



Cyber Threat Landscape Report 2022

April 2023

TLP: CLEAR

CONTENTS

03	Executive Summary
05	Context and Background
07	Cyberattacks Overview
09	Cyberattack Vectors
11	Cyberthreat Categories
15	The Way Forward

Executive Summary

United Nations agencies, funds and programmes face escalating cyberthreats. Information and communications technology assets and cyber-enabled solutions are central to the United Nations mission and its diverse mandates. These assets are a target for a variety of cyber attackers, including criminal organizations and advanced actors. The growth of UNICC's shared cybersecurity capabilities has created a common defense capability within the UN system.

In 2022, UNICC responded to a large number of cyberattacks across multiple agencies. UNICC's cybersecurity team worked confidentially with agencies experiencing cyberattacks. The threat actors ranged from opportunistic individuals to highly sophisticated groups leveraging advanced attack techniques. The impact of these cyberattacks included the theft of information, disrupting the mandate of UN agencies, leveraging technology assets as a springboard to attack constituents, stealing intellectual property, conducting cyber espionage or information asset destruction. Attacks were initiated through four common paths: phishing schemes, misuse of stolen credentials, exploitation of remote access services or exploitation of vulnerabilities in public-facing applications.

UNICC provided UN agencies with a robust set of shared cybersecurity capabilities to hunt for threat actors, disrupt their campaigns, address vulnerabilities and respond to incidents. Pooling cyberdefensive operations within UNICC allowed the UN to address cyberthreats as a united front, harnessing the collective insights gained by UNICC from all subscribing agencies. This provided greater visibility into high-risk networks and drove partnerships with key stakeholders to plan for and minimize the impact of cyberattacks. The UNICC cybersecurity team tracked several active threat actors in 2022. For example, the Common Secure Cyber Threat Intelligence sharing platform contributed to the collective defense by allowing participating agencies to prevent the attacks of actors leveraging the same attack infrastructure.

The cyber threat landscape is ever-evolving. Recent threat developments have included the weaponization of cyber tools for use in war and the infiltration of technology supply chains. In the coming years, organizations need to consider the adversarial use of Artificial Intelligence (AI) and Machine Learning (ML). The emergence of quantum computing presents significant security risks, as it has the potential to break existing encryption algorithms and undermine the security of critical infrastructure.

This report recommends a set of actions agencies could consider to address evolving cyberthreats, manage risk, remediate vulnerabilities and ensure business continuity. The UNICC cybersecurity division provides capacity building for UN agencies needing support in developing threat-informed defensive capabilities and programmes.



