UNICC

Cyber Threat Landscape Report 2023

May 2024

TLP: CLEAR

CONTENTS

Executive Summary

Cyber threats targeting United Nations organizations are increasing in frequency and severity, representing a critical risk to the entire UN system. As observed in previous years, UN organizations continued to experience cybersecurity incidents ranging from advanced actors to cyber criminals and hacktivists. UNICC's expansion into cybersecurity shared solutions has established an effective collective defence capability against these threats.

During 2023, UNICC's cybersecurity division responded to a large number of cyberattacks targeting multiple UN organizations and observed relevant malicious activities distributed over various regions worldwide. The analysis and the correlation of this data highlighted a **170% increase** in malicious activities of interest when compared to 2022 data. The UNICC cybersecurity division provided confidential support to targeted organizations to address various cyber threats.

In the majority of the incidents, the cyber threat landscape mirrored the geopolitical situation, as cyber-attacks were increasingly used to achieve objectives in strategically relevant crisis zones.

In 2023, the Common Secure Cyber Threat Intelligence team observed and tracked more than **50** different adversaries, including more than **30 never-before-seen adversaries** targeting UN organizations. These groups range from opportunistic individuals to highly sophisticated groups leveraging advanced attack techniques and capabilities. The main goals of these adversaries included information gathering, financial gain through different targeted fraud schemes or disrupting the mandate of UN organizations. The observed malicious activities of interest were initiated through various attack vectors, by far the most common being phishing schemes, followed by the misuse of stolen accounts or exploitation vulnerabilities in public-facing applications.

UNICC's cybersecurity division provided UN organizations with a robust set of shared cybersecurity capabilities to hunt for threat actors, disrupt their campaigns, address vulnerabilities and respond to incidents. Common Secure allowed a unified approach to tackling cyber threats, providing increased visibility into high-risk networks.

For this report, UNICC's cybersecurity teams have collaborated in consolidating 2023 data for supported organization to comprehend the trends in the cyber threat landscape. Moreover, this report enables UN organizations to understand the nature of common cyber threats impacting similar organizations within the UN system. Accordingly, UNICC provides a series of recommended actions that organizations could consider to better prepare to address these evolving cyber threats.

2023 UNICC Common Secure Conference in Valencia, Spain
Photo: UNICC

Context and Background

The primary objective of the UNICC Cybersecurity division is to **support United Nations organizations in ensuring service continuity and proficiently managing incidents and risks.** 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 on their members, states, 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 cyber threats.

UNICC operates a multi-tiered Common Cybersecurity Operations Centre (CSOC) operating 24/7 to centralize the detection, triage and response to cyberattacks impacting technology assets. It offers multiple levels of defence, each with increasing levels of domain expertise, that collaborate to provide comprehensive protection against cyberthreats.

The CSOC monitors the networks, hosts, applications and users leveraging a combination of tools such as intrusion detection systems, firewalls, endpoint detection and response (EDR) solutions, network logs, and events from these sources are ingested into the Security Information and Event Management system (SIEM) for correlation and analysis. When an incident is detected, it is triaged to determine the severity and impact. The Computer security emergency response team (CSIRT) then takes appropriate action to contain the incident and prevent further damage, such as isolating the affected systems and executing incident response plans.

Cybersecurity specialists located around the world with a variety of professional certifications, experience and technical expertise facilitate the analysis of multilateral cyber threats. This constant cycle of detection, triage and response contributes to guaranteeing that the United Nations organizations supported by UNICC remain secure and protected from cyberthreats. UNICC Threat Detection and Response teams support UNICC's greater mission of Digital for the UN by ensuring cybersecurity best practices are embedded in every digital product that UNICC builds.

