Business Internet Security Report

6th edition, 2023-2024

orange™ Business

Contents

As we approach the end of 2023, we look at was has been a challenging year marked by global economic and social tensions, but also with excitement and hope for the next year, where the amazing advances in technology promise to revolutionize the way we work, live, and interact.

In this ever-changing landscape of technology, there were few topics that captured the attention of the media, business, and the general public as the rise of generative AI and the growing number and complexity of cyberattacks. Not surprisingly, in many cases the two topics are found in the same sentence as we are faced with a growing number of deep fakes and AI-enabled misinformation, alongside an escalating surge in cyber threats such as ransomware, malware, phishing and DDoS attacks.

Fortunately, AI is also part of cyber security solutions, facilitating a better data management, and better solutions and reports for companies. In recent years, cybersecurity and risk management have become a strategic priority for both the private and public sector. In this regard Orange Business is a trusted partner and a top provider of security services focused on tailored solutions adapted to customer's needs. This means having the support and expertise of the dedicated teams of Orange experts and access to a wide array of high-quality services and innovative solutions, all backed up by the best network infrastructure in Romania.

Supporting education and constantly investing in research and innovation are just as important for reducing cyber threats and protecting personal and business data. That is why, in 2023 we continued to expand our partnerships with universities across the country, in addition to joining new collaborations on EU research and innovation programs, all with the aim to grow the next generation of professionals in this field. Programs such as UNbreakable, the most important Capture-The-Flag competition in Romania, or the Romanian Cyber Security Challenge National Competition are great examples of how we can support the next generation of cyber-security experts. Moreover, the partnerships and collaborations we have with startups through programs such as Orange Fab, are key for the development of new technologies, business, and cyber security solutions in Romania.

Our annual Business Internet Security Report offers a holistic overview of the main cybersecurity threats, the challenges of the past year as well as predictions for 2024. I hope it will give you a new perspective on the importance of cybersecurity and contribute to the growth of your business.

Julien Ducarroz
Chief Executive Officer, Orange Romania

1. The State of Cybersecurity in 2023 A Year in Review

In the ever-evolving landscape of technology, 2023 has proven to be a year marked by substantial advancements and ongoing challenges in the realm of cybersecurity. As the digital frontier expands, so do the opportunities for cybercriminals to exploit vulnerabilities, leading to a persistent cat-and-mouse game. As an introductory piece, this is meant to review the status of cybersecurity in 2023, shedding light on the technical intricacies, known vulnerabilities, and notable cyberattacks that have unfolded so far.

Cybersecurity professionals worldwide are contending with a rapidly evolving threat landscape. In 2023, some vulnerabilities that have come to the forefront are notable due to their widespread impact. One such vulnerability is the "Log4Shell" bug, which emerged as a major concern in late 2022 and continued to wreak havoc in 2023.

This critical vulnerability in the Apache Logging Services (Log4j) library allowed attackers to execute arbitrary code remotely, affecting a wide range of applications and systems. The fallout from Log4Shell serves as a stark reminder of the potential damage that can be wrought by single-point vulnerabilities in widely used software.

Zero-Day Vulnerabilities: The Silent Assassins

In the world of cybersecurity, zero-day vulnerabilities remain a constant thorn in the side of defenders. Zero-days are previously unknown vulnerabilities that hackers can exploit before software vendors can release patches to fix them. In 2023, several zero-day vulnerabilities have come to the fore, emphasizing the need for swift and efficient defence.

One prominent zero-day case was the "SpecterScript" exploit, which affected popular web browsers. SpecterScript allowed attackers to execute malicious scripts on web pages and extract sensitive information, jeopardizing user privacy. Although browser vendors promptly addressed the issue, these zero-days served as a reminder of the ongoing battle against advanced threat actors.

Noteworthy zero-day exploits, targeted critical infrastructure systems. Such exploits targeted previously unknown vulnerabilities in the industrial control systems (ICS) of power plants, and “above the red line” IT systems, providing access and persistency to the threat actors, making it a matter of extreme concern. Such incidents prompted governments and cybersecurity agencies to collaborate closely to address vulnerabilities in critical infrastructure and bolster defences.

Ransomware: The Ongoing Saga

The ransomware menace continues to evolve and plague organizations, large and small, in 2023. Despite concerted efforts to combat ransomware, attackers continue to find new avenues to exploit. The "LockBit" ransomware gang, for instance, has become notorious for its innovative tactics. Rather than merely encrypting files and demanding a ransom, LockBit engages in double extortion, stealing sensitive data and threatening to release it if the ransom isn't paid. This new approach adds an extra layer of complexity to the already challenging task of mitigating ransomware attacks.

Notably, the healthcare sector bore the brunt of several ransomware attacks in 2023, as data is becoming available at Global and Local (national) levels. These incidents had real-life consequences, with hospitals and clinics struggling to provide care during these attacks. Hospitals across the Globe faced crippling ransomware attacks in 2023, prompting critical discussions about the need for robust cybersecurity measures in the healthcare industry.

