two Sudanese individuals for operating Anonymous Sudan.

- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in October 2024.

Europe

Cyber policy and law enforcement

Dutch Police dismantles Redline and Meta malware operations in Operation Magnus
On October 28, Dutch Police, in collaboration with other law enforcement agencies, dismantled the infrastructure supporting Redline and Meta infostealer malware through Operation Magnus. Authorities now hold user data, credentials, and the malware's source code, enabling tracking and prosecution of users. `dismantle`

Irish Data Protection Commission fines LinkedIn EUR 310 million for GDPR breaches
On October 24, Ireland's Data Protection Commission fined LinkedIn EUR 310 million for failing to properly inform users about how their data was used for behavioural analysis and targeted advertising, violating the GDPR. The fine resulted from a 2018 complaint by French digital rights group La Quadrature du Net. `fine`

Moldova blocks Russian websites ahead of elections
On October 3, Moldova's Information and Security Service ordered the blocking of additional pro-Russia and Russia-hosted websites, including Dzen, Rutube, and Yandex, ahead of the country's presidential election later in October. `election` `moldova`

Global operation leads to arrest of four suspects linked to LockBit ransomware group
On October 1, Europol reported that law enforcement from 12 countries arrested four individuals linked to the LockBit ransomware group, including a developer, a bulletproof hosting administrator, and two others involved in the group's activities. These arrests, part of Operation Cronos, also resulted in the seizure of LockBit infrastructure servers. `arrests` `seizure`

Cyberespionage

UAT-5647 targeted Ukrainian and Polish entities
On October 17, Cisco reported that since late 2023, the Russian-speaking group UAT-5647 targeted Ukrainian and Polish entities with updated RomCom malware variants. This campaign utilised advanced malware families such as RustClaw, MeltingClaw, DustyHammock, and ShadyHammock for espionage and ransomware deployment, focusing on long-term access and data exfiltration. `russia`

GoldenJackal targeted government networks with air-gapped espionage
On October 7, ESET reported that GoldenJackal, a cyberespionage group, has been targeting government and diplomatic entities with custom toolsets since 2019. Their attacks focused on breaching air-gapped systems. GoldenJackal used highly modular malware for espionage and targeted an embassy in Belarus and other high-profile, isolated networks. `diplomacy` `public administration`

North Korea-linked hackers breached German missile manufacturer Diehl Defence
On September 30, Der Spiegel reported that North Korea-linked Kimsuky breached a German missile manufacturer. The attackers used a phishing campaign involving fake job offers and malicious PDFs. The breach highlights the group's focus on strategic intelligence. `defence` `north korea`

State actor likely behind data breach at Dutch Police
On September 27, the Dutch Minister of Justice and Security informed Parliament about a police account hack compromising work-related contact details of approximately 65,000 officers. The breach did not include investigative data.

Cybercrime

North Korea-linked threat group Andariel collaborates with Play ransomware operators
On October 30, Palo Alto's Unit 42 reported that North Korean APT group Andariel was linked to the Play ransomware operation, likely as an affiliate or initial access broker. Andariel gained access to a targeted network in May 2024, maintaining persistence until deploying Play ransomware in September. Indicators like shared accounts and tools suggest collaboration, marking North Korea's first observed connection with a ransomware group, signaling increased involvement in ransomware operations. `north korea`

Strela Stealer targets European users with stealthy WebDAV techniques
On October 29, Cyble reported on a Strela Stealer phishing campaign, disguised as an invoice e-mail and targeting German and Spanish users. Using obfuscated JavaScript in ZIP attachments, the malware downloaded a malicious DLL via WebDAV, bypassing disk storage to avoid detection. Strela Stealer captured e-mail credentials and system data, enabling attackers to conduct further exploits. `info stealer`

Kremlin-backed cybercrime actors target UK ambulance services and Ministry of Defence
On October 11, The i Newspaper reported Kremlin-backed threat actors targeted UK Ambulance Services and the Ministry of Defence, accessing sensitive communication details over the past year. This “Cyber Wagner” campaign reflects Russia’s hybrid warfare strategy, posing risks to emergency response capabilities and public health safety. MI5 Director Ken McCallum emphasized Russia’s increased reliance on cyber tactics in its ongoing aggression. `russia` `crtical infrastructure`

Information operations

Russia-linked disinformation campaign impersonating European governmental entities targets political and academic entities in Moldova
Since early August a Russia-linked threat actor targeted Moldovan entities with disinformation while impersonating European governmental entities. The campaign targeted government officials and the academic sector with PDF documents and spearphishing e-mails, disseminated through fake domains registered by the threat actor. `election` `moldova` `russia`

Data exposure and leaks

Italian data breach exposed politicians' personal data
On October 29, Italian prosecutors revealed a data breach allegedly led by an IT consultant, who, with a remote team, accessed government databases, including sensitive data of politicians. Four suspects are under house arrest, with investigations ongoing into the extent of state involvement. `insider threat`

France's second largest ISP confirmed data breach impacting 19.2 million customers
France's second-largest ISP confirmed a data breach affecting 19.2 million customers, following claims of stolen data being auctioned online since October 21. The attackers accessed a management tool, exposing personal information but not passwords or payment card data.