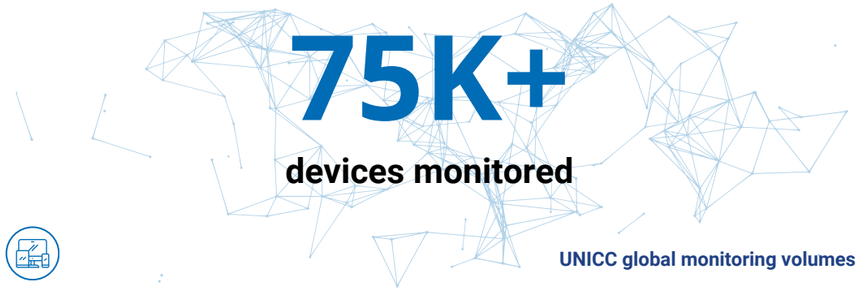
UNICC global monitoring volumes in 2023

UNICC global monitoring volumes in 2023

UNICC also relies on the Common Secure Cyber Threat Intelligence (CTI) team to aid the United Nations with situational awareness and early warning of new cybersecurity threats, incidents and challenges. Thanks to proactive communication with the various UN organizations, the CTI team has promptly shared dozens of alerts and actionable intelligence reports to the impacted entities and the wider Common Secure Threat Intelligence community, allowing other organizations to prepare proactive measures.

The UNICC CSOC, CSIRT and Common Secure Threat Intelligence teams are actively protecting **42** UN organizations, monitoring over **130k** active directory accounts and **75k** devices globally. Using data collected from monitoring these data sources and the information gathered by threat intelligence, UNICC continues to identify numerous malicious activities of interest related to UN organizations.

UNICC utilizes the term "Malicious activities of interest" to classify all cyber threats, security incidents, and events aimed at UN organizations that are relevant to advance proactive cyber defences. These malicious activities are also seen as crucial for strategic, operational, and tactical threat intelligence, contributing to improving the security posture of the different UN organizations.