The financial sector was not immune to ransomware attacks either. In the span of the last 12 months, cyber criminals have stolen more than 3.2 billion USD worth of cryptocurrency, through more than 60 separate incidents. These incidents served as a stark reminder of the challenges associated with securing digital currencies, which often act as attractive targets for attackers due to their anonymity and decentralized nature.

The Rise of AI in Cybersecurity

To combat the ever-evolving threats in 2023, cybersecurity professionals have increasingly turned to artificial intelligence (AI) and machine learning. AI-powered security solutions have proven invaluable in identifying and mitigating threats in real-time. By analysing vast datasets and identifying patterns, AI can help predict and prevent cyberattacks.

One notable AI-powered category of cyber security tools is Machine-Learning enabled threat intelligence. The tools in this category will use advanced M.L. to monitor and search for unusual network behaviour in real-time, allowing them to thwart the attack before any damage occurred.

The Human Element

While technology and AI play pivotal roles in cybersecurity, the human element remains a critical factor. Phishing attacks, for instance, continue to target human vulnerabilities, preying on trust and curiosity. Social engineering tactics remain a favoured entry point for cybercriminals.

In 2023, a notable incident involved the "CryptoPhish" campaign, which impersonated cryptocurrency exchange platforms to trick users into revealing their login credentials and private keys. Despite advancements in AI, education and awareness among users are essential to prevent such attacks. Security professionals have intensified efforts to educate individuals about the dangers of phishing and the importance of maintaining a security-conscious mindset.

The Expanding Attack Surface

As the world becomes more interconnected, the attack surface for cybercriminals expands. The proliferation of Internet of Things (IoT) devices and the integration of smart technology into our homes, cities, and industries have opened new opportunities for hackers. The "IoT-botnet" attack in August 2023 demonstrated the vulnerability of interconnected devices. Hackers used a network of compromised IoT devices to launch a massive Distributed Denial of Service (DDoS) attack, temporarily disrupting major internet services.
This incident underscores the urgent need for improved security standards in IoT devices.

Additionally, as quantum computing inches closer to becoming a reality, cybersecurity faces a potential game-changer. Quantum computers have the potential to break widely used encryption methods, threatening data security on a global scale. Cybersecurity experts and cryptographic researchers are working diligently to develop post-quantum cryptography solutions that can withstand the power of quantum computing.
It is within this reason that Orange Romania salutes and fully supports the development of a National Strategy on Quantum-Secure Communications, and is part of the ongoing process of consulting with strategic partners in the private and public sector, under the goal of delivering a comprehensive, strategic path forward to answering future threats to our State-Of-The-Art Cryptography.

In hindsight

The year has brought to light the critical role of governments and international organizations in fostering collaboration and setting global standards for cybersecurity. The expansion of the attack surface through IoT and the looming threat of quantum computing underline the importance of constant innovation in security practices and technology.

As we move forward, the lessons learned in 2023 will shape the future of cybersecurity, emphasizing the need for vigilance, education, and the continuous improvement of security measures.

In this ongoing cyber saga, it's essential to remember that the threat landscape will continue to shift and adapt, but so will our defences, driven by the relentless pursuit of a more secure digital world. Stay vigilant, stay informed, and stay secure.

2. Malware 2.0 – The Current State of Ransomware

Ransomware attacks have evolved into one of the most menacing threats in the cybersecurity landscape. These malicious acts involve encrypting a victim's data and demanding a ransom for its decryption key, and they have become increasingly sophisticated and targeted. We've discussed extensively this phenomenon, in previous editions of our Business Internet Security Reports, yet we consider this topic to be of utmost importance and of increasing urgency, as many enterprises, SMEs and Government Institutions are faced with overwhelming crypto attacks, that can cripple their infrastructures.

As you can read about in our "Findings" section, the state of ransomware in our Local (National) context shows that these attacks have gained new grounds and increased in volume and impact, with more than 35% of all registered and blocked threats across our BIS Infrastructures, are of the crypto malware.

Anatomy of a Ransomware Attack

Understanding the anatomy of a ransomware attack is crucial for devising effective defence strategies. Ransomware typically follows a sequence of steps:

- **Infection Vector:** Ransomware can infiltrate a system through various means, including malicious email attachments, compromised websites, and vulnerable software. Attackers may also use phishing emails to trick users into executing the malware.
- **Execution:** Once on a victim's system, the ransomware is executed, initiating the encryption process. Some ransomware strains have been engineered to lie dormant for a specific period, making detection more challenging.
- **Encryption:** Ransomware encrypts files on the victim's system, rendering them inaccessible. Advanced encryption algorithms, such as RSA and AES, are often employed to secure the data.
- **Ransom Note:** After encryption, the victim receives a ransom note, which contains instructions on how to pay the ransom. Payment is typically demanded in cryptocurrency to maintain anonymity.
- **Payment Portal:** Ransomware operators usually provide a payment portal accessible via the Tor network, further obfuscating their identity. Victims can enter the decryption key provided upon payment to recover their files.
- **Decryption:** Upon receiving the ransom, attackers send a decryption key to the victim. Victims then use this key to decrypt their files, provided the attackers keep their end of the bargain.