2022 UNICC Common Secure Conference in Valencia, Spain
Photo: UNICC

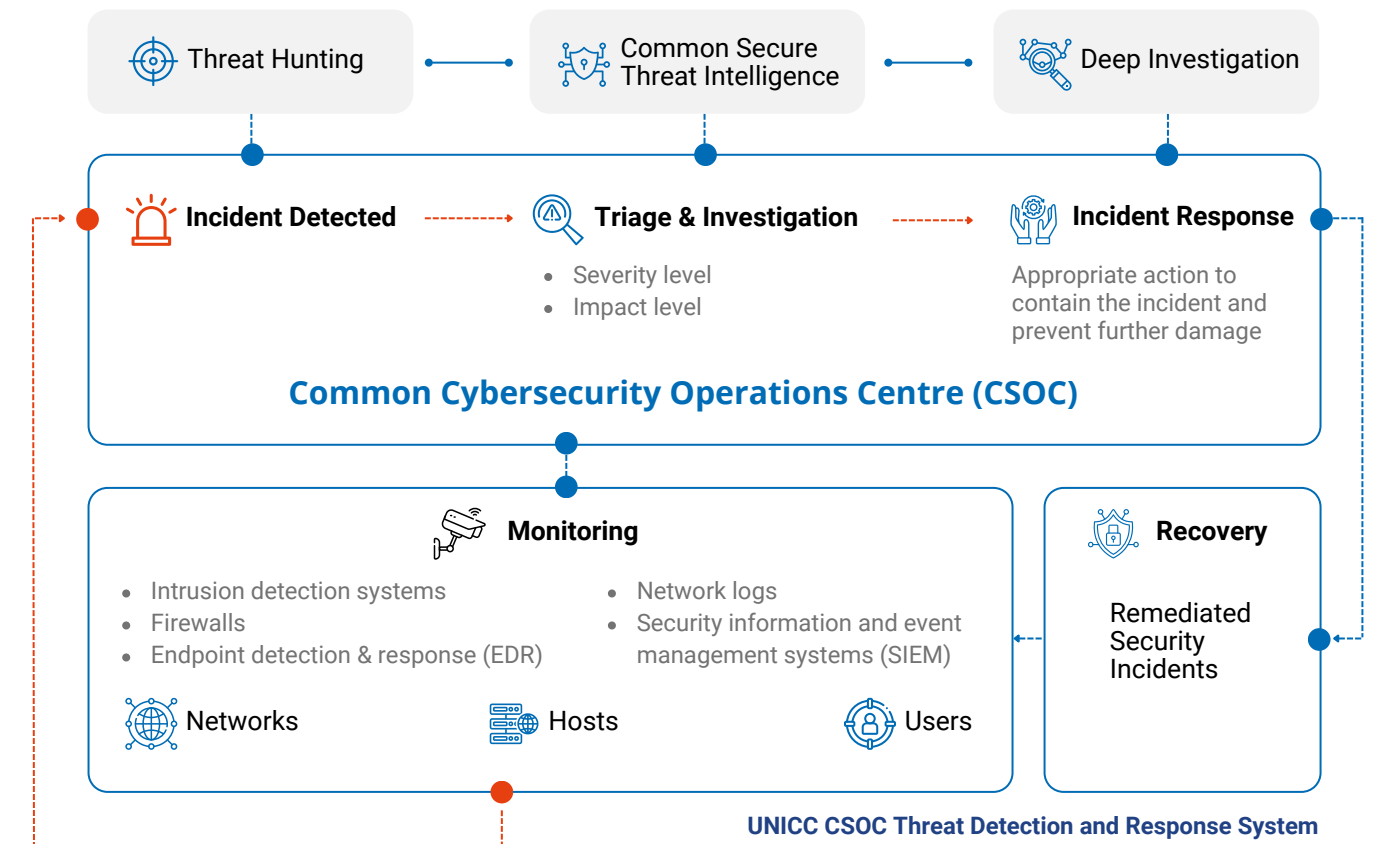
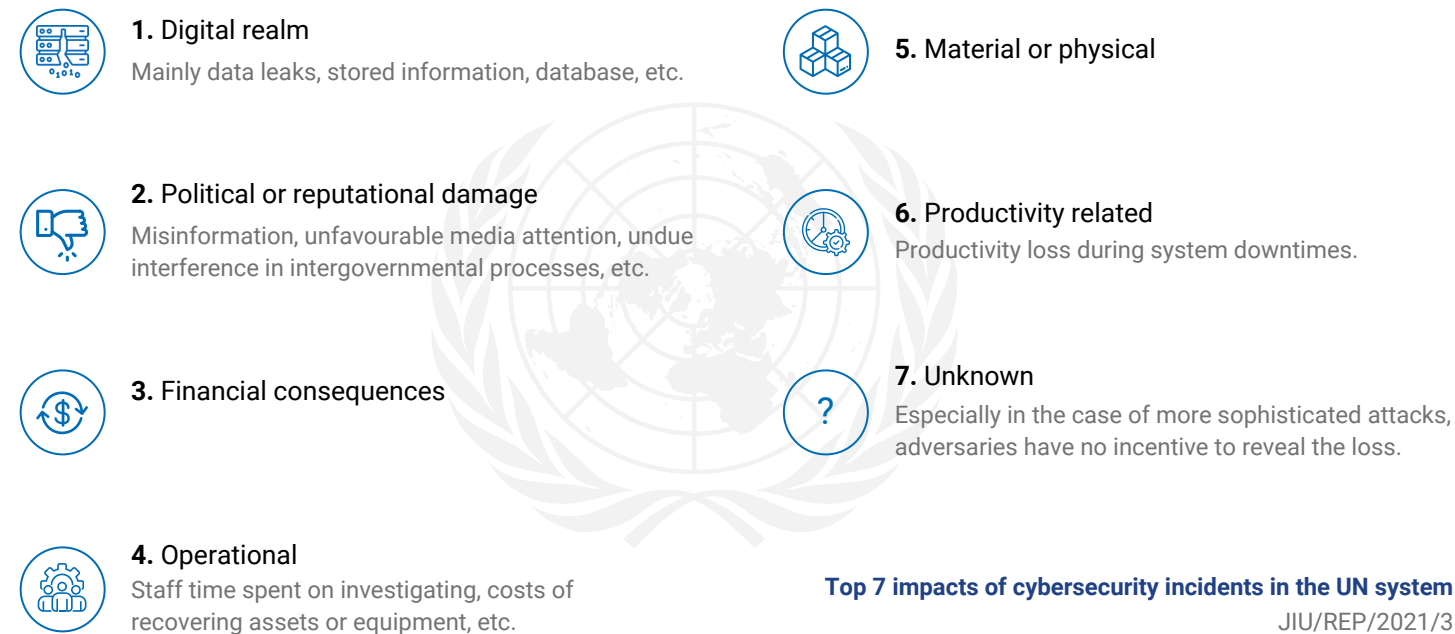
Context and Background