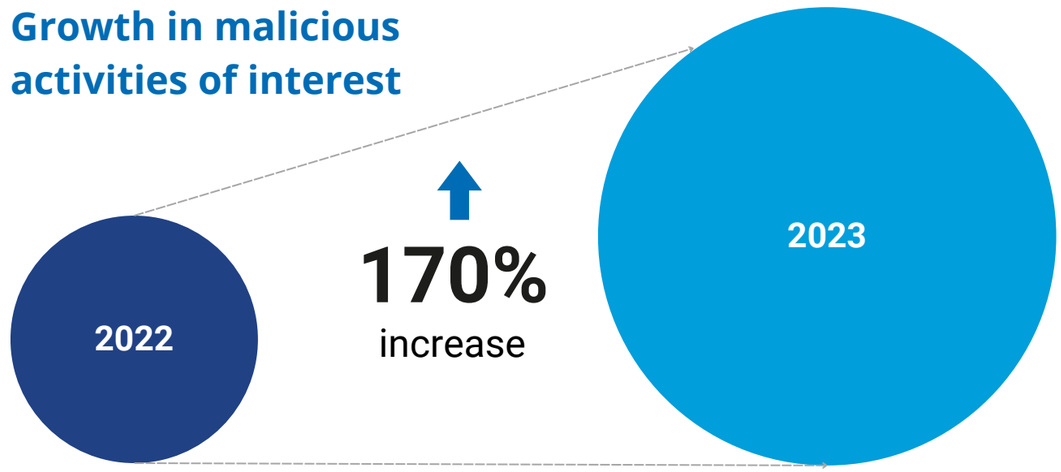
UNICC global monitoring volumes in 2023

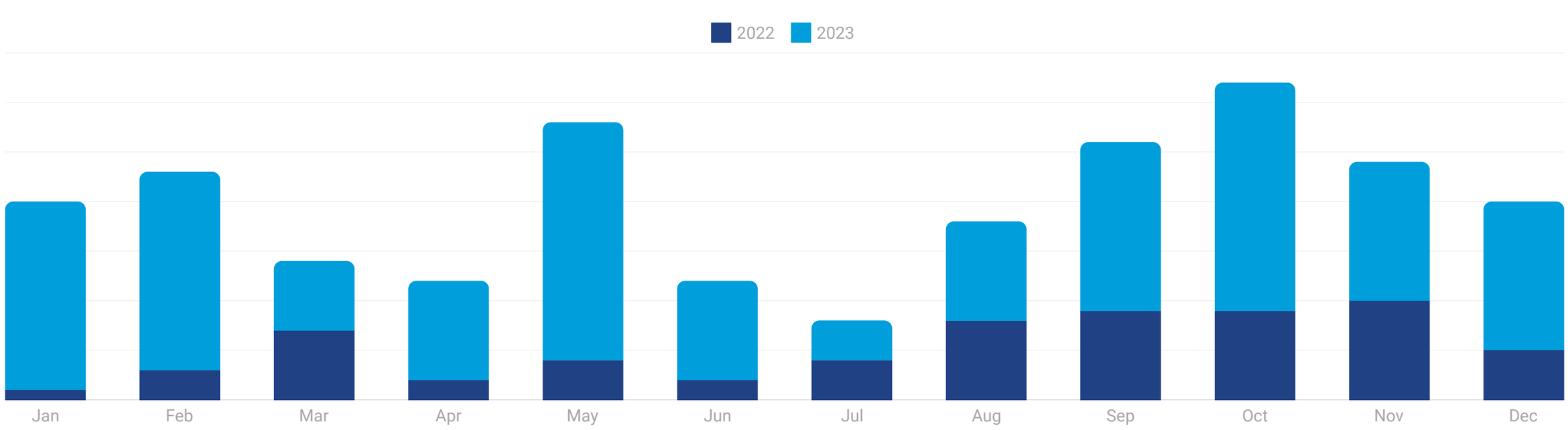
Malicious Activities of Interest - Overview

In 2023, the UNICC CSOC, CSIRT and Common Secure Cyber Threat Intelligence teams observed a **170%** increase in the malicious activities of interest with respect to 2022 levels. The collective analysis of these malicious activities empowered the United Nations to work together and provide a united response to more effectively address these cyber threats than if they had worked independently as individual organizations.

UNICC Threat Detection and Response teams used automated and manual means to conduct a thorough analysis of these security events. Organizations impacted by security incidents that had 24x7 detection capabilities in place took less time to contain and resolve the security incidents compared to those without such capabilities.

Towards the end of 2023, the number of malicious activities of interest increased, as was also observed in 2022.





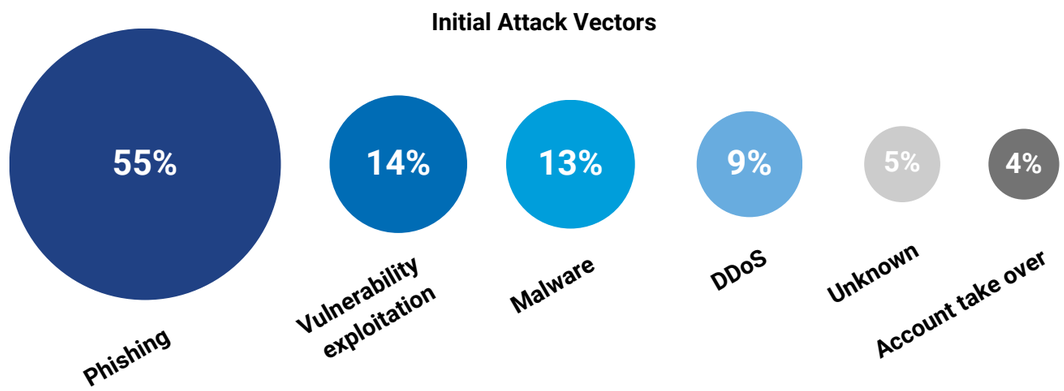
Malicious activities of interest volume over the year

Initial Attack Vectors

In 2023, the multitude of malicious events targeting the different UN organizations managed by the UNICC CSIRT team or identified by the Common Secure - Cyber Threat Intelligence team were initiated predominantly through attack vectors of phishing schemes, misuse of stolen accounts or exploiting vulnerabilities in public-facing applications.