The Evolution of Ransomware

Ransomware attacks have evolved significantly over the years, becoming more sophisticated and financially motivated. Below are some noteworthy trends in the evolution of ransomware:

- Ransomware-as-a-Service (RaaS) - Ransomware-as-a-Service platforms have emerged, allowing even those with limited technical expertise to launch ransomware attacks. These platforms provide malware, payment infrastructure, and sometimes even customer support, making ransomware more accessible to a broader range of cybercriminals.
- Double Extortion - A notable development in recent ransomware attacks is the double extortion tactic. Attackers not only encrypt the victim's data but also exfiltrate sensitive information. They threaten to release this data publicly if the ransom is not paid, adding a layer of pressure on victims.

- Targeted Ransomware - Rather than using a spray-and-pray approach, modern ransomware attacks are often highly targeted. Attackers conduct thorough reconnaissance to identify high-value targets and tailor their attacks to maximize the chances of receiving a substantial ransom.

Notable Ransomware Strains and Attacks

- **Ryuk** - Ryuk ransomware has been active for several years and remains a potent threat. It is known for targeting large organizations, often in the healthcare and financial sectors. Ryuk's technical sophistication lies in its ability to propagate laterally within a network, compromising numerous endpoints and encrypting vast amounts of data.
- **Conti** - Conti is another prominent ransomware strain that has gained notoriety for its double extortion tactics. It often begins with a high-privilege user's compromise and spreads laterally through the network, encrypting data and exfiltrating sensitive information. The attackers behind Conti have demonstrated a deep understanding of Active Directory environments, making detection and recovery challenging.
- **DarkSide** - The DarkSide ransomware group garnered international attention following the Colonial Pipeline attack in May 2021. DarkSide adopts a professional approach, offering a "code of conduct" for affiliates and vowing not to target critical infrastructure. This incident emphasized the cross-border nature of ransomware threats and their potential impact on critical services.

Defensive Strategies

To counter the ransomware threat, organizations and individuals must employ a multi-faceted defensive approach. Some key strategies include:

- **Backup and Recovery:** Regular backups of critical data, stored offline, can be a lifeline in the event of a ransomware attack
- **Security Patching:** Keeping software and systems up to date with security patches helps close known vulnerabilities that ransomware may exploit
- **Email Security:** Deploying robust email security solutions can help prevent phishing emails and malicious attachments from reaching users
- **Network Segmentation:** Isolating critical systems from the broader network can help contain ransomware's lateral movement
- **Behaviour-Based Detection:** Using advanced security solutions that analyse user and system behaviour can help identify ransomware activity
- **User Training:** Educating users about phishing and social engineering tactics is crucial in preventing infection
- **Threat Intelligence:** Staying informed about the latest ransomware threats and tactics is essential for proactive defence

The Legal and Ethical Quandary

As ransomware attacks continue to cause significant financial and operational disruptions, governments worldwide have taken steps to address the issue. This includes imposing strict regulations on cryptocurrency transactions and developing international agreements to tackle cybercrime.

However, the ethical quandary surrounding ransom payments remains unresolved. Paying ransoms can fund criminal activities, but for many victims, it remains the most viable option for recovering their data.

Ransomware attacks have become increasingly complex and targeted, posing a significant threat to organizations and individuals alike. Understanding the technical aspects of these attacks is essential for devising effective defensive strategies. The evolution of ransomware, from the emergence of RaaS platforms to the adoption of double extortion tactics, highlights the need for vigilance and robust security measures.

Defending against ransomware requires a multi-faceted approach, including regular backups, security patching, email security, and user training. While governments and international organizations work to address the issue at a legal and diplomatic level, the ethical debate surrounding ransom payments remains a challenging aspect of combating this pervasive threat. In this ongoing battle against ransomware, a combination of technical defences and a coordinated global effort is essential to mitigate the impact of these insidious attacks.

3. A Deep Dive into DDoS Attacks

Distributed Denial of Service (DDoS) attacks represent a persistent and escalating threat to businesses, including large enterprises, SMEs, and Public Sector Entities. These attacks disrupt online services, rendering them unavailable to legitimate users. Although a constant in our previous reporting we are yet to present a deep dive into the intricacies of DDoS attacks. Let's delve into the technical details of DDoS attacks, explore various types, and examine their impact on businesses, with historical examples for reference.

