UNICC | Cybersecurity

Cyber Threat Landscape Report 2024

April 2025

TLP: CLEAR

CONTENTS

Executive Summary

Cyberthreats targeting United Nations organizations are increasing in both frequency and severity, and represent a critical risk to the entire UN system. As observed in previous years, UN organizations continue to experience a growing number of cyberattacks initiated by a wide range of adversaries. The analysis and correlation of 2024 data from UNICC Cybersecurity teams' monitoring and incident response activities showed a **35% increase in malicious activities of interest when compared to 2023 data**.

Financially motivated adversaries and information-gathering operations tied to geopolitical events have been observed by UNICC to be the key cyberthreats in the 2024 threat landscape. These malicious activities of interest often reflect the geopolitical situation, where adversaries increasingly target strategically significant data related to the crisis zones.

In 2024, the UNICC Common Secure Cyberthreat Intelligence team observed and tracked more than **90 adversaries**, of which **60 had not been previously observed targeting UN organizations**, and the remaining 30 were already known for targeting UN organizations. These adversaries range from opportunistic individuals to highly sophisticated groups leveraging advanced techniques and capabilities. In 2024, the principal goals of these adversaries included information gathering and financial gain through different targeted fraud schemes or other more sophisticated techniques. These malicious activities of interest were initiated through various attack vectors, by far the most common being **phishing schemes**, followed by the **exploitation of publicly exposed application vulnerabilities**, and the **misuse of stolen credentials/compromised accounts**.

This report consolidates 2024 data from organizations supported by UNICC, offering insights into cyberthreats trends and common risks affecting the UN system. It also provides strategic recommendations to help organizations mitigate evolving cyberthreats. The statistics presented in this report reflect the data gathered by SOC, Incident Response and Threat Intelligence teams with sources including various UN organizations sharing unique and sensitive information. These numbers are not absolute but are based on UNICC's analysis of the available information and provide insight into the current state of cyberthreats targeting the UN system.

As in previous years, the threat landscape provides clear evidence that the UN system continues to be highly exposed to cyberthreats. To effectively address these threats, the efforts of individual organizations will need to form part of a collective and systemic approach. This is where UNICC plays a crucial role in supporting UN organizations, providing common capabilities and services, promoting a community approach to exchange intelligence and developing a coordinated response to common threats from these adversaries.

2024 UNICC Common Secure Conference in Valencia, Spain
Photo: UNICC

Context and Background

The primary objective of the UNICC Cybersecurity teams is to **support United Nations organizations in ensuring service continuity by detecting, preventing and responding to cyberattacks.** Digital and cyber-enabled solutions are central to the United Nations mission and its diverse mandates. United Nations organizations conduct business online and hold a vast amount of information based on their mandates, members, partners, and employees. Any of these assets is an attractive target for adversaries, and organizations can benefit from UNICC's collective defence capabilities against common cyberthreats.

UNICC's 24/7 Common Cybersecurity Operations Centre (CSOC) centralizes detection, triage, and response to cyberattacks. Incidents are assessed for severity with the Computer Security Emergency Response Team (CSIRT) acting to contain and mitigate damage. The Common Secure Cyberthreat Intelligence (CTI) team provides timely and actionable intelligence to help UN organizations prevent, detect, and respond to threats. Through the interaction and cooperation of the teams providing these capabilities, the UNICC Cybersecurity teams have issued hundreds of alerts and intelligence reports, allowing UN entities and the Common Secure community to take preventive measures.

In 2024, the UNICC CSOC, CSIRT and Common Secure Threat Intelligence teams protected 44 UN organizations and monitored over 100,000 active directory accounts and more than 80,000 endpoints globally. Thanks to this visibility, it was possible to monitor and pivot cyberthreat data across different organizations, thus allowing cybersecurity analysts to investigate threats that often target several UN organizations at the same time. This unique perspective and visibility provide UNICC with a unique vantage point into the cyberthreat landscape affecting the UN system.

Throughout 2024, the SOC, CSIRT and the Common Secure team collaborated on a threat-hunting initiative targeting the assets of UN organizations protected by UNICC. This effort enabled UNICC to identify previously undetected threats that had evaded existing security defences, allowing the interception of ongoing cyberattacks.