IBANs of Freebox subscribers were among the stolen data, though the company asserts these alone cannot authorise direct debit. The company filed a complaint and notified French authorities. `telecommunications`

Hacktivism

Pro-Palestine supposed hacktivists targeted Cyprus' critical infrastructure in coordinated cyberattacks
On October 21, websites of Cyprus' critical infrastructure faced a series of DDoS attacks by pro-Palestine groups. The hacktivist threat actors cited Cyprus' support for Israel as narrative. Most attacks were DDoS, though some claimed data theft. Authorities confirmed no major impact, urging vigilance amid ongoing threats. `cyprus` `critical infrastructure`

Pro-Russia supposed hacktivist NoName targeted CCB Belgium and several ports in the country
Between October 8 and 10, the pro-Russia supposed hacktivist group NoName claimed responsibility for DDoS attacks on Belgium's Centre for Cybersecurity (CCB) and several ports. The attacks followed Belgium's recent announcement of donating Caesar guns to Ukraine. `cybersecurity` `russia` `transport`

World

Cyber policy and law enforcement

Canada released its Cyber Security Readiness Goals for critical systems
On October 29, Canada's Cyber Centre introduced voluntary Cyber Security Readiness Goals to strengthen cyber resilience in critical infrastructure sectors. The guidelines feature 36 security practices across six pillars and align with international standards. Updated regularly, this resource aims to address growing cyber threats, with a strong focus on Canada's energy sector. `critical infrastructure`

Man sentenced in Japan's first AI-generated malware case
On October 28, a Tokyo court convicted a citizen for creating malware using generative AI, sentencing him to three years imprisonment, suspended for four years. The citizen exploited AI to generate ransomware code, was motivated by financial gain. The judge considered his remorse, opting for a suspended sentence, marking Japan's first such case involving generative AI misuse for malware. `artificial intelligence`

US charges tech companies for misleading investors about SolarWinds breaches
On October 22, the US government charged four companies for downplaying the impact of cybersecurity incidents linked to the 2020 SolarWinds hack. Each company allegedly provided misleading disclosures about the breaches, with fines ranging from 990,000 to 4 million US dollars. The findings revealed that the companies minimised the severity of the incidents, potentially leaving investors uninformed about the true risks. `united states`

US indicted two Sudanese brothers for operating Anonymous Sudan DDoS group
On October 16, the US Department of Justice unsealed an indictment against two Sudanese brothers for operating the supposed hacktivist group Anonymous Sudan, associated to over 35,000 DDoS attacks. The group, active since 2023, targeted major tech companies, government agencies and healthcare organisations, and its infrastructure was seized by US authorities in March 2024, disrupting their DDoS operations. `indictment` `russia` `united states`

US and Microsoft disrupted Russia-linked Callisto spearphishing infrastructure
On October 3, the US Department of Justice announced the seizure of 41 internet domains used by Russian threat actors and their proxies for spearphishing, coordinated with Microsoft's civil action to restrain 66 domains. The domains were linked to the Callisto Group targeting US government and private sector entities to steal sensitive information. `russia` `seizure` `united states`

US District Court ordered Microsoft to seize Star Blizzard infrastructure
On October 3, Microsoft reported that its Digital Crimes Unit disrupted Star Blizzard's technical infrastructure, a Russian nation-state actor. The statement coincided with the unsealing by the United States District Court for the District of Columbia of a civil action brought by Microsoft, including its order authorising Microsoft to seize 66 unique domains used by Star Blizzard in cyberattacks. `russia` `take down` `united states`

Kaspersky's Android security app removed from Google Play Store
In the beginning of October, Google removed Kaspersky's Android security apps from the Google Play Store and disabled the Russian company's developer accounts. Google's decision followed the US Department of Commerce's Bureau of Industry and Security announcement of a variety of restrictions on Kaspersky. `russia` `united states`