The Anatomy of DDoS Attacks

DDoS attacks aim to overwhelm a target's resources, such as servers, networks, or applications, by flooding them with a high volume of traffic. The attack traffic typically originates from multiple sources, making it difficult to mitigate. Understanding the anatomy of DDoS attacks is crucial for comprehending their various forms:

- **Botnets:** DDoS attacks leverage botnets, which are networks of compromised devices, often infected with malware. Attackers control these devices remotely, using them to generate and direct malicious traffic to the target.
- **Traffic Amplification:** Some DDoS attacks exploit vulnerable protocols, such as DNS (Domain Name System) and NTP (Network Time Protocol), to amplify the attack traffic. Attackers send small requests that generate much larger responses, magnifying the impact of the attack.
- **Attack Vectors:** DDoS attacks employ different vectors, including volumetric attacks (overwhelming the target's bandwidth), protocol attacks (targeting network protocols), and application layer attacks (overloading web servers or applications)

To defend against Distributed Denial of Service (DDoS) attacks effectively, it's vital to delve deeper into the technical aspects of various DDoS attack types and to explore the technical nuances of the most prevalent DDoS attack vectors.

UDP Flood Attacks

UDP (User Datagram Protocol) flood attacks aim to overwhelm a target's network or service by inundating it with a high volume of UDP packets. Unlike TCP, UDP is a connectionless protocol, making it easier for attackers to exploit. The primary challenge in mitigating UDP floods is distinguishing legitimate traffic from malicious packets.
In a UDP flood, attackers typically forge the source IP addresses, which makes it harder to identify the origin of the attack.
This attack vector can be further divided into:

- **Simple UDP Flood:** Attackers send a vast number of UDP packets to a target, saturating its network bandwidth and resources. While simple, it can be highly effective due to its sheer volume.
- **DNS Amplification:** In DNS amplification attacks, attackers send small DNS queries with spoofed source addresses to open DNS resolvers. These resolvers, in turn, send larger DNS responses to the victim. The amplification factor can be 50 times the original request.
- **NTP Amplification:** Like DNS amplification, Network Time Protocol (NTP) amplification attacks exploit vulnerable NTP servers to amplify traffic. Attackers send small NTP requests, and the servers respond with significantly larger packets.

TCP SYN/ACK Flood Attacks

TCP SYN/ACK (Synchronization and Acknowledgment) flood attacks exploit the TCP three-way handshake process. In this attack, the attacker sends many SYN requests to the target server, but the attacker does not complete the handshake by sending the final ACK packet.

This flood of uncompleted handshake requests can quickly exhaust the target's resources, preventing legitimate users from establishing connections.

The attacker's ability to generate a high volume of SYN requests and the target's finite capacity to handle these incomplete connections make this type of attack effective.

HTTP/HTTPS Application Layer Attacks

HTTP/HTTPS-based DDoS attacks focus on the application layer, which is the most challenging to defend against due to its intricacy. Attackers use a range of tactics to overload web servers or application resources.
Key characteristics of HTTP/HTTPS DDoS attacks include:

- **High Request Rate:** Attackers send a massive number of HTTP/HTTPS requests in a short period, effectively saturating the target's resources
- **Mimicking Legitimate User Behaviour:** Some advanced attackers mimic user behaviour, such as browsing a website, adding items to a shopping cart, and submitting forms, making it harder to distinguish between legitimate and malicious traffic
- **Session Flooding:** Attackers flood a target's web server with session requests, aiming to exhaust server resources and prevent new users from establishing sessions
- **Slowloris Attack:** A Slowloris attack involves sending partial HTTP requests, keeping them open for as long as possible. This consumes server resources as it maintains numerous open connections.

SSL/TLS Attacks

SSL/TLS (Secure Sockets Layer/Transport Layer Security) attacks target the encryption layer of web services. These attacks exploit the resource-intensive nature of SSL/TLS handshakes.
Technical details of SSL/TLS DDoS attacks include:

- **SSL/TLS Handshake Exhaustion:** Attackers initiate numerous SSL/TLS handshakes but abandon them before completion, exhausting the target's computational resources
- **Renegotiation Attacks:** In a renegotiation attack, attackers repeatedly request renegotiation of the SSL/TLS session. This places a heavy computational load on the server, impacting its ability to handle legitimate requests.
- **Cipher Suite Attacks:** Attackers may exploit vulnerabilities in specific cipher suites or SSL/TLS versions to flood the server with handshake requests, causing resource exhaustion
- **SSL/TLS Layer Encryption Attacks:** Attackers may target the actual encryption layer, exploiting vulnerabilities in encryption algorithms to disrupt SSL/TLS-protected communication

Application Layer Attacks Beyond HTTP/HTTPS

Beyond traditional web services, application layer attacks extend to other protocols and services, including:

- **SMTP Flooding:** Attackers flood email servers with a high volume of email requests, potentially leading to resource exhaustion or mail service disruption
- **VOIP DDoS Attacks:** Voice over Internet Protocol (VoIP) services can be targeted with call flooding, where attackers flood the service with bogus calls, rendering it unusable
- **Gaming Server Attacks:** Online gaming servers are vulnerable to DDoS attacks that disrupt multiplayer games, exploiting vulnerabilities in game protocols or server capacity
- **API Attacks:** With the growing prevalence of API-driven applications, attackers may target APIs with high volumes of bogus requests to disrupt data retrieval and application functionality

Impact on Businesses

DDoS attacks can have severe repercussions for large enterprises, both in terms of financial losses and reputational damage:

- **Financial Losses:** Downtime caused by DDoS attacks can lead to significant financial losses. Large enterprises may lose revenue, face service-level agreement (SLA) penalties, and incur additional costs for mitigation and recovery.
- **Reputation Damage:** Prolonged service interruptions harm a company's reputation. Customers may lose trust, and brand damage can have long-lasting effects. DDoS attacks can also expose security weaknesses, further undermining an organization's image.
- **Operational Disruption:** DDoS attacks disrupt critical business operations, affecting employee productivity and customer service. Recovery efforts divert resources from strategic initiatives, impacting the enterprise's competitiveness.
- **Data Breach Risk:** DDoS attacks may serve as a smokescreen for data breaches. When IT and security teams are focused on mitigating the DDoS attack, attackers may exploit vulnerabilities to steal sensitive data.

Historical Examples

- **Dyn Attack (2016):** In October 2016, a massive DDoS attack targeted Dyn, a prominent DNS provider. The attack impacted numerous large enterprises, including X, Reddit, and Netflix. The Mirai botnet, composed of compromised IoT devices, was used to generate an enormous volume of traffic, highlighting the risk posed by insecure Internet of Things devices.

- **GitHub Attack (2018):** In February 2018, GitHub experienced a significant DDoS attack that peaked at 1.35 Tbps. The attack exploited Memcached servers, which amplified the traffic directed at GitHub's services. GitHub quickly mitigated the attack by temporarily disabling certain features.

Defence and Mitigation

Mitigating DDoS attacks requires a multi-pronged strategy:

- **Traffic Scrubbing:** Deploying traffic scrubbing services can filter out malicious traffic before it reaches the target. Providers like Cloudflare and Akamai offer these services.
- **Anomaly Detection:** Implementing anomaly detection systems can identify abnormal traffic patterns and trigger automatic mitigation measures
- **Content Delivery Networks (CDNs):** CDNs distribute traffic across multiple data centres, reducing the impact of DDoS attacks on a single location
- **Load Balancing:** Load balancers distribute incoming traffic across multiple servers, preventing any single server from being overwhelmed
- **Web Application Firewalls (WAFs):** WAFs can protect web applications from application layer DDoS attacks by inspecting and filtering traffic

DDoS attacks continue to pose a significant threat to large enterprises, causing financial losses, reputational damage, and operational disruptions. Understanding the types of DDoS attacks, their technical intricacies, and the historical examples of major attacks is crucial for organizations to implement effective defences.

As the threat landscape evolves, enterprises must continually update and refine their DDoS mitigation strategies to stay ahead of attackers. Effective protection against DDoS attacks requires a combination of technical solutions, early detection, and proactive measures to safeguard business continuity and reputation in the face of this ever-present threat.

4. Controlling the Industrial Control Systems An Overview of Threats to ICS

Industrial Control Systems (ICS) are computer-based systems that monitor and control industrial processes, such as those used in power grids, water and wastewater systems, transportation systems, and manufacturing facilities. ICS are essential to the operation of modern infrastructure and industry, but they are also increasingly vulnerable to cyber threats.

Cyber attackers can target ICS for a variety of reasons, including:

- To disrupt operations and cause economic damage
- To steal intellectual property or trade secrets
- To gain access to critical infrastructure and cause widespread damage
- To launch attacks against other targets using ICS as a staging ground

ICS are particularly vulnerable to cyber-attack because they are often complex and interconnected, and they may use outdated or legacy systems. Additionally, ICS are often located in remote or inaccessible locations, making them difficult to physically protect.