Phishing leads the ranking, used in more than **50%** of the attacks, so UNICC can confirm the preference of adversaries targeting various UN organizations to use methods that exploit user 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 access the corporate network via improperly patched systems that are exposed on the internet.



Phishing

The UNICC Common Secure Cyber Threat Intelligence team observed different phishing schemes used by multiple threat actors during 2023.

In some cases, the team observed QR codes tricking users into opening malicious links. In other cases, malicious domains similar to those of UN organizations have been used to trick victims into providing credentials or personal information. Additionally, malicious email threads incorporating domains that mimic UN organizations have been occurrences, serving fraudulent or info-gathering purposes. In other instances, users were convinced to download malware, leading to its execution and potential infection of their computers.

Suggested mitigations:
Unaware users represent a significant initial threat attack vector. Users should be trained on how to identify phishing emails and how to respond appropriately to them.

Vulnerability exploitation

The UNICC CSIRT team analyzed various instances of malicious events to identify the “patient zero” for various instances of malicious events, the most common initial vector was found to be internet exposed hosts with vulnerabilities. The attacker can take advantage of known vulnerabilities in the application code to execute malicious actions, such as data theft or system compromise.

Suggested mitigations:
Implementing regular security patches, utilizing robust cyber security controls will help to mitigate this attack vector that several known adversaries commonly attempt to exploit on a daily basis.

Malware

This cluster has been created in order to include all attacks aimed at deploying malware without user interaction such as man-on-the-side attacks or automated exploitation via USB.

UNICC managed various incidents related to an extremely sophisticated threat actor able to leverage a man-on-the-side attack that doesn't require any interaction with the target to lead to a successful infection.

Suggested mitigations:
The only way for potential targets to defend against such intrusions is to remain extremely vigilant and have robust security procedures involving regular threat hunting activities, analysis of outbound network traffic, local hunting rules and extensive logging to detect anomalies.

Denial of service attack (DDoS)

Many DDoS attacks have been detected and mitigated over the 2023 by the UNICC teams. These attacks mainly followed geopolitical events and most of them were perpetrated by hacktivism motivated groups.

Suggested mitigations:
Mitigating DDoS attacks requires a combination of network infrastructure improvements and specialized DDoS mitigation services. This can involve traffic filtering, rate limiting, and other techniques to distinguish legitimate from malicious traffic.

Account take over

Threat Actors employ techniques such as credential stuffing, password spray attacks, or purchasing credentials from underground markets to access corporate resources or UN organizations’ assets. UNICC observed different incidents where the initial vectors were the corporate compromised accounts.

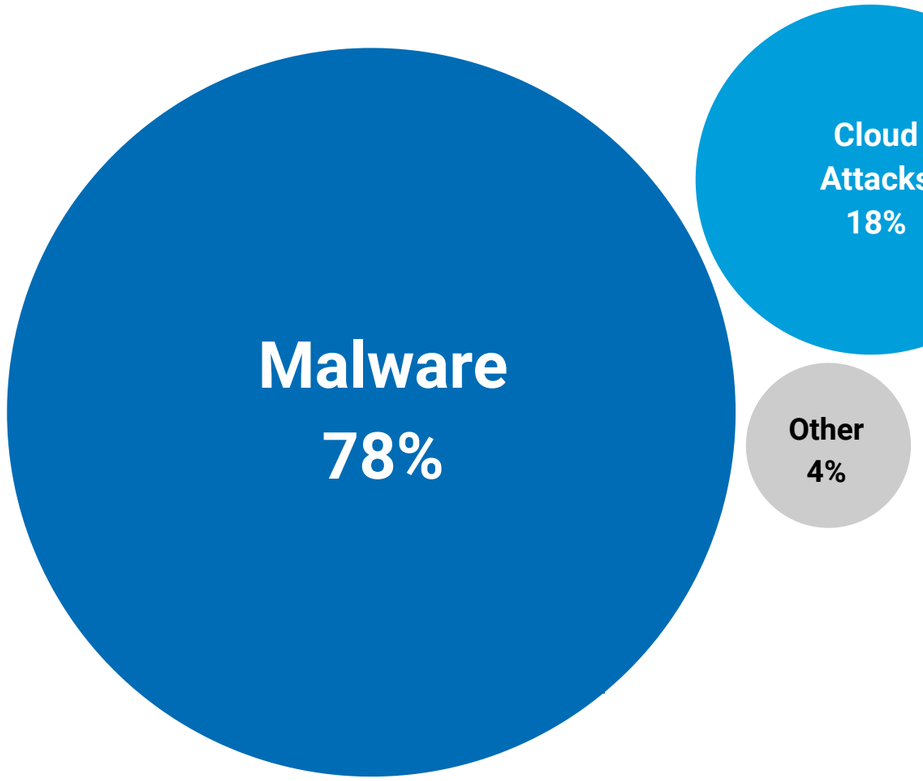
Suggested mitigations:
The UNICC Common Secure Cyber Threat Intelligence team constantly monitors underground communities for stolen credentials related to various UN organizations. As a result of this monitoring, UNICC was able to alert several organizations and prevent further credential fraud or advanced attacks.