Turkey and Russia blocked Discord after platform refuses to share user data amid criminal activity concerns
On October 9, Turkey blocked access to Discord following a court decision, after the platform refused to share requested user data with authorities. The block comes amid suspicions of criminal activity, including child abuse, on the platform. Turkey's Information Technologies Authority confirmed the ban. Russia also blocked Discord for non-compliance with local laws. `ban` `russia` `china`

Evil Corp faced new sanctions and BitPaymer ransomware charges
On October 1, the US Treasury's Office of Foreign Assets Control sanctioned seven individuals and two entities linked to the Evil Corp cybercrime syndicate, while also indicting an individual for BitPaymer ransomware attacks in the US. The sanctions, coordinated with the UK and Australia, freeze assets and prohibit transactions, further restricting ransomware payments to Evil Corp without approval to avoid violating sanctions. `sanctions`

China expanded its regulation on generative AI
As of January 1, 2025, an expanded regulatory framework for generative AI will enter into force in China. The framework will establish measures such as that Chinese data should be processed in local data-processing centres. The regulations aim to supposed China in asserting greater control over data sovereignty and digital infrastructure. `artificial intelligence` `china`

Cyberespionage

China-nexus threat actors target phones of Trump and Vance in campaign-related cyberattack
On October 25, the New York Times reported that China-nexus threat actors targeted phones used by former President Donald Trump and Senator JD Vance, aiming to access data about their communications. The FBI and CISA attributed the attack to Salt Typhoon. The infiltration, affecting both Republican and Democrat campaign members, highlights national security risks amid the upcoming 2024 election. `china` `election` `united states`

The FBI and CISA investigated unauthorised access to commercial telecommunications infrastructure by Chinese threat actors
On October 25, the FBI and CISA disclosed that Chinese threat actors breached US telecom providers, targeting communications infrastructure for espionage. They alerted affected

companies and advised other potential targets to reinforce cyber defences. china telecommunications united states

China-linked cyber actors create global botnet using compromised IoT devices
On September 18, the US FBI and NSA publicly reported that China-linked cyber actors compromised over 260,000 internet-connected devices globally, creating a botnet for malicious activities like DDoS attacks. This botnet, managed by the China-based Integrity Technology Group, uses the Mirai malware to target IoT devices, with affected devices found across North America, Europe, and other regions, prompting network defenders to take immediate security measures. china

OpenAI confirmed threat actors' use of ChatGPT to enhance malware and phishing attacks
On October 9, OpenAI confirmed that malicious actors are using ChatGPT for various cyber operations, including writing malware, spreading misinformation, and conducting phishing attacks. Among the cases, Chinese and Iranian threat actors exploited the AI for tasks such as vulnerability research, scripting, and post-compromise activities, enhancing their cyberattack capabilities. china russia technology

APT29 conducted spearphishing campaign using RDP file attachements
On October 22, Microsoft reported on a spearphishing campaign linked to APT29 targeting thousands across government, academia, and NGOs. The attackers used signed Remote Desktop Protocol (RDP) files to establish a connection from victims' devices to their server, allowing access to system resources like files, drives, and peripherals. This use of RDP files highlights a targeted method for information gathering. russia social engineering supply-chain compromise

US, UK warn of Russian APT29 hackers targeting Zimbra, TeamCity servers
On October 10, US and UK cyber agencies warned of Russian APT29 hackers targeting vulnerable Zimbra and TeamCity servers globally. Exploiting CVE-2022-27924 and CVE-2023-42793, these attacks aimed at gaining access to unpatched systems, threatening government and private organisations. Network defenders are urged to apply security patches to block these ongoing intrusions, which have targeted various sectors worldwide. APT29 is linked to Russia's Foreign Intelligence Service (SVR). russia

North Korean IT workers extorted employers after infiltrating Western companies
On October 16, Secureworks reported that North Korean IT workers infiltrated Western companies, stole sensitive data, and demanded a ransom to prevent its exposure. Using false identities, VPNs, and AI tools to conceal their real location, these workers posed as contractors, while working for North Korea's government to fund weapons programmes, with some incidents involving data theft immediately following employment. north korea

Cybercrime

Cloud credentials exposed in operation targeting Git config files
On October 30, Sysdig's Threat Research Team uncovered EmeraldWhale, a global operation targeting misconfigured Git config files, resulting in the theft of over 15.000 cloud credentials from 10.000 private repositories. Exploiting exposed files on misconfigured servers, attackers extracted valuable credentials for resale, mainly for phishing. misconfigurations