Malicious activities of interest - Definition

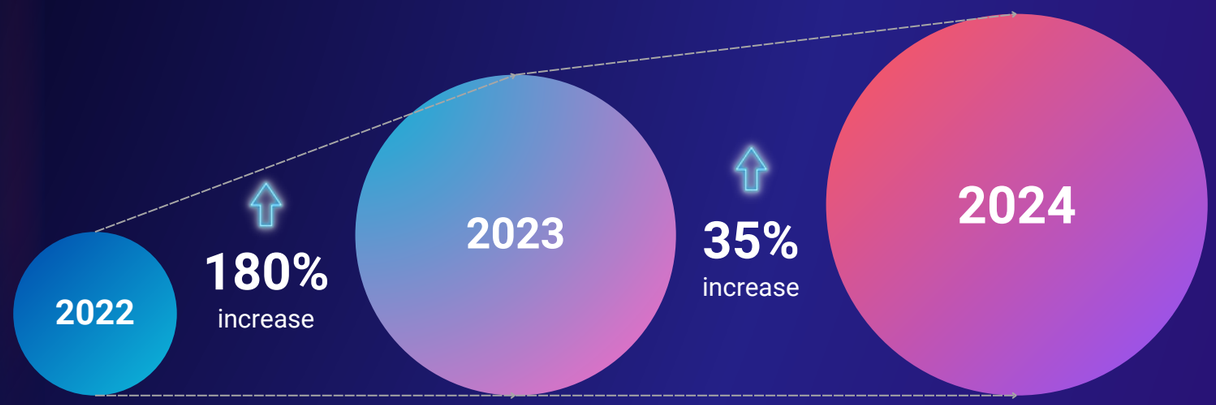
Using data from various sources, the UNICC cybersecurity teams identified numerous malicious activities and incidents affecting UN organizations. UNICC selected a subset of incidents labelled as the "malicious activities of interest"— considered the incidents most relevant for strategic and intelligence purposes. The dataset generated by these activities is used to compile this report and the annual statistics featured in the cyberthreat landscape reports.

To define whether a malicious activity should be classified as "of interest", the Common Secure team has defined an internal taxonomy with a defined rationale to analytically define what is relevant and those that can be excluded from the statistics.

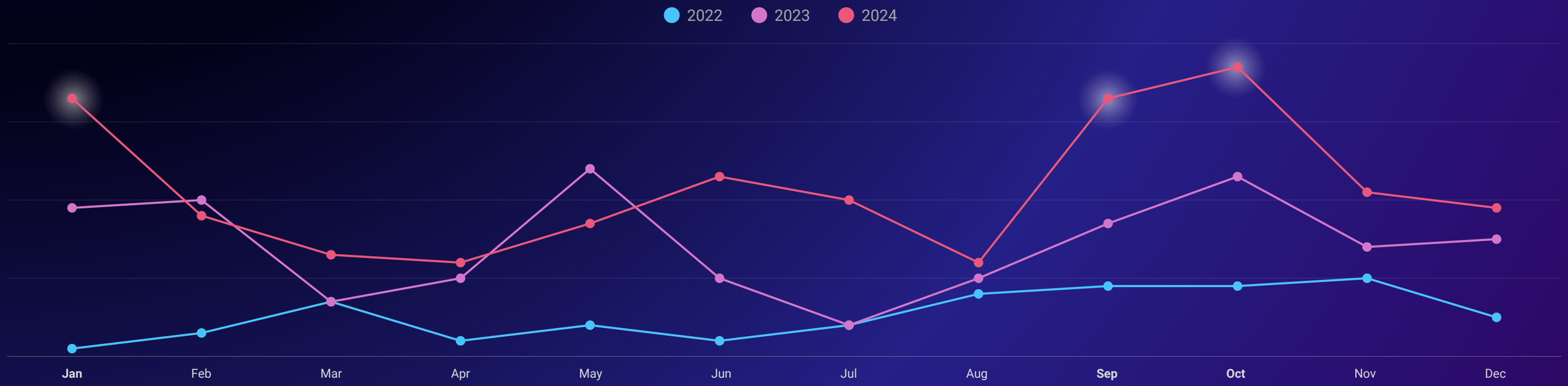
Malicious Activities of Interest - Overview

In 2024, the UNICC CSOC, CSIRT and Common Secure Cyberthreat Intelligence teams observed a 35% increase in the malicious activities of interest compared to 2023 levels. The number of detected malicious activities of interest has never been higher, demonstrating a continuously growing trend with the continuous interest by different adversaries towards the data and infrastructure related to the UN system.

It is notable that over the last three years, a seasonal pattern to the malicious activities of interest has been observed, with activity concentrated mainly in the months of **January, September and October**. Although UN organizations and readers should be vigilant throughout the year, particular attention should be placed on these months.



Growth in malicious activities of interest (2022-2024)



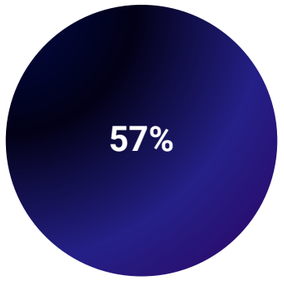
Malicious activities of interest volume over the year (2022-2024)

Initial Attack Vectors

In 2024, the majority of the observed malicious activities of interest were initiated predominantly through phishing schemes, exploiting vulnerabilities in public-facing applications, and the misuse of stolen accounts.

