Cyber Security Brief (September 2023)

October 3, 2023 - Version: 1.0

TLP:CLEAR

Disclosure is not limited.

TLP:CLEAR information may be distributed freely.

Executive summary

- We analysed 254 open source reports for this Cyber Security Brief[1].
- Relating to **cyber policy and law enforcement**, Polish authorities probed OpenAI for GDPR violations, France has approved a digital law targeting online misconduct, and the UK and US have sanctioned 11 Russians tied to ransomware operations. In the rest of the world, Pakistan warned against using Indian AI products and China and neighbours cracked down on an online scam.
- On the **cyberespionage** front, there were cyber attacks against the International Criminal Court and the European Telecommunications Standards Institute, and three new threat actors; two of them were China-linked. Globally, China targeted South Korea, and reportedly targeted the US and Japan via router firmware. China accused US intelligence of cyber attacks.
- Relating to **cybercrime**, ransomware incidents in the UK, including a military supplier and a police department ransomware, exposed sensitive data and the BlackCat ransomware group evolved tactics to target Azure cloud storage. A financial platform suspended transactions after a 200 million US dollar hack. In Europe, for September, the top most active ransomware operations have been RANSOMEDVC, AlphV, LostTrust, NOESCAPE, and Play; the most targeted sectors have been retail, manufacturing, legal and professional services, healthcare, and hospitality.
- Regarding **data exposure and leaks**, a Swedish insurance company was fined for exposing customer data, Microsoft AI researchers accidentally exposed internal data and a digital risk firm leaked billions of records.
- On the **hacktivism** front, in September, in Europe, pro-Russia hacktivist groups, on several occasions targeted countries which support Ukraine, including in large-scale attacks in Latvia and DDoS attacks in Germany, Denmark, Estonia, Norway, Spain, the UK, Canada, and Bulgaria. The group Beregini claimed to have leaked NATO documents.
- In this Cyber Brief we have included several significant vulnerabilities and associated advisories reported in September 2023.

Europe

Cyber policy and law enforcement

Poland investigates OpenAI over GDPR violations *Data protection*
Poland's Personal Data Protection Office (UODO) is investigating a complaint against US-based artificial intelligence company OpenAI, citing misuse of user data and lack of transparency in data processing, which may potentially violate the European Union's General Data Protection Regulation (GDPR). The complainant, Lukasz Olejnik, claimed that OpenAI breached several EU regulations related to data protection, including lawful basis, transparency, fairness, data access, and privacy rights, raising concerns about the company's compliance with EU data-protection regulations.

Digital law project in France *Regulation*
On September 21, a committee of the French National Assembly approved legislation to secure and regulate the digital space, targeting illegal online content and behaviours. The law includes measures like an "anti-scam filter" for search engines, user verification on porn sites, and penalties for cyberbullying and online hate. Concerns exist about the effectiveness of some measures and their compatibility with tools like VPNs.

Sanctions on ransomware operators *Sanctions*
The UK's National Crime Agency, along with US authorities imposed, on September 7, sanctions on eleven Russian nationals linked to the TrickBot and Conti ransomware operations. The sanctions came after leaks of internal communications from these groups led authorities to their crackdown. The sanctions make it illegal for UK and US organisations to conduct financial transactions with these individuals, complicating ransom payments and potentially leading to the downfall or rebranding of these ransomware operations.

Cyberespionage

China-linked Earth Lusca targeting government entities in the Balkans and other regions *Chinese threat actor*
The security company Trend Micro reported that in 2023 they continued to observe activity by Earth Lusca (a.k.a. Aquatic Panda, Charcoal Typhoon), a China-linked threat actor. The threat actor has been active since at least 2021. In 2023 the researchers found, the group was utilising a new backdoor, targeting Linux systems, named SprySOCKS. Targeting of the group focuses primarily on countries in South-east Asia, Central Asia, and the Balkans.

North Korean threat actor breaches Spanish aerospace company *North Korean threat actor*
According to security company ESET, the North Korean Lazarus threat actor exploited a novel 'LightlessCan' backdoor to breach a Spanish aerospace company, luring employees through fake job opportunities on LinkedIn. Upon downloading a malicious file during a faux recruitment process, an employee inadvertently granted the hackers access for cyberespionage.