North Korea-linked Jumpy Pisces partners with Play ransomware
On October 30, Unit 42 linked North Korea's Jumpy Pisces group to a ransomware incident involving the Play ransomware group, also known as Fiddling Scorpius. This marks the first collaboration between Jumpy Pisces and a ransomware group. north korea ransomware

ReliaQuest exposed Black Basta's new social engineering tactics via Microsoft Teams and QR codes

On October 25, cybersecurity company ReliaQuest uncovered that Black Basta uses involving Microsoft Teams chats and QR codes. Black Basta targeted users through spam e-mails, posing as help desk agents in Teams to convince victims to install remote monitoring tools. This campaign aims to facilitate ransomware deployment, with attackers intensifying methods and expanding scope, especially within diverse sectors. `social engineering`

Perfctl malware targets millions of Linux servers putting thousands at risk

On October 3, Aquasec reported that Perfctl malware has targeted millions of Linux servers over the past four years by exploiting over 20,000 misconfigurations. This malware employs rootkits, TOR for communication, and privilege escalation techniques, primarily to run cryptominers and proxy-jacking software, and evades detection by stopping noisy activities when a user logs in. `technology`

Data exposure and leaks

Change Healthcare breach impacted 100 million individuals

On October 22, Change Healthcare reported that a February ransomware attack exposed personal and healthcare data of approximately 100 million individuals. The breach, linked to BlackCat ransomware, compromised data like health records, billing information, and social security numbers. `health` `united states`

Cisco investigated potential data breach following alleged sale of stolen information on hacking forum

On October 14, Cisco confirmed that it was investigating a potential data breach after a threat actor named IntelBroker claimed to have stolen a large amount of sensitive information and began selling it on a hacking forum. The allegedly compromised data includes source code, credentials, certificates, customer documents, and various internal projects. `supply-chain attack` `technology`

Internet Archive data breach exposes authentication data of 31 million users

On October 8, Internet Archive suffered a data breach, exposing authentication data for 31 million users. The stolen database contains e-mails, usernames, and bcrypt-hashed passwords. The breach, discovered after the hacker displayed a JavaScript alert on the website, reportedly included a SQL file with the compromised data.

Rackspace data breach exposes limited customer information via ScienceLogic zero-day

On October 1, Rackspace reported they experienced a data breach exposing limited customer monitoring data after threat actors exploited a zero-day vulnerability in a third-party utility used by the ScienceLogic SL1 platform. ScienceLogic quickly developed and distributed a patch to all affected customers, while Rackspace assured that no customer configurations or hosted data were accessed, and all impacted customers have been notified. `supply-chain attack` `technology`

Information operations

US intelligence agencies warn about foreign interference with elections

On October 25, the Office of the Director of National Intelligence warned about foreign interference with the upcoming US presidential elections. The declassified report states that Russia, Iran and China will likely focus on information operations even after the elections. The outcome of the information operations will likely include claims of election fraud. election united states

Chinese influence campaign targeted US Republican candidates ahead of elections
On October 23, Microsoft reported that since July 2024, the Chinese influence group Taizi Flood aka Spamouflage targeted down-ballot US Republican candidates critical of China. The campaign criticised politicians like Barry Moore, Marco Rubio, Marsha Blackburn, and Michael McCaul, often using antisemitic language and baseless accusations of corruption or insider trading. These attacks, amplified by online assets, aimed to support opposing candidates but gained minimal authentic engagement. china election united states

Iranian cyber groups escalatec US election interference efforts
On October 23, Microsoft reported that Iranian cyber group Bushnell's Men has urged Americans to boycott US elections and promoted anti-Israel protests on US campuses, using social media and Telegram. Microsoft discovered Iranian-led cyber reconnaissance of US swing state election sites by Cotton Sandstorm and targeted disinformation campaigns from Storm-2035. Iran's efforts, including account hacks and media manipulation, are expected to intensify closer to the 2024 election, prompting warnings from the FBI and CISA. election iran united states

Russian disinformation targeted Kamala Harris with deepfakes and staged videos
On October 23, Microsoft reported that Russian actors produced a deepfake video of Kamala Harris in September, falsely depicting her making offensive remarks about Trump, to incite public anger. Russian influence group Storm-1516 also staged misleading videos involving Harris and Tim Walz, targeting Western audiences. Another group, Storm-1679, spoofed credible news outlets to spread misinformation about Harris on X, while the US government issued warnings on Russia's influence efforts, highlighting coordinated disinformation campaigns. election russia united states