Phishing leads the ranking, and it is used in approximately **57%** of the attacks, so UNICC can confirm the preference of adversaries targeting various UN organizations to use methods that target users and exploit cybersecurity awareness weaknesses as the main attack vector.

The next most common vector in the ranking is the exploitation of vulnerabilities. This is a very effective method as adversaries can detect and exploit the vulnerabilities to access the corporate network via improperly patched systems that are exposed to the internet.



Phishing

In 2024, the UNICC Common Secure Cyberthreat Intelligence team identified various phishing schemes used by multiple threat actors. Some attacks involved malicious domains designed to deceive victims into revealing credentials or personal information. Additionally, phishing emails with domains mimicking UN organizations were observed, aimed at fraud or information gathering. In other cases, users were tricked into downloading malware.

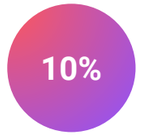
Recommended mitigations:
Effective awareness programmes are fundamental to ensure users are prepared to recognize phishing emails and know how to respond appropriately.

Vulnerability Exploitation

The UNICC CSIRT team analyzed several instances of malicious events to identify the "patient zero" for each case.

In many cases exposed vulnerable systems have been detected as initial attack vector. Attackers exploited known flaws in application code to perform malicious actions, such as data theft or system compromise.

Recommended mitigations:
Regular security patching, a defense in-depth approach and the use of WAF and EDR technologies can help mitigate this attack vector, which is frequently targeted by known adversaries.



Account Take Over
Password Brute Force

Threat actors use techniques such as credential stuffing, password spraying, or purchasing credentials from underground markets to gain access to corporate resources or UN organizations' assets. UNICC observed several incidents where compromised corporate accounts served as the initial attack vector.

Recommended mitigations:
Rely on a Cyberthreat Intelligence service to continuously monitors underground communities for stolen credentials, enable multi-factor authentication, enforce strong password policies, monitor for anomalies, limit login attempts, and educate employees to mitigate credential-based attacks.

Denial of Service Attack (DDoS)
Mail Flooding
Subscription Bombing

The UNICC teams detected and mitigated numerous DDoS attacks throughout 2024, many of which were linked to geopolitical events and carried out by hacktivist groups. In addition to network DDoS attacks, other types, such as mail flooding and subscription bombing, were also observed.

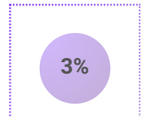
Recommended mitigations:
Mitigating DDoS attacks requires a combination of network infrastructure enhancements and specialized mitigation services. This may include traffic filtering, rate limiting, and other techniques to differentiate between legitimate and malicious traffic.

Malware

This cluster was created to include all the attacks focused on deploying malware without user interaction, such as man-on-the-side attacks or automated exploitation via USB.

The Common Secure team observed various cases involving a highly sophisticated threat actor capable of executing a man-on-the-side attack, which does not require any target interaction to achieve a successful infection.

Recommended mitigations:
The best defence against such intrusions is heightened vigilance and strong security procedures, including regular threat hunting, analysis of outbound network traffic, local hunting rules, and extensive logging to detect anomalies.



Others

Second Stage Techniques

The UNICC cybersecurity teams conducted extensive analysis on the initial vector of identified malicious events and have invested significant effort to track the second-stage techniques used by adversaries once access was obtained to the compromised network or accounts.

UNICC observed that malware continues to be used frequently and that the use of cloud threats has decreased slightly in 2024 compared to 2023. In most of the cases analyzed and managed by UNICC, adversaries have deployed malware on the compromised host as a primary action after the initial compromise. The malware observed in the various cases had different capabilities with the possibility of acting as backdoors, infostealers or more advanced codes composed of various modules that could be activated by the adversary based on the needs and type of target and victim.