The UNICC Cybersecurity Threat Landscape Report aims to support service continuity, incident and risk management of United Nations organizations by defining the **evolving nature of cyberthreats** contained and responded to by UNICC.

Information and communications technology assets and cyber-enabled solutions are central to the United Nations mission and its diverse mandates. United Nations agencies 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 cyberthreat actors and agencies can benefit from **collective defense capabilities** against the common cyberthreats.

UNICC operates a multi-tiered Common Cybersecurity Operations Centre (CSOC) designed to centralize the detection, triage and response to cyberattacks impacting technology assets 24/7. It has multiple levels of defense, each with increasing levels of security, that work together to provide comprehensive protection against cyberthreats.

The CSOC monitors the networks, hosts and users utilizing a combination of tools such as intrusion detection systems, firewalls, different endpoint detection and response (EDR) tools, network logs and security information and event management systems (SIEM). When an incident is detected, it is triaged to determine the severity and impact. The computer 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 ongoing cycle of detection, triage and response helps ensure that the United Nations agencies supported by UNICC remain secure and protected from cyberthreats to the greatest extent possible.

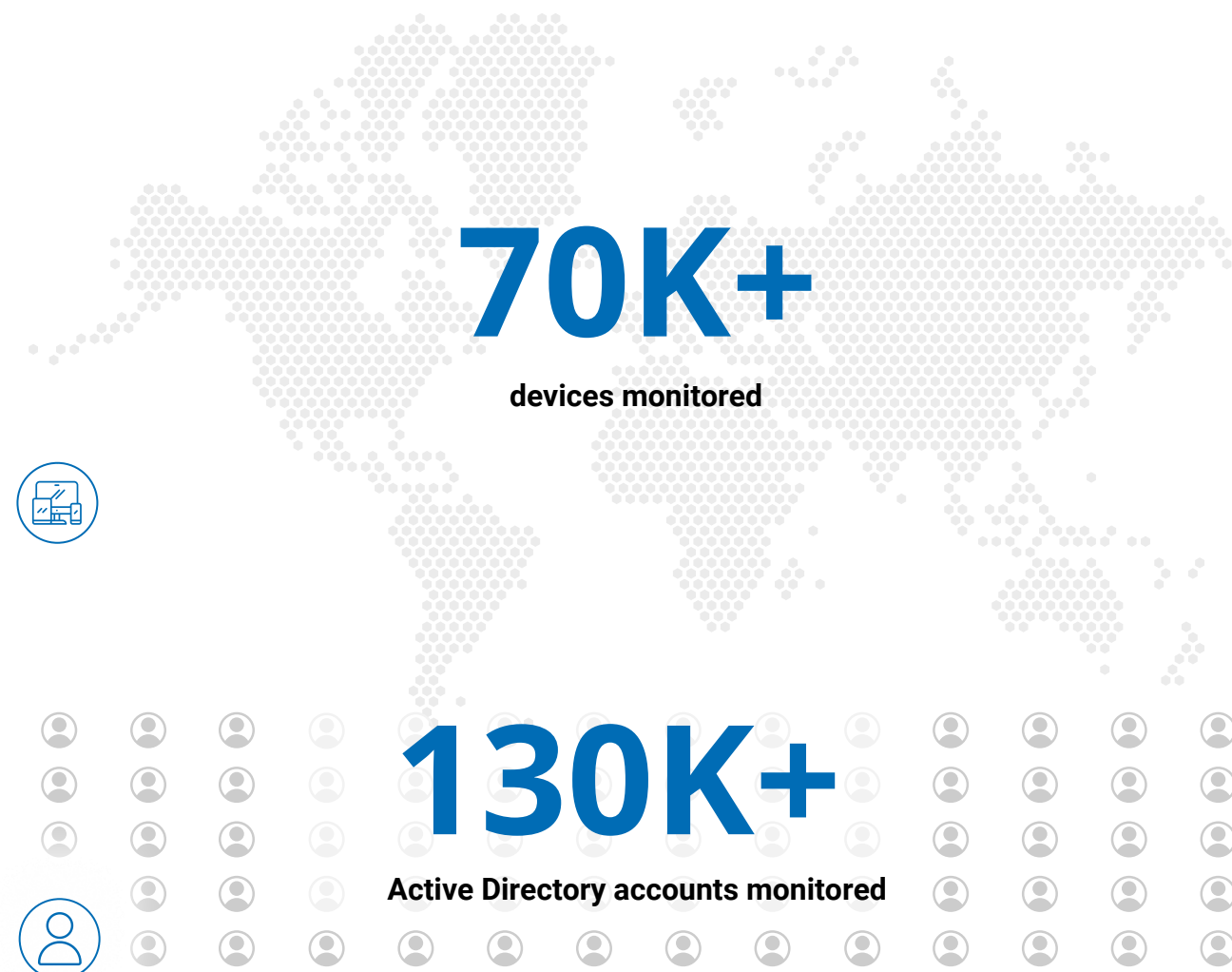
UNICC Threat Detection and Response teams support UNICC’s greater mission of technology delivery for all its partners. UNICC also relies on the Common Secure Cyber Threat Intelligence (CTI) team to aid the United Nations with situational awareness and advance warning of new cybersecurity threats, incidents and challenges.

Thanks to proactive communication with the various UN agencies, the CTI team promptly shared dozens of alerts and actionable intelligence reports to the impacted entities and to the entire Common Secure Threat Intelligence community.