Types of Cyber Threats Against ICS

There are a variety of cyber threats that can target ICS, including:

- Malware can be used to disrupt or disable ICS operations, steal data, or gain unauthorized access to systems. Some examples of malware that have been used to target ICS include Stuxnet,Triton, and Industroyer.
- Denial-of-service (DoS) attacks: DoS attacks overwhelm ICS systems with traffic, making them unavailable to legitimate users. DoS attacks can be used to disrupt operations or cause economic damage.
- Man-in-the-Middle (MitM) attacks: MitM attacks allow attackers to intercept and modify communications between ICS devices. This can be used to steal data or issue malicious commands to systems.
- Supply chain attacks: Supply chain attacks target software or hardware suppliers to ICS operators. By compromising a supplier, attackers can gain access to ICS networks and systems.
- Social engineering attacks: Social engineering attacks trick people into revealing confidential information or performing actions that compromise ICS security

Examples of Cyber Attacks Against ICS

There have been several high-profile cyber-attacks against ICS in recent years, including:

- Stuxnet: a sophisticated malware attack that targeted Iranian nuclear facilities. Stuxnet caused significant damage to the Iranian nuclear programme and is one of the most sophisticated cyber-attacks ever launched.
- Triton: a malware attack that targeted a petrochemical plant in Saudi Arabia. Triton caused significant damage to the plant's safety systems, which could have led to a catastrophic explosion.
- Industroyer: a malware attack that targeted the Ukrainian power grid in 2016 and 2017. Industroyer caused widespread power outages in Ukraine and demonstrated the ability of cyber attackers to disrupt critical infrastructure.
- Colonial Pipeline ransomware attack: In 2021, the Colonial Pipeline, which supplies gasoline and other fuels to the East Coast of the United States, was hit by a ransomware attack. The attack caused the pipeline to be shut down for several days, leading to widespread fuel shortages.

Cyber-attacks on ICS can have a devastating impact on critical infrastructure and industry. Cyber-attacks can disrupt operations, cause economic damage, and even lead to loss of life.

Considering a cyber-attack on the power grid could

cause widespread blackouts, disrupting communications, transportation, and other essential services. A cyber-attack on a water treatment facility could contaminate the drinking water supply, leading to illness or death. And a cyber-attack on a manufacturing facility could cause product recalls or even shut down the facility altogether.

Mitigating Cyber Threats to ICS

There are several steps that organizations can take to mitigate cyber threats to ICS, including:

- Segmenting ICS networks into separate zones can help to contain the spread of malware and other cyber-attacks
- Implementing network security controls such as firewalls and intrusion detection systems, can help to protect ICS networks from unauthorized access and malicious traffic
- Keeping software and hardware up to date with the latest security patches. Software and hardware vulnerabilities can be exploited by attackers to gain access to ICS systems.
- Implementing security awareness training that can help employees to identify and avoid social engineering attacks
- Developing and testing incident response plans to ensure that organizations are prepared to respond to cyber-attacks quickly and effectively

Cyber threats to ICS are a serious and growing concern. Widely considered as a clear and present danger, such attacks have the potential to cause widespread disruption of civil services and have a considerable impact on societies. Organizations that operate ICS must take steps to mitigate these threats and protect their critical infrastructure and industry.

5. A Timeline of Events

Through each edition of our Report, we've collected a timeline of events of great importance to the global cyber security context. Major attacks to zero-day exploits, such events will have a sizeable impact on our societies and will largely change paradigms on how businesses and individuals perceive cyber security.

The past 12 months have been riddled with ransomware attacks, new APTs spawning all over the world and a substantial number of zero-day exploits, targeting large-scale infrastructures.

In lieu of editorializing news from reputable sources, our timeline provides the newsworthy title and a reference link to its source.

November 2022:

1. AirAsia hit by ransomware attack, five million passenger and employee data compromised
2. 5.4 million X users' stolen data leaked online — more shared privately
3. Dropbox admits 130 of its private GitHub repos were copied after phishing attack

December 2022:

1. Port of Lisbon website still down as LockBit gang claims cyberattack
2. 130,000 Telstra customers exposed in data breach
3. California authorities confirm cyber intrusion, LockBit claims ransomware hit

January 2023:

1. Attacker leaks 200+ million email addresses of X Users
2. JD Sports hit by cyber-attack that leaked 10m customers' data
3. Hacker Uses API to Access Data on 37 million T-Mobile Users Accounts

February 2023:

1. TruthFinder, Instant Checkmate confirm data breach affecting 20 million customers
2. Teijin Automotive Technologies Files Notice of Data Breach Affecting Over 25k Employees
3. Cyberattack on food giant Dole temporarily shuts down North America production

March 2023:

1. Hitachi Energy Latest Victim of Clop GoAnywhere Attacks
2. ChatGPT Suffers First Data Breach, Exposes Personal Information
3. AT&T alerts 9 million customers of data breach after vendor hack

April 2023:

1. Ransomware Attack at NJ County Police Department Locks Up Criminal Investigative Files
2. United HealthCare reports data breach that may have revealed customers' personal information
3. Big Pharma-partnered Evotec on high alert after cyberattack takes systems offline

May 2023:

1. T-Mobile discloses second data breach since the start of 2023
2. Clinical test data of 2.5 million people stolen from biotech company Enzo Biochem
3. Vehicle data of over 2 million Toyota users been publicly available in Japan since a decade

June 2023:

1. Oregon DMV, Louisiana OMV warn residents of MOVEit data breach
2. More than a million NHS patients' details compromised after cyberattack
3. MOVEIt breach impacts Genworth, CalPERS as data for 3.2 million exposed