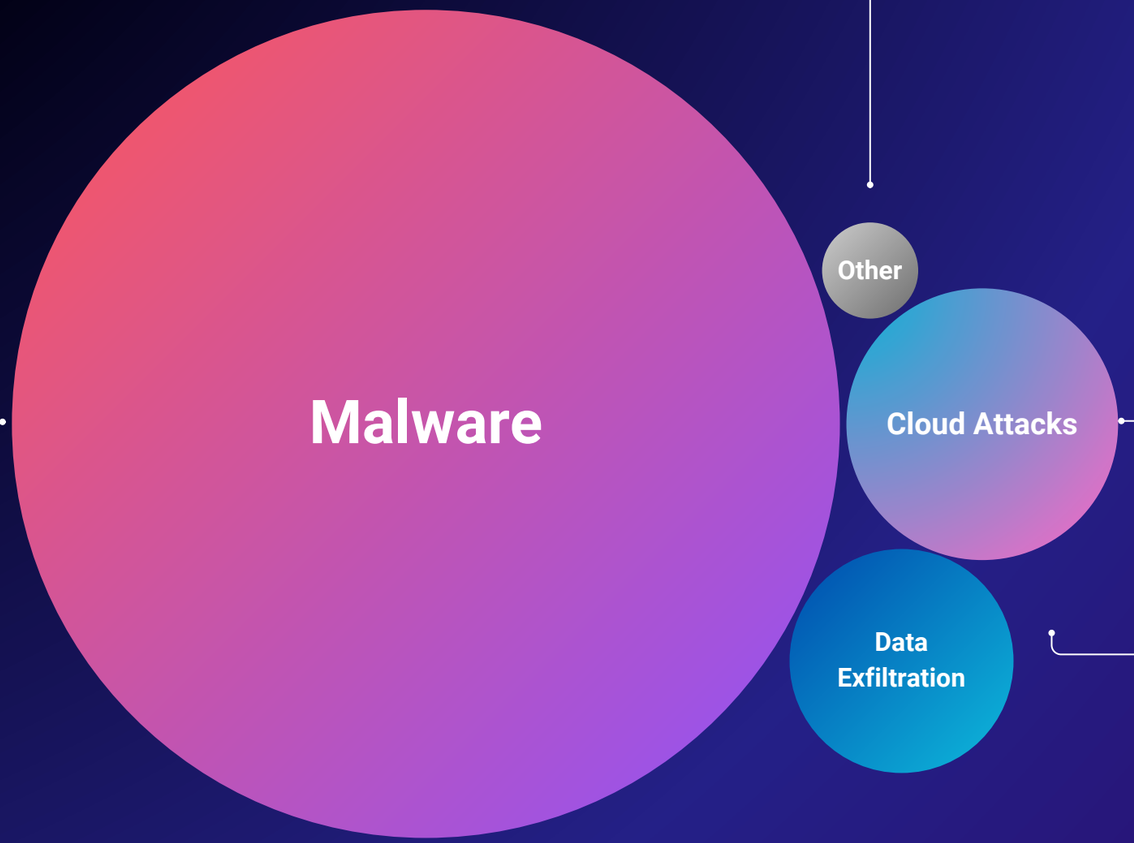
UNICC identified other techniques used in the second phase of the attacks, which affected the UN organizations to a much lesser extent (**2%** of the total). Among these techniques, UNICC has observed disruption activities or the use of compromised hosts or accounts to distribute phishing emails.

Unauthorized attempts to collect intelligence from cloud resources, especially via compromised accounts such as those in Microsoft Office 365, fall under this category of malicious events. These events can take various forms such as implementing custom rules in the O365 settings to forward emails or data directly to the attacker infrastructure. This category accounts for **8%** of the events recorded in 2024.

A special mention goes to an adversary who was able to steal sensitive data from a UN organization by abusing an O365 configuration that was set-up by some UN users.

UNICC observed that in **84%** of the analyzed cases, adversaries deployed malware to pursue their goals. Based on the type and the maturity of the different adversaries, the deployed malware had different purposes and levels of sophistication to evade security measures on the infected devices.

Special mention should be made this year to many cases handled related to families of infostealers malware, thus increasing the percentage of this category and significantly impacting the cyberthreat landscape scenarios of 2024. A large spike in detections related to a specific infostealer was detected from August 2024 onwards. This threat was immediately identified as a significant 2024 threat scenario and remained very active throughout the following months.



This year, we have recorded **6%** data exfiltration techniques perpetrated by different adversaries. This category includes techniques that instead of using the other vectors described such as malware or cloud for this purpose, they have directly used exfiltration techniques to try to steal sensitive data and achieve their goals. In some cases, adversaries manually exfiltrated data directly from the compromised systems.

Adversaries - Overview

Malicious activities against UN organizations are increasing in frequency and severity. Some of these malicious actions are being conducted by advanced actors with long-term objectives, while others are perpetrated by cybercriminals with the aim of financial gain. Hacktivist groups have also been pursuing objectives dictated by geopolitical events.

During 2024, UNICC observed **48 UN organizations being targeted by various organized adversaries**.