Second Stage Techniques

The UNICC Threat Detection and Response teams conducted extensive analysis on the initial vector of identified malicious events, and have also invested significant effort to track the second stage techniques in use by the 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 is on the rise in 2023. In the majority of cases analyzed and handled by UNICC, adversaries deployed malware on the compromised host as a primary action following the initial compromise. Once the cyber-attacker has compromised the secured system, they are able to execute additional malicious code to achieve their final objectives.

UNICC observed that in **78%** 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.



Unauthorized attempts to collect intelligence from cloud resources, especially via compromised accounts like 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.

In addition to the larger two categories, UNICC identified other techniques used in the second phase of the attacks, which affected the organizations to a much lesser extent. UNICC has classified these techniques as a single category. Among these techniques, UNICC has observed ransomware-like activities, the use of compromised hosts or accounts to distribute phishing emails and site defacement techniques.

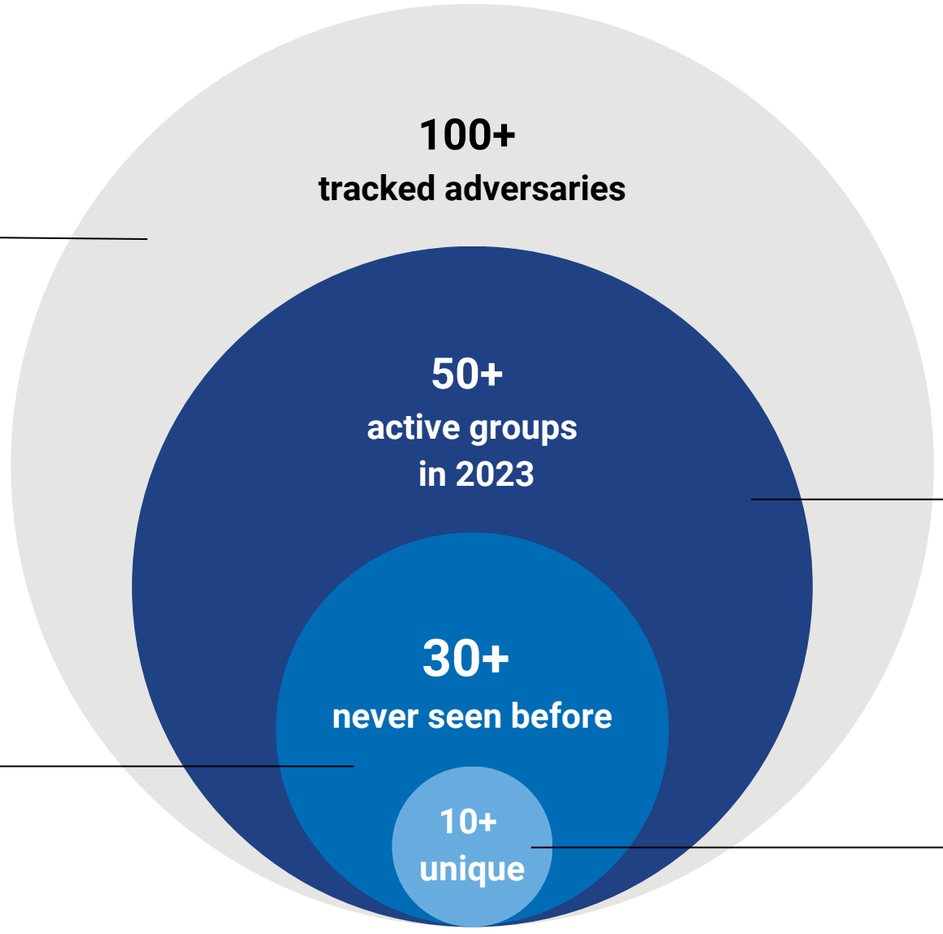
Adversaries - Overview