International Criminal Court discovers cyber attack *Unattributed threat actor*
On September 19, the International Criminal Court (ICC) in The Hague detected a cyber attack on its systems and initiated an investigation with Dutch authorities. The extent of the attack's impact and whether any data was compromised remain undisclosed as the ICC focuses on safeguarding its core operations and enhancing cybersecurity measures.

European Telecommunications Standards Institute breach *Unattributed threat actor*
On September 27, ETSI, the European Telecommunications Standards Institute, announced that it had suffered a cyber incident. An unnamed threat actor exploited a vulnerability in the ETSI portal, an IT system dedicated to its members' work. The threat actor subsequently exfiltrated a list of their online users. Passwords may also have been exposed.

New APT group Sandman targets telecoms in Europe and other countries *Unattributed threat actor*
The security company Sentinel Labs has issued a report about a previously unknown advanced persistent threat (APT) threat actor they are calling Sandman. The group was active in August 2023, targeting telecommunications companies in Western Europe, the Middle East and North Africa, and South Asia.

Threat actor Earth Estries targets government and technology sector *Unattributed threat actor*
Trend Micro published an article on Earth Estries, a newly identified group, active since at least 2020. The group, focused in cyberespionage, targets the government and technology sectors in several countries including in Europe, Germany.

Phishing attacks on Ukrainian military using a drone manual lure *Unattributed threat actor*
The Ukrainian military have been targeted by a phishing campaign named STARK#VORTEX, which uses drone manuals as bait to deliver a Go-based malware toolkit called Merlin. The attack starts with a Microsoft CHM file that contains malicious JavaScript and PowerShell code to fetch an obfuscated binary from a remote server.

Cybercrime

Attack on UK security supplier *Phsysical security*
According to news reports on September 4, a UK-based supplier of high-security fencing for military bases, fell victim to a cyber attack led by the LockBit ransomware operation. The breach, due to an obsolete system used at the company, may have exposed data on some of the UK's military and research sites.

Manchester Police suffer unauthorised access to personal data *Law enforcement*
On September 14, the UK's Greater Manchester Police said that some of its employees' personal data was impacted by a ransomware attack that hit a third-party supplier.

Disruption

German financial agency hit by DDoS *Financial*
Germany's Federal Financial Supervisory Authority (BaFin) experienced a DDoS attack on its website since September 1, forcing the regulatory agency to take defensive measures including disabling its public site. While BaFin has not confirmed who is behind the attack, there was speculation that pro-Russian hacktivists might be responsible due to Germany's support for Ukraine.

cyber attack targeted Bulgarian fact-checking platform *Fact-checking platform*
Factcheck.bg, Bulgaria's leading fact-checking platform, renowned for combating Russian disinformation, was hit by a cyber attack on September 21. It resulted in the deletion of various posts on Factcheck.bg and Facebook, along with content from the Association of European Journalists Bulgaria (AEJ), the platform's manager. The culprits have not been unidentified.

Hacktivism

Attacks on Latvia *Latvia*
Pro-Russia hacktivist groups issued, on September 4, a call for attacks against countries supporting Ukraine. The Latvian CERT issued an advisory on the same day, about large-scale cyber attacks carried out by allegedly Russia-supported hacker groups. The attacks were targeting state, financial, and healthcare institutions in Latvia. The advisory highlighted observed tactics including phishing, website defacement, and potential ransomware attacks, urging institutions to take precautionary measures.

DDoS attacks on German entities in protest of Ukraine defence meeting *Germany*
On September 19, the CyberTriad hacktivist group claimed to have successfully carried out DDoS attacks targeting multiple Berlin-based entities, including public transport, media, and law enforcement, as a protest against Germany's hosting of the Ukraine Defense Contact Group at Ramstein Air Force Base. CyberTriad, which aims to oppose what they view as warmongering foreign policies by Western countries, had previously declared its goals to prevent conflict and promote a world without violence.