Disruption

Global internet disruptions rise in Q3 2024 amid disasters and shutdowns
On October 29, Cloudflare's Q3 report detailed widespread internet disruptions caused by government-imposed shutdowns, power outages, and infrastructure damage from natural disasters. Key incidents included exam-related blackouts in Iraq, Syria, and Bangladesh, as well as storm-induced outages in the Caribbean and Africa. The report stresses the need for resilient power and telecom infrastructure to maintain global connectivity. telecommunications

US waster water company disconnects some of its systems in response to cyberattack
On October 3, American Water Works Company Inc filed a public report to the US Securities and Exchange Commission in which they acknowledged a cyberattack. The company reported that it disconnected or deactivated certain of its systems and stated that it believes that none of its water or wastewater facilities or operations had been negatively impacted by the incident. critical infrastructure

Iran hit by major cyberattacks targeting government and nuclear facilities amid regional tensions
According to a former secretary of Iran's Supreme Council for Cyberspace, Iran faced significant cyberattacks on October 11, targeting government branches and nuclear facilities. The attacks disrupted infrastructure, affected the judiciary, legislature, and executive branches, and compromised sectors like transportation and fuel distribution. These events followed Israel's response to Iran's October 1 missile strike, escalating tensions in the region. energy iran public administration transport

Hacktivism

Pro-Ukraine supposed hacktivists DDoS Russian TV broadcaster
On October 7, Sudo rm -RF, a pro-Ukraine supposed hacktivist, claimed a DDoS attack against a Russian TV broadcast company. The DDoS coincided with the birthday of the Russian President.

`russia`

Significant vulnerabilities

QNAP NAS Zero-Day Vulnerabilities On October 29 and 30, 2024, QNAP released patches for two critical zero-day vulnerabilities, CVE-2024-50387 and CVE-2024-50388, affecting NAS devices. These vulnerabilities allow remote attackers to gain root access and execute arbitrary commands on compromised devices. See CERT-EU's SA 2024-115.

Multiple Critical CISCO Vulnerabilities On October 25, a security advisory was issued for a set of critical vulnerabilities affecting Cisco Adaptive Security Appliance (ASA) Software, Cisco Firepower Threat Defense (FTD) Software, Cisco Secure Firewall Management Center (FMC) Software, and Cisco Nexus Dashboard Fabric Controller (NDFC). See CERT-EU's SA 2024-114.

Critical 0-day Vulnerability in Fortinet FortiManager On October 24, a security advisory was issued for a critical 0-day vulnerability in a FortiManager product. If exploited, a remote unauthenticated attacker could execute arbitrary code or commands on the affected device. See CERT-EU's SA 2024-113.

Critical Vulnerability in Kubernetes On October 17, a security advisory was issued for a critical vulnerability affecting the Kubernetes Image Builder project. It is recommended updating the Kubernetes Image Builder, and redeploying or mitigating Virtual Machines created by the vulnerable Kubernetes Image Builder. See CERT-EU's SA 2024-112.

Multiple Vulnerabilities in Splunk Enterprise and Splunk Cloud On October 16, a security advisory was issued for multiple high and medium severity vulnerabilities affecting Splunk Enterprise and Splunk Cloud. These vulnerabilities could lead to arbitrary file write to Windows system root directory, access to potentially restricted data and remote code execution. See CERT-EU's SA 2024-111.

Critical Vulnerability in Ivanti Products On October 16, a security advisory was issued for a critical vulnerability in Ivanti Connect Secure and Ivanti Policy Secure. See CERT-EU's SA 2024-110.

Critical vulnerabilities in Gitlab On October 11, a security advisory was issued for several critical vulnerabilities in GitLab EE/CE affecting versions from 8.16 to 17.4.1. See CERT-EU's SA 2024-109.

Palo Alto Critical Vulnerabilities On October 11, a security advisory was issued for multiple critical vulnerabilities in its Expedition tool that can lead to unauthorised access to firewall credentials and sensitive data, including usernames, passwords, and API keys. The vulnerabilities allow attackers to execute arbitrary commands, read or write files, and exploit SQL injection flaws. Successful exploitation could result in a full takeover of affected systems. See CERT-EU's SA 2024-108.

Critical Vulnerability in Firefox On October 11, a security advisory was issued for a security advisory regarding a critical use-after-free vulnerability (CVE-2024-9680) in Mozilla Firefox. See CERT-EU's SA 2024-107.

Multiple Critical Vulnerabilities in Microsoft Products On October 9, a security advisory was issued for Microsoft vulnerabilities including five zero-day vulnerabilities and three critical vulnerabilities. See CERT-EU's SA 2024-106.

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 its 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.