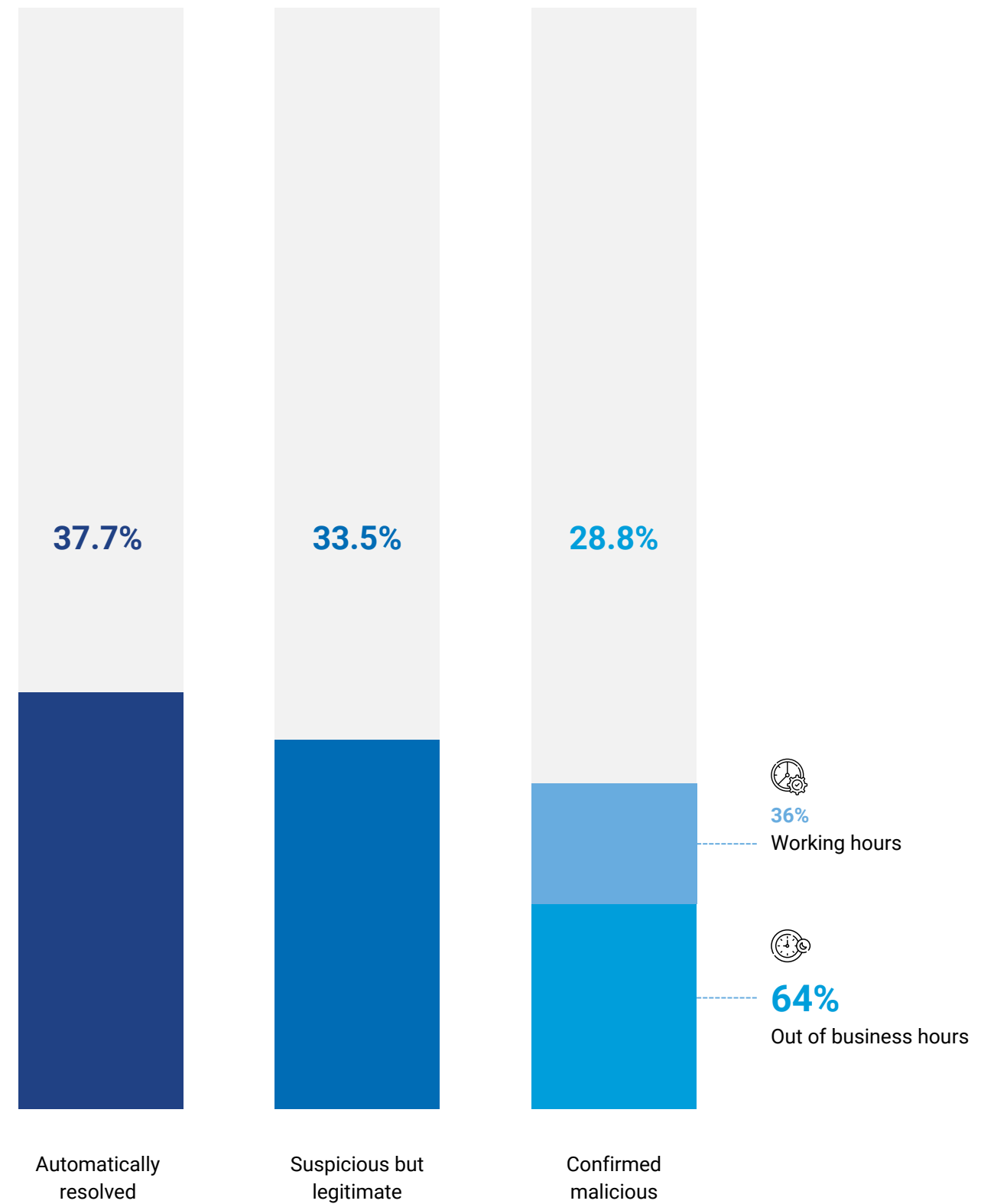
Cyberattacks Overview

In 2022, UNICC's cybersecurity teams responded to a large number of cyberattacks across multiple UN agencies. The collective analysis of these incidents empowered the **United Nations to operate as a united front** to address cyberthreats, harnessing the collective insights gained by UNICC from all subscribing agencies. The cybersecurity division worked confidentially with victim agencies to address the attacks.

UNICC Threat Detection and Response teams used automated and manual means to conduct thorough analysis on events. Agencies impacted by security incidents that had 24x7 detection capabilities in place needed shorter periods to contain and resolve the security incidents versus the ones that did not have 24x7 monitoring capabilities implemented.