NoName DDoS attacks on multiple European entities *Multiple European countries*
The pro-Russia hacktivist group NoName057(16), also known as NoName, has claimed responsibility for launching DDoS attacks against multiple entities in Denmark, Estonia, Germany, Norway, Spain, and the UK. These attacks are purportedly in response to various countries' military support for Ukraine and Estonia's adherence to a recent European Union decision restricting Russian vehicles from entering EU countries. The attacks resulted in several targeted websites becoming inaccessible.

Pro-Russia group targets Canada and Bulgaria *Bulgaria*
Between September 13 and 14, the pro-Russia hacktivist group NoName conducted DDoS attacks on 20 Canadian government-related websites as well as the websites of four entities in Bulgaria, including a port and government sites. NoName declared the attacks to be a response to Canada's support for Ukraine and anger towards certain Canadian laws, as well as retaliation against Bulgaria for lifting a grain import ban from Ukraine and planning to build a NATO base.

Pro-Russia group claims it has NATO documents *European countries*
On September 13 and then on September 23, the pro-Russia hacktivist group Beregini claimed to be in possession of leaked NATO unclassified, but non-publicly available documents, which reportedly contained information on member states and military information passed to Ukraine. The authenticity of the document and the group's claims cannot be confirmed. Beregini has a history of similar activities against Ukraine and its allies since at least 2016.

Information operations

Meta removes Georgia-based network for coordinated inauthentic behavior *Meta*
Meta's Quarterly Adversarial Threat Report revealed the removal of a Georgia-based network consisting of 117 assets linked to the country's Strategic Communications Department, citing coordinated inauthentic behaviour (CIB). The operation used fake accounts to amplify pro-government content and criticise opposition, spending 33.500 US dollar on advertising to broaden its reach.

Data exposure and leaks

Swedish insurance company exposes customer data *Insurance*
The Swedish Authority for Privacy Protection (IMY) fined the insurance company Trygg-Hansa 2,79 million euros after it exposed sensitive data of approximately 650.000 customers on its online portal for over two years. The exposure was due to a flaw that could be exploited by simply modifying the client ID number in a URL sent to customers. Despite being aware of the flaw, Trygg-Hansa failed to address the issue.

World

Cyber policy and law enforcement

US sentences OneCoin co-founder for crypto ponzi scheme *Sentence*
On September 12, the US Department of Justice sentenced the co-founder of the OneCoin cryptocurrency to 20 years in prison. Since 2014, OneCoin conspirators marketed and sold the fraudulent cryptocurrency OneCoin to more than 3,5 million victims, defrauding these individuals of more than 4 billion US dollar, in total.

Pakistan warns against use of Indian-origin AI products *Warning*
The Pakistani federal government is cautioning IT and financial services entities, as well as regulators, against using AI and ICT products originating from India, citing potential threats to critical information systems, including passive monitoring and data-collecting malware. The government has urged ministries to assess these alleged risks and explore native alternatives as AI technologies face increasing scrutiny globally for potential security vulnerabilities.

Coordinated operation to crack down cybercriminals in China *Arrest*
On 5 September, China, Myanmar, Thailand, and Laos conducted a coordinated law enforcement operation to crack down on cybercriminals. 1.200 Chinese nationals allegedly involved in criminal online scams in eastern Shan State have been arrested and extradite.

Cyberespionage

A Chinese state-sponsored group targeted South Korea for years *Chinese threat actor*
A cyberespionage campaign which primarily targets South Korean academic, political, and government organisations, has been linked to Chinese military intelligence. The campaign is motivated by regional geopolitics and is expected to intensify, aiming to support China's diplomatic and business engagements with South Korea, amid rising tensions between China, the US, and its regional allies.

China-linked threat actor backdoors unspecified Cisco router firmware *Chinese threat actor*
On September 27, the US CISA reported on BlackTech activity, a China-linked threat actor. BlackTech was observed targeting routers firmware and exploiting the routers' domain-trust relationships to gain further access to networks and systems, pivoting from international subsidiaries to reach Japanese and US systems, identified as the end targets.