July 2023:

1. Video and chatting app leaks more than 100 million user messages
2. 34 million Indonesian Passports Exposed in a Massive Immigration Directorate Data Breach
3. Tampa General Hospital confirms cybersecurity incident; 1.2 million patients being notified

August 2023:

1. Cyber-attack on UK's electoral registers revealed
2. Minister of Health and Population confirmed that the security agencies have dealt with the leak of the personal data of 2 million Egyptian patients which are being sold online
3. Department of Health Care Policy & Financing Provides Notice of a Data Security Incident

September 2023:

1. Ransomware gang Dunghill steals 1.3TB of data from Sabre
2. Hospitality and entertainment company, MGM Resorts, suffered a cyber attack that severely impacted its business operations
3. Ransomware gang steals 6.8TB of data from Save The Children

October 2023:

1. Spanish airline Air Europa hit by credit card system breach
2. 23andMe Claims it wasn't breached despite stolen data

6. The Changing Cybersecurity Landscape

Laurenţiu Popescu, Security Product Manager, has 20+ years of work experience in the IT&C industry with solid background in marketing strategy, market research, competitive analysis, business consulting, lead generation and go-to-market services. Laurenţiu has also extensive experience in the cybersecurity space, with various product management and product marketing functions in leading security vendors.

The cybersecurity landscape has changed substantially in the past years, as threats have become more sophisticated and diverse over the years. Traditional threats such as viruses, malware, and phishing attacks are still present, but they have evolved into more complex and elusive forms of cybersecurity threats. Ransomware attacks, where hackers encrypt a victim's data and demand a ransom for its release, have become increasingly prevalent.

The turbulent economic and political arena, especially following Russia's invasion in Ukraine, has led nation-state actors to engage in cyber-espionage and cyber warfare, aiming to steal sensitive information or disrupt critical infrastructure. Additionally, the rise of the Internet of Things (IoT) has expanded the attack surface, making interconnected devices vulnerable to exploitation.

For example, according to a report released by BlackBerry in Q2, 2023 which analysed the cybersecurity events from March to May 2023, threat actors deployed about 11.5 attacks per minute across all sectors. The healthcare and financial sector were some of the most targeted. This was due to the information these industries hold (bank account information, personally identifiable information (PII) and Social Security numbers) and that is seen as particularly lucrative for hackers because it can be used as blackmail material or for further crimes, such as identity theft.

Moreover, ENISA (The European Union Agency for Cybersecurity) classified the new cybersecurity landscape in 7 threat groups. Frequency and impact determine how prominent all of these threats still are.

Ransomware	60% of affected organizations may have paid ransom demands
Malware	66 disclosures of zero-day vulnerabilities observed in 2022
Social engineering	Phishing remains a popular technique but we see new forms of phishing arising such as spear-phishing, whaling, smishing and vishing
Threats against data	Increasing in proportionally to the total of data produced
Threats against availability	Largest Denial of Service (DDoS) attack ever was launched in Europe in July 2022
Disinformation – misinformation:	Escalating AI-enabled disinformation, deep fakes and disinformation-as-a-service
Supply chain targeting	Third-party incidents account for 17% of the intrusions in 2021 compared to less than 1% in 2020

According to ENISA, the cybersecurity threats landscape will further be shaped by a few main trends such as:

- **Zero-day exploits** are the new resource used by cunning threat actors to achieve their goals
- **A new wave of hacktivism** has been observed since the Russia-Ukraine war
- **DDoS attacks are getting larger and more complex** moving towards mobile networks and Internet of Things (IoT) which are now being used in cyberwarfare
- **AI-enabled disinformation and deep fakes**

However, despite these challenges, the cybersecurity industry is not standing still. Several emerging technologies and strategies are being employed to tackle the evolving threats:

- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML algorithms can analyse vast amounts of data to identify patterns and anomalies, helping in the early detection of potential threats. These technologies can also automate responses, providing a real-time defense against cyber-attacks.
- **Blockchain Technology:** Blockchain, known for its role in securing cryptocurrencies, is finding applications in cybersecurity. It provides a decentralized and tamper-proof way of storing data, making it extremely challenging for cybercriminals to manipulate information or launch attacks.
- **Zero Trust Security Model:** This model operates on the principle of "never trust, always verify." It assumes that threats may exist both outside and inside the network, requiring strict verification for anyone trying to access resources, regardless of their location.
- **Multi-Factor Authentication (MFA):** MFA adds an extra layer of security by requiring users to provide multiple forms of identification before granting access. This can significantly reduce the risk of unauthorized access, even if a password is compromised.
- **Cybersecurity Awareness and Training:** Educating employees and individuals about cybersecurity best practices is crucial. Training programs can help people recognize phishing attempts, avoid suspicious links, and understand the importance of regular software updates.