UNICC global monitoring volumes in 2022

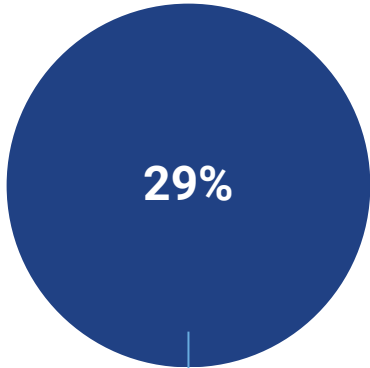



Cyberattack Vectors

Attacks on UN agencies are increasing in frequency and severity. Some of these attacks are being conducted by advanced actors. UN agencies need to learn from these incidents and apply mitigation steps to address these attacks.

The major cyberattacks against the different UN agencies detected by the Common CTI team and managed by the UNICC CSIRT team were initiated through **four common attack paths**. UNICC conducted extensive analysis on the initial vector of attack against UN agencies.

Phishing

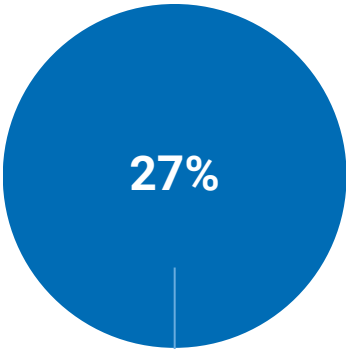




Phishing was one of the top attack vectors. Major cyberattacks could have been prevented if users were better trained to spot and respond to malicious emails.

A widely used phishing scheme involved Microsoft 365-like pages with session cookies to bypass multi-factor authentication processes. The team also found malicious domains that looked like UN agency ones in order to trick victims into providing credentials or personal information.

Another scheme involved domains mimicking UN agencies in malicious email threads for espionage purposes.

Valid credentials

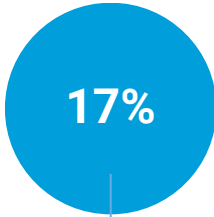




Credential stuffing, password spraying and buying credentials on the underground markets are all methods for misappropriation of accounts. UNICC monitors underground communities for UN system stolen credentials to alert affected organizations and prevent further fraud or advanced attacks.

In an attack analyzed by the UNICC CSIRT, after the initial foothold was established, a threat actor used password spraying as a technique to gain unauthorized access to the internal network of a UN agency. Inside the network, the threat actor performed internal discovery activities to plan further actions.

The UN agency's security controls were able to detect the attack and the discovery actions. The threat actor was contained by tracing back and blocking the malicious communications channels. The incident was remediated and the exploited weaknesses mitigated.

External remote access services





In 2022, a number of high-profile vulnerabilities were identified in remote access services that allowed attackers extraordinary access to systems. Once an attacker gains access to a network, they can carry out further malicious activities, such as data theft, system compromise and disruption of operations.



In one of the attacks analyzed by the UNICC team, an advanced threat actor gained access to a UN workstation, leveraging a remote access service and the previously stolen user's credentials. Once in control, the threat actor used stealthy techniques like a custom backdoor to perform malicious activities. Additionally, multiple techniques were used to prevent host reboot.

To monitor user actions and collect data, a threat actor used malicious browser extensions and an efficient keylogger. The group was able to exfiltrate confidential data, including sensitive information related to ongoing operations. The CTI and CSIRT teams contained and remediated the attack.

Unattributed



Public-facing applications

Cyberattacks against vulnerabilities in public-facing applications target weaknesses in applications that are accessible to the public through the internet. The attacker may take advantage of known vulnerabilities to execute malicious actions, such as data theft or system compromise.