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 cyber criminals with the aim of financial gain. These include exploiting the UN organization's brand or carrying out cyber attacks to mine cryptocurrencies. Hacktivist groups have also been pursuing objectives dictated by geopolitical events.

During 2023, UNICC observed **46 UN organizations being targeted by various 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 2023.

46 targeted UN organizations in 2023



UNICC historical data from tracking adversaries or similar cluster of malicious activities.

Adversaries actively targeting the UN system in 2023.

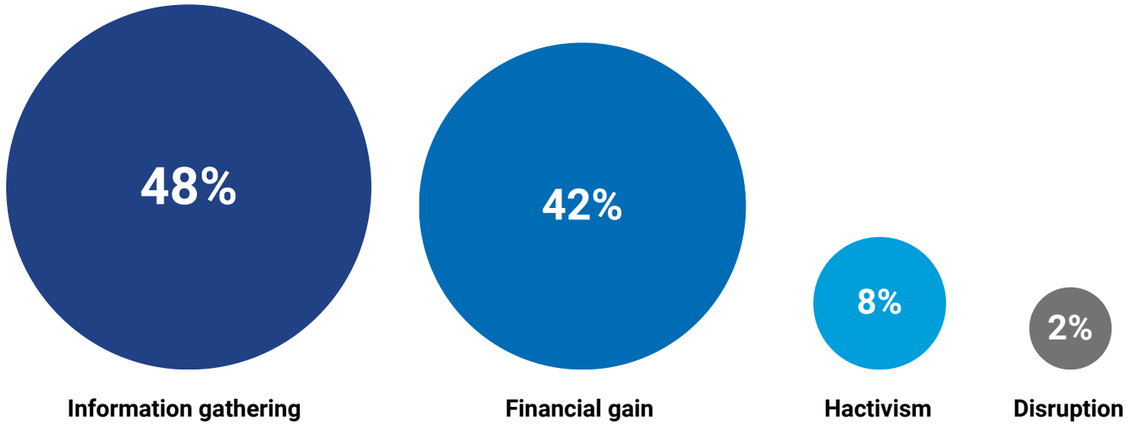
A majority of the adversaries active in 2023 were not previously observed targeting UN organizations.

UNICC is working to attribute to a 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) reports show that information gathering is the most prominent threat against the UN system.

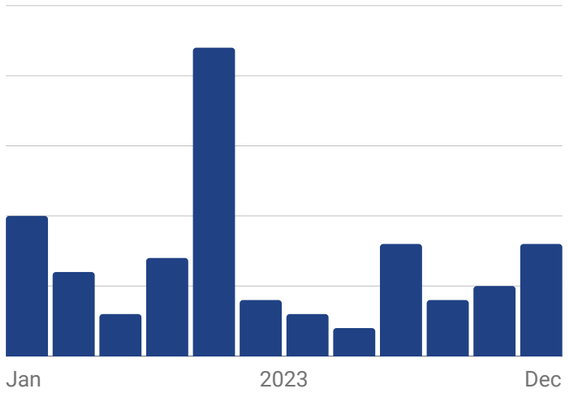
The infographics represent the percentages of the various goals of adversaries identified during 2023, with specific details and real examples for each category:



Information Gathering

Information gathering continues to be a prime goal of the adversaries' campaigns and cyber attacks against the UN system. Under the goal of information gathering, UNICC has included attacks where the main objective is the theft of sensitive information and data from the affected organizations based on their mission/mandate.