Spyware apps target Uyghur speakers *Chinese threat actor*
On September 8, Kaspersky researchers reported that they had identified Android malware targeting users who speak traditional Chinese, simplified Chinese and Uyghur. The malware was spread via malicious Telegram mods which had been tested by and available on Google Play. Kaspersky dubbed the malicious apps Evil Telegram.

Chinese cyber intrusions in Africa indicate strategy to extend influence *Chinese threat actor*
According to security company Sentinel One, malicious strategic activity has been observed targeting Africa's telecommunication, finance, and government sectors. The activity is attributed to the BackdoorDiplomacy APT and the threat group orchestrating Operation Tainted Love.

Iranian hackers engage in password spray attacks, stealing sensitive data *Iranian threat actor*
Iranian hackers, known as APT33, conducted password spray attacks on thousands of organisations globally since February 2023, stealing sensitive data from some victims in defence, satellite, and pharmaceutical sectors. Microsoft reported that these attacks, which also involved exploiting vulnerabilities and advanced tactics, likely serve Iranian state interests and are more sophisticated than previous APT33 operations.

DPRK-linked actors targeted Russian government *North Korean threat actor*
On September 7, Microsoft Threat Analysis Centre, reported that multiple North Korean threat actors have recently targeted the Russian government and defence industry, likely for intelligence collection, while simultaneously providing material support for Russia in its war on Ukraine.

Nation-state actors breached US aeronautical sector organisation *Unattributed threat actor*
On September 7, US Cyber Command reported that multiple nation-state threat actors had exploited a public-facing Zoho ManageEngine ServiceDesk Plus application to establish persistence, and move laterally through the network of a US organisation in the aeronautical sector.

Redfly compromised Asian national electricity grid for six months *Unattributed threat actor*
Symantec reported that between February 28 and August 3 the Redfly group had compromised an Asian country's national grid with a Shadowpad infection.

Chinese government accuses US intelligence of hacking Huawei servers *US threat actor*
On September 19, China's Ministry of State Security (MSS) accused US intelligence agencies, particularly the NSA's Computer Network Operations team, of conducting cyber attacks, since 2009, against China-based entities, including Huawei. The MSS alleges that US legislation, including the Foreign Intelligence Surveillance Act, allowed American technology companies to install backdoors in equipment, software, and applications to monitor and steal global data. They also accused the US government of exaggerating China's cyber threat and conducting its own cyber attacks against multiple countries, though no evidence was provided to support these claims.

Cybercrime

Nigerian national pleads guilty to business e-mail compromise attacks *Business e-mail compromise*
A 29-year-old Nigerian, extradited from Canada to the US, has pleaded guilty to wire fraud and money laundering. In 2017, while living in South Africa, he collaborated with US individuals to hack into business and employee e-mails. Using these compromised accounts, the group sent e-mails with fake sender addresses to trick businesses into believing they were communicating with trusted partners.

BlackCat ransomware targets Azure Cloud Storage with stolen Microsoft accounts and Sphynx Encryptor *Azure Storage*
The BlackCat ransomware gang has adapted by using stolen Microsoft accounts and a new Sphynx encryptor variant to target and encrypt Azure cloud storage. They gained access to victims' systems, disabled security features, and encrypted both local systems and Azure cloud storage, successfully compromising 39 Azure Storage accounts in the process, highlighting their ongoing sophistication and adaptability in targeting enterprises globally.

Mixin Network suspends operations after 200 million dollar theft *Digital platform*
Mixin Network, a digital asset transaction platform, has halted deposits and withdrawals following a 200 million dollar hack targeting its cloud service provider on September 23. The substantial financial loss has created significant concern among the platform's users.

Data exposure and leaks

Microsoft AI researchers accidentally leak terabytes of sensitive data *Microsoft*
According to Microsoft's Security Response Center and cloud security company Wiz, Microsoft AI researchers accidentally exposed terabytes of internal sensitive data, including passwords and private keys, when publishing an open-source training data storage bucket on GitHub. While no customer data was exposed, the incident highlights the need for additional security checks and safeguards as development teams handle massive amounts of data.

Data breach hits US educational nonprofit affecting schools *Nonprofit*
The National Student Clearinghouse disclosed a data breach affecting 890 US schools, after attackers gained unauthorised access to its MOVEit managed file transfer server on May 30. The issue was reported to the nonprofit by their third-party software provider, Progress Software.