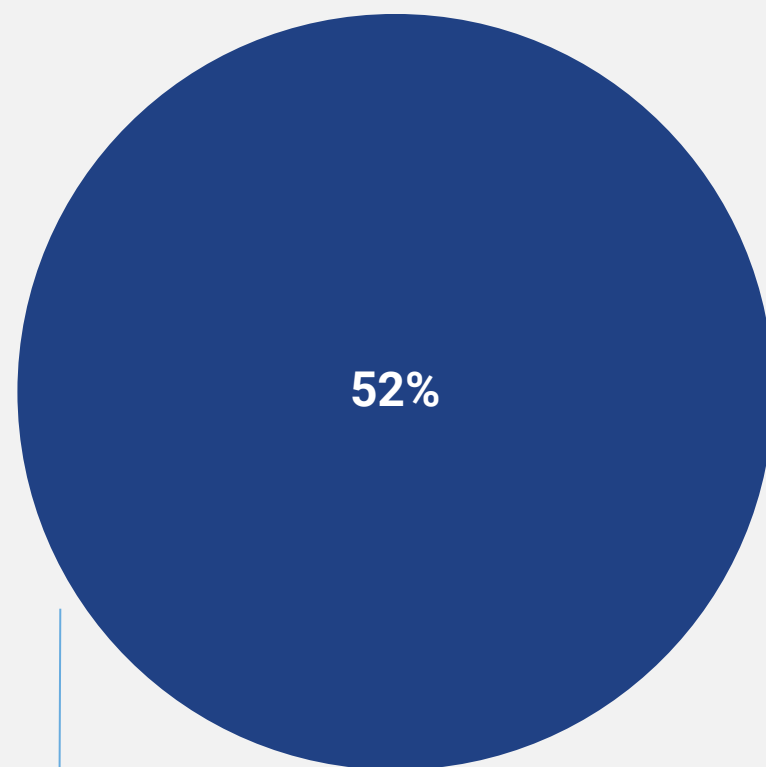
The UNICC team analyzed an attack where a sophisticated threat actor targeted a UN agency to conduct financially-motivated cybercrime operations. During threat hunting activities performed by UNICC, the compromised service was identified, contained and remediated. The impacted agency could have suffered reputational and financial damage.

Cyberthreat Categories

UNICC's cybersecurity team has been able to identify multiple cyberthreat categories impacting different UN agencies.

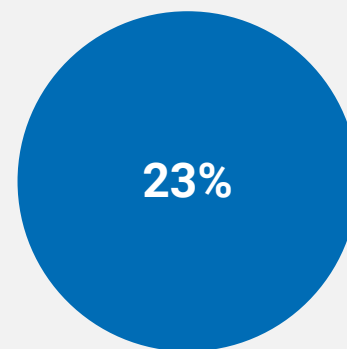
Cyberthreats range **from opportunistic individuals to highly sophisticated groups** leveraging advanced attack techniques. Based on the intelligence gathered by UNICC and the attacks analyzed by its teams, four cyberthreat categories have been defined based on actors' goals.

Advanced threat actors



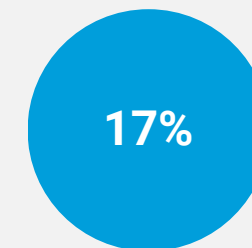
Advanced threat actors are highly skilled individuals or groups who use sophisticated techniques and tools to carry out cyberattacks. They often have specific targets in mind and have the capabilities to evade traditional security measures.

Cybercrime



Cybercrime threat actors are individuals or groups who engage in illegal activities using digital means. They use various techniques to steal sensitive information, disrupt systems or extort money.

Opportunistic



Opportunistic threat actors are individuals or groups who take advantage of vulnerabilities or misconfigurations in computer systems or networks to gain unauthorized access or perform malicious activities. These actors may not have a specific target in mind, but rather exploit any opportunity they come across to gain access to sensitive information or disrupt systems.

Unattributed



Advanced Threat Actors

Given UNICC’s visibility and data telemetry, the Common Secure Cyber Threat Intelligence team identified clusters of malicious activity, sophisticated advanced threat actors that were **targeting more than one organization simultaneously**. UNICC has categorized the most relevant advanced actors (with UNICC assigned internal code names) discovered and tracked during 2022.