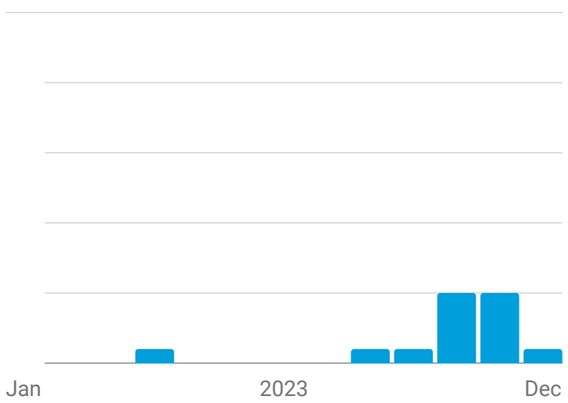
UNICC observed prominently targeted info-gathering campaigns against multiple UN organizations in May 2023. However, UNICC has tracked an ongoing and persistent endeavour by various groups throughout the year to persist in attempting to infiltrate their designated targets.



Hacktivism

Hacktivism represented 8% of the 2023 tracked goals. Recent geopolitical events have increased the number of active groups promoting a political or social agenda.

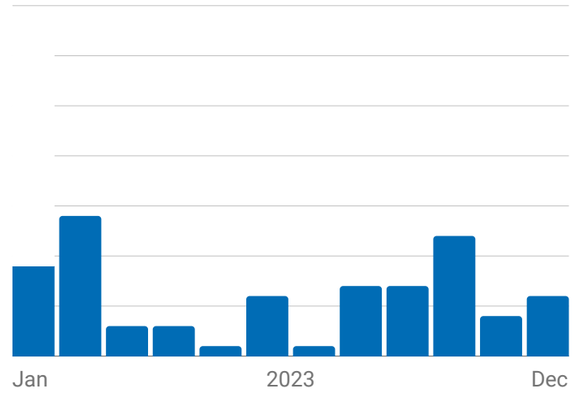
Hacktivist group activity was observed throughout 2023, with a large spike in Q4. This spike was mainly caused by geopolitical events which mobilized and reactivated many hacktivist groups, perpetrating several attacks such as DDOS or defacements of the assets of various UN organizations operating in the field or that are involved in the related crises.



Financial gain

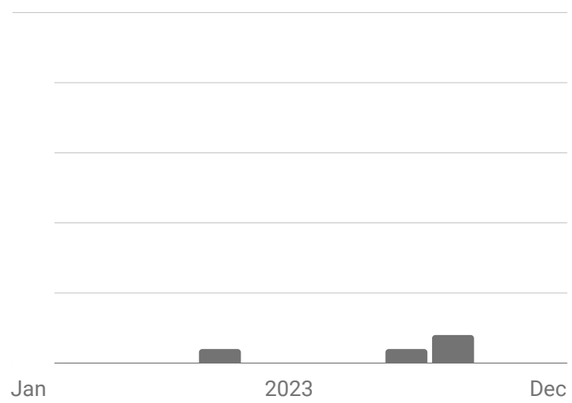
Following closely behind Info-gathering, the second most common goal for threat actors was financial gain. Once systems were compromised, UNICC observed financially motivated adversaries installing crypto miners or info-stealers; adversaries invested significant effort to convince victims to pay.

In other cases, cybercriminals have posted stolen data for auction in underground communities.



Disruption

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



Relevant Adversaries

The UNICC Common Secure Cyber Threat Intelligence team has listed 5 of the most relevant or impactful adversaries who have taken center stage in 2023.