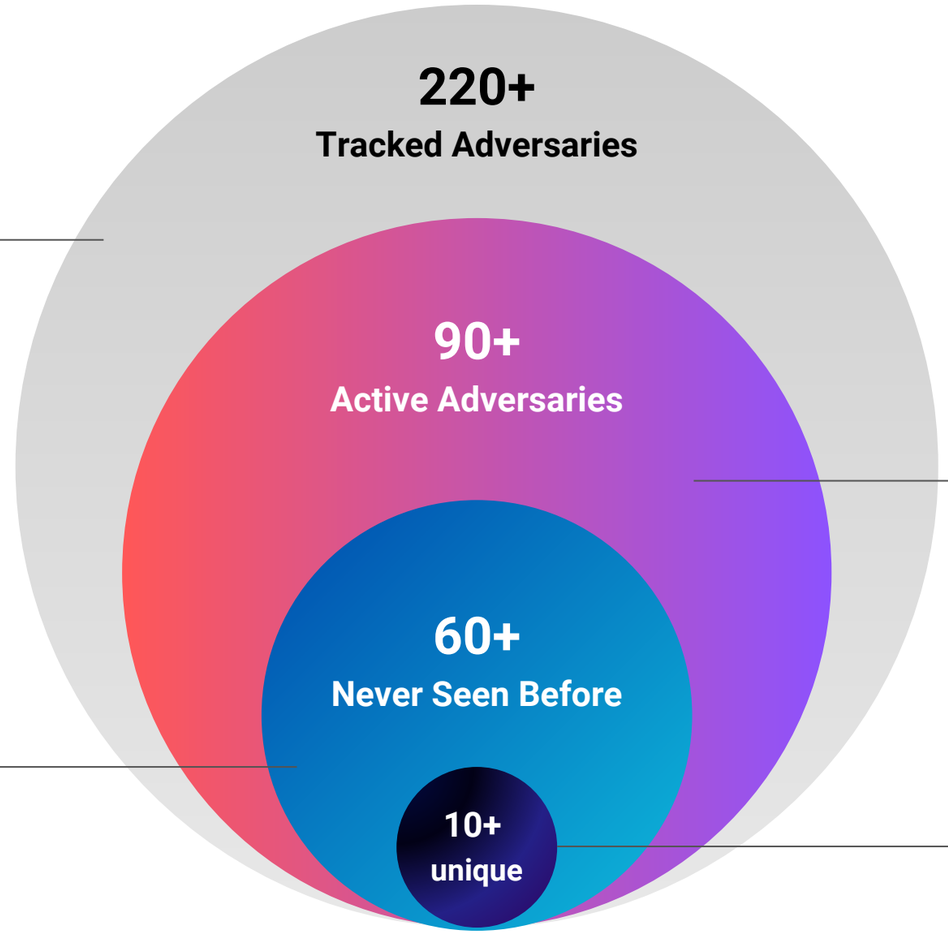
The graph below shows the historical data for the number of adversaries UNICC has been monitoring, and the increasing number of new and active groups detected in 2024.

48
Targeted UN Organizations

Based on UNICC visibility and ongoing monitoring by the Common Secure Cyberthreat Intelligence team, it was possible to identify 48 unique UN organizations that were targeted during 2024.

UNICC historical data related to the different adversaries or similar clusters of malicious activities.

Thanks to a detailed analysis of the retained logs related to the malicious activities of interest, it has been possible to outline over 220 adversary profiles that have targeted the UN system in recent years.



UNICC observed more than 90 different adversaries actively targeting the UN system in 2024.

Among these 90+ adversaries, about 30 different adversaries have been seen repeatedly over the past few years targeting various UN organizations.
These 30 adversaries are considered by UNICC as recurring threats and actively contribute to defining the cyberthreat landscape year after year.

A majority of the adversaries active in 2024 were not previously observed targeting UN organizations.

UNICC classified the various adversaries by looking for common characteristics such as Tactics, Techniques, and Procedures (TTPs), infrastructure and motivations. In 2024, a large number of new adversaries or adversary clusters have appeared on the scene.

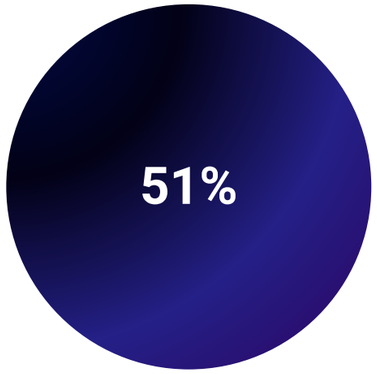
Within these new never-before-seen groups we have identified more than 10 unique ones where UNICC is working to attribute to a new cluster of malicious activity or known adversaries.

Adversaries - Goals

UNICC has identified, where feasible, the motives behind the numerous malicious activities of interest that have been directed at several UN organizations. UNICC investigations and Common Secure Threat Intelligence (CTI) analyses show that financial gain is currently the most prominent threat against the UN system.