MOVEit: 3,4 million people affected in BORN Ontario data breach *Government*
The Better Outcomes Registry & Network (BORN), funded by the Ontario government, has fallen victim to Clop ransomware's MOVEit hacking campaign, affecting 3,4 million individuals. The threat actors exploited a zero day vulnerability (CVE-2023-34362) in Progress MOVEit Transfer software, compromising critical data related to pregnancy, birth, and childhood in Ontario.

MOVEit: 753.261 people affected in Financial Institution Service Corporation data breach *Finances*
The Financial Institution Service Corporation has fallen victim to Clop ransomware's MOVEit hacking campaign. The threat actors compromised and published critical data related to financial account or credit card numbers (in combination with security code, access code, password or PINs for the accounts).

DarkBeam data leak exposes 3,8 billion records *Digital platform*
DarkBeam, a digital risk protection firm, inadvertently exposed over 3,8 billion records, including user e-mails and passwords, due to an unprotected Elasticsearch and Kibana interface. The data leak poses risks not only to DarkBeam's customers but potentially to others as well.

Disruption

Pro-Iranian hacktivist group targets Israeli Railroads *Cyber Avengers*
The Iranian hacktivist group known as the "Cyber Avengers" has reportedly targeted Israel's railway network, claiming to have attacked the electrical infrastructure. While Israeli Railways denied a cyber attack, the group has a history of cyber attacks against Israeli entities, including an attack on Israel's largest oil refining company in July 2023, according to Mandiant.

Bermuda government IT systems hit by threat actors *Bermuda*
The Government of Bermuda suffered a cyber attack affecting all of its departments' IT systems. The attack has caused disruptions in internet, e-mail, and phone services across all the government. The country's Premier said that the threat actor was sophisticated and that the size, scope, and nature of this incident were significant.

Hacktivism

Indian hacktivists targeted Canadian Dental Clinic site amid diplomatic tensions *Indian Cyber Force*
A group called Indian Cyber Force, claiming to support India, breached a Canadian dental practice's website, leaving pro-India messages. The activity followed allegations by Canadian Prime Minister that India was responsible for the death of a Canadian activist. The hacking incident occurred in the backdrop of diplomatic tensions, where both countries have expelled diplomats but the targeted dental clinic had no political affiliations.

Hacktivists claim breach of Russian software development company *Software development*
On September 22, hacktivist group ThreatSec claimed to have breached and leaked data from a Russian software development company. In a Telegram post, the hacktivists mentioned that they compromised the software developer's change logs, messaging logs, and private files. ThreatSec alleges the software developer creates spyware for the Russian government.

Information operations

Meta stops Chinese and Russian influence campaigns *Social Media*
Meta announced, on September 5, the dismantling of two major covert influence campaigns originating from China and Russia by removing thousands of accounts and pages across its platforms. The Chinese operation, known as Spamouflage, involved 7.704 Facebook accounts, 954 Pages, 15 Groups, and 15 Instagram accounts that distributed spam content and targeted global audiences. Meanwhile, the Russian operation called Doppelganger, previously disrupted in 2022, had focused on creating fake news websites to spread propaganda related to the war in Ukraine, and had now expanded its target countries to include the US and Israel.

Significant vulnerabilities

Zero-Click Vulnerabilities in Apple Operating Systems *iOS*

In an article published on September 7, Citizen Lab uncovered an actively exploited zero-click vulnerability used to deliver NSO Group's Pegasus spyware on an employee of a Washington, DC based civil society organisation. This exploit, named "BLASTPASS" could compromise iPhones running the latest iOS version without user interaction. The exploit involved "PassKit" attachments containing malicious images sent from an attacker iMessage account to the victim. Citizen Lab promptly reported their findings to Apple, who issued two CVEs related to this exploit chain (CVE-2023-41064 and CVE-2023-41061). These vulnerabilities have now been patched in iOS, iPadOS, watchOS and macOS. See CERT-EU's SA 2023-061.