The following table identifies the most relevant adversaries discovered and tracked during 2023 with their main goals and characteristics. UNICC assigned internal code names to the different adversaries or clusters of malicious activities.

Adversary	Main Goal	Targeted UN organizations	Description
PRYSM	Information gathering	**13**	The info-gathering group PRYSM has been observed using temporary infrastructure, diverse payloads, and obfuscation methods. PRYSM relied on phishing as a primary method to gain initial access and compromise targeted hosts. PRYSM targeted specific UN organizations, diplomatic and government entities by focusing on organizations that could provide fresh intelligence about conflicts in specific regions.
SIREN	Information gathering	**6**	SIREN is a persistent adversary that has been active for years targeting UN organizations using a unique infection chain for intellectual property theft. SIREN has been observed to compromise hosts by employing customized malware variants and sometimes using UN organization brands as bait. The group, active throughout 2023, poses a severe and recurrent threat, with a focus on entities located in specific areas.
MIMICORE	Information gathering	**14**	MIMICORE focuses on information gathering by creating numerous fake domains that resemble UN organizations and then distributing phishing emails referring to fake conferences or events which abuse the different UN organizations' brands. By mimicking official UN communication, MIMICORE aims to deceive recipients and collect sensitive information and personal data.
DARKPOKE	Information gathering	**3**	DARKPOKE is a sophisticated adversary which has been observed targeting UN organizations located in specific areas suggesting a well-defined and focused info-gathering agenda. The main goal of the group is to gather sensitive data by executing commands and maintaining persistence on the targeted hosts. DARKPOKE uses sophisticated methods to perpetrate its attacks, including the use of man-on-the-side attacks to intercept and manipulate network traffic. The malware operated by DARKPOKE is stealthy and difficult to detect, often masquerading as legitimate software updates or other innocuous files.
TITAN	Information gathering	**1**	TITAN is a sophisticated and highly skilled adversary that has been observed targeting a UN organization in a conflict region. TITAN used Living off the land (LOTL) technique via compromised accounts to exfiltrate sensitive information from the targeted hosts. The adversary has demonstrated advanced skillset by using uncommon and stealthy techniques to quickly achieve their goal.

The Way Forward

2023 UNICC Common Secure Conference in Valencia, Spain
Photo: UNICC

Cyber adversaries consistently target UN organizations. In 2023, UNICC observed over **170%** growth in detected activity orchestrated by multiple threat actors with different motivations, emphasizing the need for UN organizations to remain vigilant.

As attackers increasingly leverage Artificial Intelligence (AI), the threat landscape is expected to evolve, making detection of these threats increasingly difficult. UNICC's cybersecurity division will continue to support partner organizations through shared solutions, enhancing defence capabilities through a collective approach to safeguarding UN organizations.

Considering the observations in this 2023 Cyber Threat Landscape Report, UNICC offers the following practical recommendations to UN organizations to contend with the ever-changing landscape of cyber threats, manage associated risks, rectify identified vulnerabilities, and establish robust defensive architectures:

1. **Threat intelligence-driven cybersecurity capabilities**

   Organizations should continue to collaborate and share threat intelligence with each other as this allows early detection of advanced threats and inform the implementation effective prevention controls.

2. **Continuous monitoring**

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

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

   Prioritizing the vulnerability management program to swiftly address vulnerabilities and implementing robust hardening practices, particularly on internet-exposed services, can significantly reduce the success rate of cyberattacks.

4. **User awareness programs**

   Unaware users represent a significant initial threat attack vector. Although technical controls can mitigate attacks targeting users, it is still essential to adopt and follow comprehensive user awareness programs to ensure that users are not the weak link in the chain but actively participate in the defence of their organizations.

5. **Identity protection**

   Threat actors continue to exploit vulnerabilities in identity management systems that grant access to sensitive information. Using secure modern authentication approaches, such as passwordless authentication and security keys, will reduce the likelihood of successful attacks, especially against cloud services.

UNICC

www.unicc.org

TLP: CLEAR