Financially motivated adversaries lead the 2024 ranking, followed by info-gathering adversaries that have also created a high impact. Hacktivists and adversaries aiming to disrupt infrastructure remain present. Disinformation campaigns targeting the UN system were observed in small numbers during 2024.

The infographics represent the percentages of the various goals of adversaries identified during 2024, with specific details for each category:

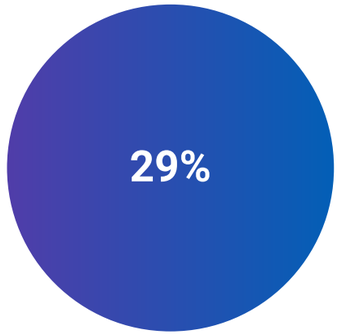


Financial gain

The goal of the Threat Actors most observed by UNICC during 2024 is financial gain.

Compared to last year, we have seen a higher presence of financially motivated adversaries. This statistic is partly due to the large presence of info-stealers whose main goal is to sell the stolen information to the highest bidder or directly on dedicated markets.

In a repeat of last year's observations, UNICC has also detected financially motivated adversaries installing crypto miners.



Information Gathering

Information gathering continues to be a major goal of adversary campaigns and cyberattacks against the UN system. Under the information gathering objective, UNICC has included attacks where the primary goal is the theft of sensitive information and data from targeted organizations based on their mission/mandate.

UNICC has observed sustained and persistent information-gathering attempts by various adversaries throughout the year, attempting to infiltrate their designated targets.

Hacktivism

Hacktivism accounted for 13% of the targets tracked for 2024. Recent geopolitical events have increased the number of active groups promoting a political or social agenda.

Disruption

To a lesser extent, UNICC has observed attacks with the sole goal of disrupting the targeted infrastructure. In this group of attacks, UNICC has included those attacks without a specific motivation or other goal.

Disinformation

UNICC observed online smear campaigns accusing UN organizations of corruption and ineffectiveness.
Disinformation techniques observed included recycling old media or republishing identical or slightly modified messages across multiple platforms to amplify false narratives to mislead the public and manipulate public perception.