Cisco Remote Access VPN Vulnerability *Cisco Remote Access VPN*

On July 12, Cisco released an advisory to address a vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defence (FTD) software. It could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations or an authenticated, remote attacker to establish a client-less SSL VPN session with an unauthorised user. In addition, Cisco warns that the vulnerability could be actively exploited by ransomware groups to gain initial access to corporate networks. See CERT-EU's SA 2023-062.

Google Chrome Critical Vulnerability *Chrome*

Google has released an emergency security update to address a critical vulnerability found in Chrome. This vulnerability, tracked as CVE-2023-4863, is caused by a WebP heap buffer overflow weakness. It affects Chrome running on Windows, Mac, and Linux systems and has already been exploited in the wild, according to Google. Users are advised to update their Chrome web browser to version 116.0.5845.187 (Mac and Linux) and 116.0.5845.187/.188 (Windows) immediately. See CERT-EU's SA 2023-063.

Microsoft September 2023 Patch Tuesday *Microsoft*

Microsoft has released its September 2023 Patch Tuesday Security Updates, addressing a total of 59 CVEs, including two actively exploited zero-day vulnerabilities. See CERT-EU's SA 2023-064.

Adobe Acrobat and Reader Zero-Day Vulnerability *Adobe Acrobat and Reader*

On September 12, Adobe released a security update that addresses a critical, zero-day vulnerability, which has been exploited in the wild. The vulnerability affects both Windows and MacOS systems and is being tracked as CVE-2023-26369. See CERT-EU's SA 2023-065.

Mozilla Firefox and Thunderbird Zero-Day Vulnerability *Mozilla Firefox and Thunderbird*

On September 12, Mozilla released an emergency security update that addresses a zero-day vulnerability, which has been exploited in the wild. The vulnerability impacts its Firefox web browser and Thunderbird e-mail client and is being tracked as CVE-2023-4863. The issue is being exploited in the wild. See CERT-EU's SA 2023-066.

Critical Flaw in GitLab *Gitlab*

On September 18, GitLab has released security updates to address a critical flaw identified by "CVE-2023-4998" that, if exploited, would allow an attacker to run code, modify data or trigger specific events within the GitLab system. This could result in loss of intellectual property, damaging data leaks, supply chain attacks, and other high-risk scenarios. See CERT-EU's SA 2023-067.

High Severity Vulnerability in Bitbucket Data Center and Server *Bitbucket*
On September 19, Atlassian released a security bulletin addressing several vulnerabilities among which a high severity vulnerability, identified by "CVE-2023-22513", that could allow an authenticated attacker to execute arbitrary code on the server. See CERT-EU's SA 2023-068.

Zero-Day Vulnerabilities in Apple Products *Apple*
On September 21, Apple issued emergency patches for three zero-day bugs, identified by CVE-2023-41992, CVE-2023-41991 and CVE-2023-41993. These vulnerabilities are affecting iOS, iPadOS, and macOS devices and are currently being used in the wild for spyware installation purposes. See CERT-EU's SA 2023-069.

Critical Vulnerabilities in Progress WS_FTP Server Software *Progress software*
On September 27, Progress Software released an advisory announcing multiple vulnerabilities in its enterprise-grade WS_FTP Server secure file transfer software. Two of the vulnerabilities, identified by "CVE-2023-40044" and "CVE-2023-42657", are rated as critical. These flaws expose systems to unauthenticated remote command execution and directory traversal attacks. Immediate patching is strongly advised. See CERT-EU's SA 2023-070.

Cisco Catalyst SD-WAN Manager Vulnerabilities *Cisco Catalyst SD-WAN Manager*
On September 27, Cisco issued a Security Advisory for five new vulnerabilities in their "Catalyst SD-WAN Manager" products, with the most critical flaw allowing unauthenticated remote access to the server. "Cisco Catalyst SD-WAN Manager" for WAN is network management software allowing admins to visualise, deploy, and manage devices on wide area networks (WAN). See CERT-EU's SA 2023-071.

All CERT-EU's Security Advisories are available to the public on CERT-EU's website, `https://www.cert.europa.eu/publications/security-advisories#2023`

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.

TLP	Disclosure	Message
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.