Name	Years operating	Goal	Details	Targets							
				UN Orgs.	Govt.	NGOs	Private sector	Public Sector	Spec.	Think tanks	
VEGA	5+ years	Cyberespionage Intellectual property theft	The primary tactic of Vega is sending phishing emails with malicious attachments. Usually this group uses its own custom backdoor and compromises sites to use them as a proxy for remote command and control. The backdoor is a first-stage malware and the actor usually uploads additional tools after its installation. This threat actor also has the ability to quickly modify its techniques and tools based on its goals.	●	●		●				
ECLIPSE	10+ years	Intelligence collection	Eclipse employs common social engineering tactics, phishing and watering hole attacks to exfiltrate desired information from victims. Watering hole attacks are an advanced strategy where the attacker guesses or observes which websites an organization often uses and infects one or more of the websites with malware. Eclipse has lately expanded its geographic reach.	●	●					●	●
SIREN	Several years	Cyberespionage Intellectual property theft	Siren uses multiple custom malware and unique infection chains to perform their cyber espionage and intellectual property theft operations.	●	●	●					
VORTEX	4+ years	Information exfiltration Intelligence collection	Vortex’s activity has been varied using custom components written in different programming languages as well as tools bought from a Malware-as-a-Service provider. The group used highly targeted phishing operations with a focus on the FinTech market and a UN organization.	●			●	●			
HYPERION	2+ years	Information theft Ransomware activity	Hyperion uses a worm that is often installed via USB drives. Its activity cluster relies on legitimate Microsoft tools to call out to its infrastructure, often compromised public devices, using encrypted web requests that contain the victim’s user data. This threat has also been observed to use TOR exit nodes as additional command and control infrastructure. After an initial infection, the attacker follows on with interactive commands activities for cybercrime purposes like reselling access to the compromised host or initiating a ransomware operation.	●			●	●			
ELYSIUM	1+ years	Malware infection Information theft Ransomware activity	Elysium modifies its victims' computer settings and redirects user traffic. The malware is introduced via an ISO file that baits users into executing it. Elysium uses administrative tools to inject itself into the victim's computer's browser and adds a malicious browser extension. The malware allows the attacker to exfiltrate data from the user's browser sessions. The malware boasted a wide range of variants that have been discovered in the wild over the last few months.	●			●	●			

The Way Forward



2022 UNICC Common Secure Conference in Valencia, Spain
Photo: UNICC

UN agencies are under constant attack by cyberadversaries. In 2022, UNICC managed a number of incidents perpetrated by advanced actors seeking to steal information for a variety of reasons. The tactics used to attack UN agencies varied in sophistication from simple phishing attacks to exploiting perimeter vulnerabilities.

UN agencies must remain vigilant. In the coming years the threat landscape will evolve with attackers using Artificial Intelligence and quantum computing. Network defense will become more complicated. Collaborating and sharing experiences leveraging common cybersecurity capabilities will strengthen the UN system as a whole.

In addition to the ongoing initiatives related to cybersecurity in each UN agency, UNICC identifies the following four areas that would limit the likelihood of occurrence of the major cybersecurity incidents.

1 Threat intelligence-driven cybersecurity operations capabilities

Organizations should continue to collaborate and share threat intelligence with each other as this allows early detection of advanced threats. Agencies should also direct their cybersecurity operations initiatives with a threat intelligence-driven approach.

2 Continuous monitoring

As observed during 2022, most cyberattacks analyzed were performed during out-of-business hours. In some cases, this allowed threat actors to perform activities that went undetected until deep investigation was performed. Adopting a continuous monitoring capability will allow agencies to detect, respond and remediate cyberthreats in early stages of the cyberattack.

3 Prompt remediation of vulnerabilities and secure hardening

Most security incidents observed during 2022 leveraged exploitation of vulnerabilities on Internet exposed services. Prioritizing the vulnerability management programme to remediate vulnerabilities and implement hardening best practices on services exposed to the internet will significantly reduce the likelihood of cyberattacks to become successful.

4 User awareness programs

Unaware users represent a significant initial threat attack vector. Although technologies mitigate attacks targeting users, it is still essential to adopt and follow comprehensive user awareness programs to ensure that users become active participants in the defense of their organizations.



UNICC

www.unicc.org

TLP: CLEAR