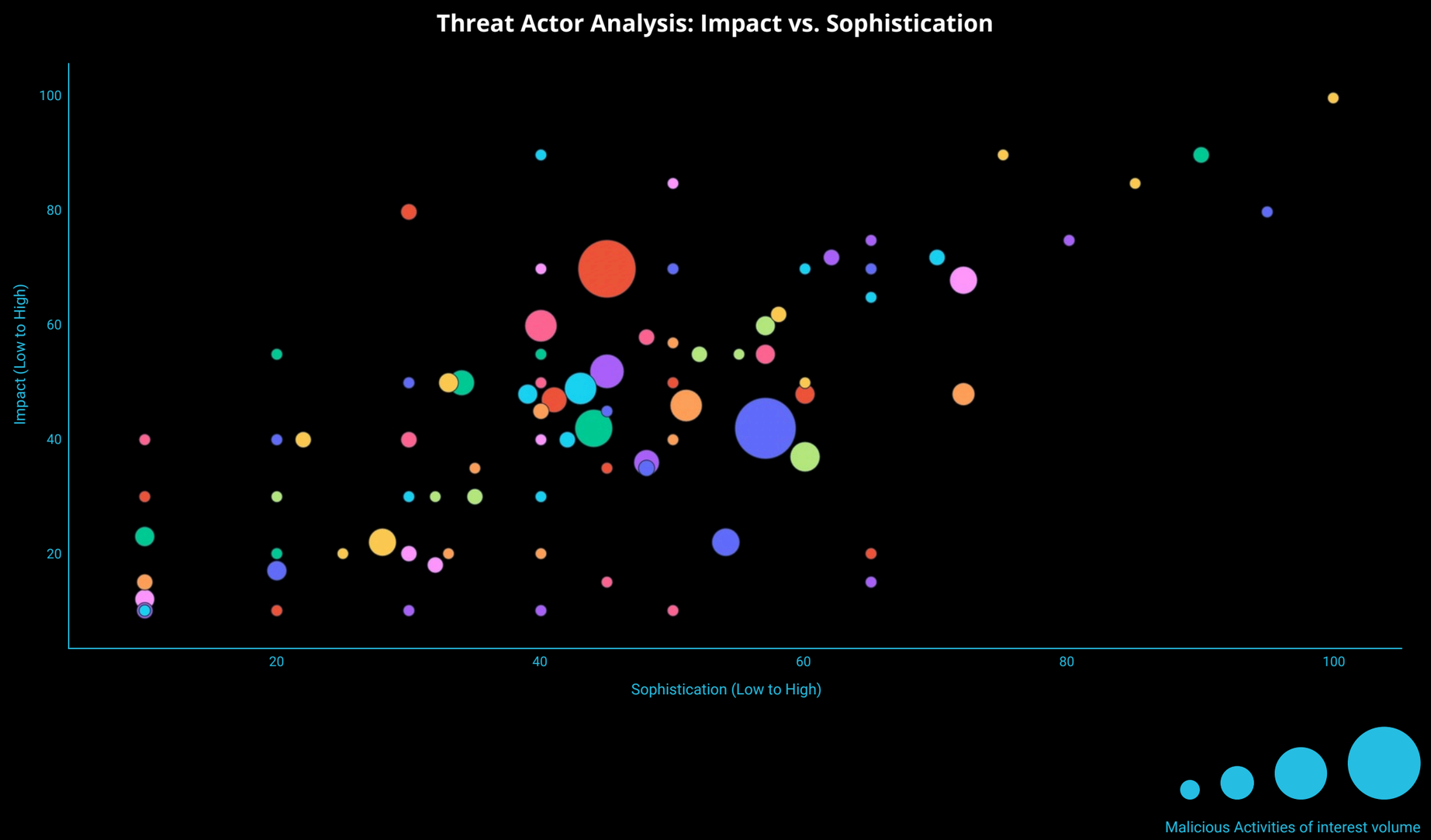
Adversaries - Graph

In 2024, the Common Secure Cyber Threat Intelligence implemented a new schema that rates on a scale from 0 to 100 the impact generated by the various malicious activities of interest and the sophistication used by the adversary who perpetrated the attack.

To calculate the impact and sophistication, an analytical approach was used based on a series of questions that allow for precise calculation for the observed use cases.

In addition to the impact and sophistication, the Common Secure team calculated the volume of malicious activities of interest for each adversary. This approach provides three parameters which have been used to create this graphic, representing the cyberthreat landscape scenario for the different observed adversaries with the relative impacts and sophistication used.

This approach allows us to identify the effectiveness of security defences against such adversaries. Thanks to this view is possible to immediately identify the success stories, where the adversaries utilized various advanced techniques to perpetrate their attacks but resulting in a limited impact. Alternatively, it is possible to easily identify the cases where security defences were either insufficient or ineffective, and with little sophistication, the adversaries succeeded in their intent, generating a high impact.



Relevant Adversaries

Goal: Financial gain - Ransomware attack
Targets: 1 UN organization office
Multiple UN organizations impacted
Description: Ransomware deployed

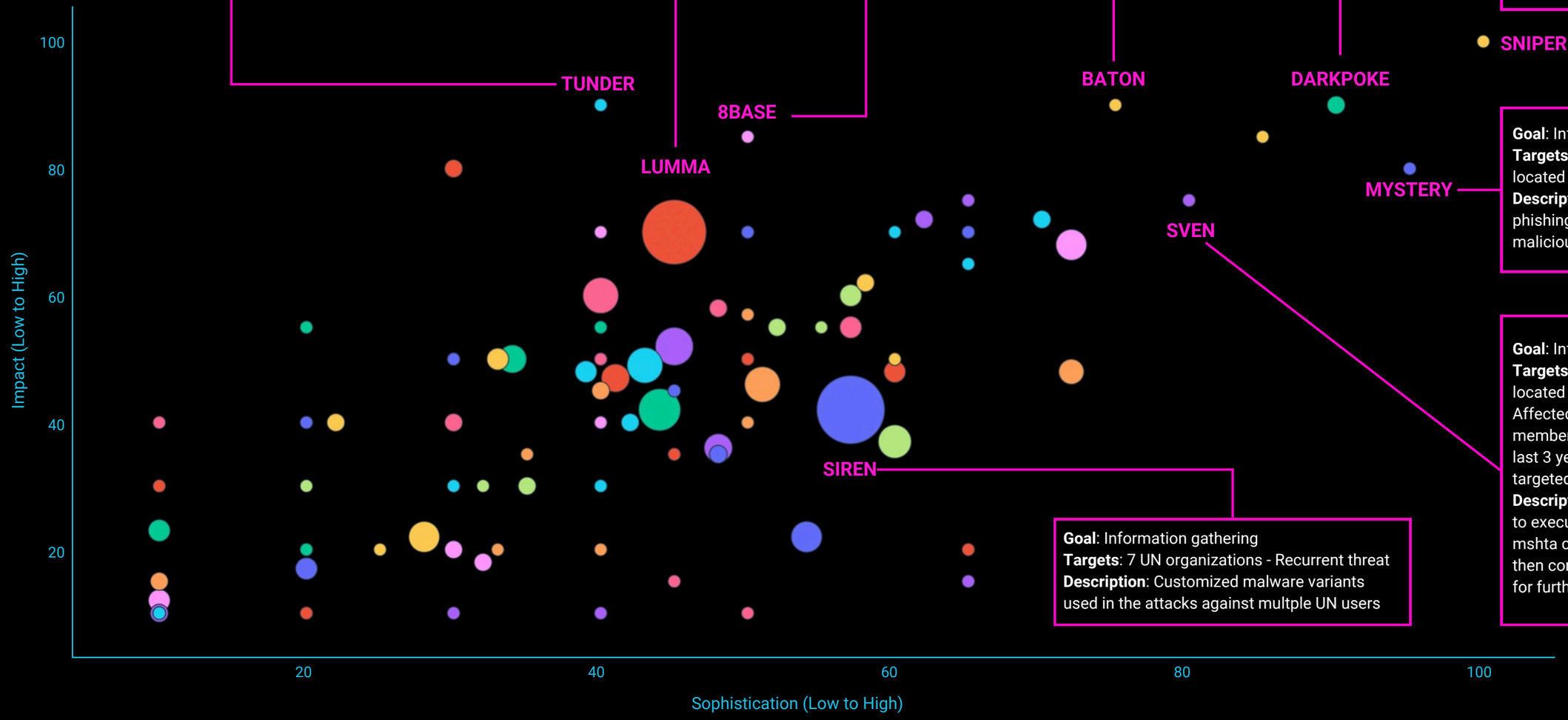
Goal: Information gathering
Targets: Offices of 3 UN organizations located in specific country
Description: Man-on-the-side attacks to intercept and manipulate network traffic and inject the malware

Goal: Long term intelligence gathering operation
Targets: *Compromised:* 5 UN organizations
Unauthorized Access: 10 UN organizations using a known compromised account
Description: Targeted Windows IIS internet-facing servers, using mostly deserialization attacks, to load a custom malware executing completely in-memory

Goal: Information gathering - Stealing email data
Targets: Multiple UN accounts related to a UN organization
Description: Compromised cloud accounts to steal emails from the victims

Goal: Information Stealing
Targets: 7 UN organizations
Description: Infostealer malware targeting users via phishing campaigns

Goal: Financial gain - Cyber criminal activities
Targets: 2 UN organizations
Description: Threat Actor who operates on cybercrime forums and Telegram to sell or share leaked databases



Goal: Information gathering
Targets: UN staff members located in a specific country
Description: Targeted phishing emails with malicious attachments

Goal: Information gathering
Targets: UN staff member located in a conflict region. Affected select UN staff members targeted in the last 3 years indicating targeted operations.
Description: LNK files used to execute wscript and mshta commands, which then connect to C2 servers for further malicious activity

Goal: Information gathering
Targets: 7 UN organizations - Recurrent threat
Description: Customized malware variants used in the attacks against multple UN users

The Way Forward

UNICC Valencia Office, Spann. Photo: UNICC

Cyberadversaries persistently target UN organizations. In 2024, UNICC recorded a more than 35% increase in detected cyberactivity, orchestrated by multiple threat actors with varying motivations, underscoring the critical need for UN organizations to continue to be vigilant.

With attackers increasingly exploiting the capabilities of Artificial Intelligence (AI), the cyberthreat landscape is expected to become more complex, making threat detection increasingly challenging. UNICC's Cybersecurity teams will continue to support partner organizations by providing shared solutions and capabilities, strengthening defences through a collective approach.

Based on the findings of the 2024 Cyberthreat Landscape Report, UNICC offers the following practical recommendations to assist UN organizations in navigating the evolving cyberthreat landscape, mitigating associated risks, addressing identified vulnerabilities, and establishing resilient cyberdefense architectures.

1. **Enhancing Threat Intelligence through collaboration**

   Organizations should continue to collaborate and mutually share threat intelligence as this allows early detection of advanced threats and the timely implementation of effective countermeasures.

2. **Continuous monitoring**

   Implementing continuous monitoring capabilities enables UN organizations to identify, respond to, and mitigate cyberthreats at an early stage, enhancing overall cybersecurity resilience.

3. **Prompt remediation of vulnerabilities and secure hardening**

   Regularly assess and patch vulnerabilities to minimize exposure to cyberthreats. Implement security best practices, such as system hardening and configuration management to strengthen defences.

4. **User awareness programs**

   Conduct regular cybersecurity training to educate employees on recognizing and mitigating common threats and periodically evaluate training effectiveness through simulated phishing and social engineering attacks. Foster a security-first culture across the organization.

5. **Identity protection**

   Enforce strong authentication measures, including multi-factor authentication (MFA) and zero-trust principles, to safeguard user identities and prevent unauthorized access.

UNICC | Cybersecurity

www.unicc.org

TLP: CLEAR