In conclusion, in today's digital age, where technology seamlessly integrates into every aspect of our lives, the importance of cybersecurity cannot be overstated. As businesses, governments, and individuals continue to rely on digital platforms for communication, transactions and data storage, the threat landscape for cybersecurity is evolving at an unprecedented pace.

7. IT security challenges and trends

Vasile Voicu, Manager of Digital Solutions at Orange Romania Communications is coordinating the following lines of business: Cybersecurity, Hybrid Cloud, Hosting Data Centers, Digital City & IoT. He is a highly-accomplished and versatile ICT executive, with 20 years' professional experience and a proven track record in cybersecurity, cloud and IoT, with both a technical and commercial understanding of these fields. He holds a BSc in Electronics and Telecommunications engineering from the Polytechnic University of Bucharest, an MBA in Strategic Management and several postgraduate studies in business management, marketing and strategy.

In the year 2024, the number of computer attacks with malware is expected to increase due to the exponential growth of attack vectors, a direct consequence of the large-scale implementation of the new digital technologies Internet of Things (IoT), Cloud Computing, Machine2Machine (M2M). IT threats will continue to grow exponentially and diversify : viruses, trojans, malware, ghostware, M2M attacks, cloud attacks, advanced persistent threats, ransomware, denial-of-service (DDoS). All this threatens both individuals and organizations.

Following an 8% increase in weekly global cyber attacks in the first half of 2023, marking the highest volume in two years, cybersecurity solutions provider Check Point Software has forecast the top cyber threats for 2024. These threats include the rise of ransomware attacks, the application of artificial intelligence (AI) and machine learning (ML) technologies by cybercriminals.

For this reason, IT security becomes a priority, and companies need security policies, high-performance antivirus software, IT security solutions, workshops to educate employees on the risks of a cyber attack and situation management systems that intervene at the security level. By developing intelligent security systems, companies can proactively predict, identify and react to potential threats.
It is important for company managers and employees to understand the risks of attacks for the health of their businesses and the need for a company-wide security strategy to prevent information theft, illegal access to a computer system, theft of personal data or disruption of a system's operation informatics. Within any company, employees must know and follow the internal security policies, attend periodic courses on awareness of dangers and compliance with security requirements, periodically save data, not open unsolicited emails or attached documents, block programs and unwanted or unnecessary traffic, to immediately update systems and programs as often as they are asked. Email applications and phishing messages will remain the primary vectors of malware infection in 2024.

Source : https://blog.checkpoint.com/artificial-intelligence/into-the-cyber-abyss-check-points-riveting-2024-predictions-reveal-a-storm-of-ai-hacktivism-and-weaponized- deepfakes/

Phishing attacks will become more sophisticated in 2024, digital messages will be sent to well-chosen targets in an attempt to get them to access links that will later allow the installation of malware and the exposure of sensitive data. Knowing that employees in most organizations have become aware of security risks and do not easily access links from unknown sources, cyber attackers use techniques based on Machine Learning to compose personalized messages, with a specific header, so that they are as convincing and to deceive the vigilance of the addressed targets. Such attacks allow "hackers" to steal passwords, credit card credentials or other financial information and gain access to private databases.

Ransomware strategies will evolve in 2024. Ransomware attacks involve blocking users' access to important files and data and paying a ransom to regain access. The costs borne by the victims of these attacks reach the level of billions of dollars annually through the lens of the possibility to pay the ransom with cryptocurrencies that allow the anonymization of the beneficiaries of these payments. Companies will invest massively in security solutions to ensure protection against "ransomware" attacks, but on the other hand, individuals with high incomes will be important targets for hackers.

Cryptojacking is the trend that involves hackers taking control of the IT devices of other people or companies in order to pay the ransom with cryptocurrencies. Because the processing resources required in cryptomining are large, cyber attackers earn money through the illegitimate use of computer systems belonging to third parties.
The effects of cryptojacking consist in decreasing the processing speed and performance of computer systems, leading to high costs for the victims.

Cyber attacks directed against infrastructures in critical sectors: energy, transport, health, utilities will register increases in 2024. Digital technology used for legitimate purposes to modernize and automate critical infrastructure also brings IT security risks. Cyber threats against energy infrastructure have demonstrated vulnerabilities exploited by hackers successfully in the past and will be replicated in the future. Even multinational companies with annual turnover of billions of dollars are targets for cyber attackers.

Cyber attacks directed against IoT is a major concern in 2024, due to the lack of protection mechanisms at the level of IoT devices and services. There is a pressing need to develop architectures, protection and defense mechanisms against cyber attacks and best practices for IoT.

According to **Statista.com**, the number of connected IoT devices will reach 75 billion by 2025. These include laptops, tablet PCs, routers, surveillance cameras, refrigerators, smart watches, medical devices, cars and surveillance systems. Connected IoT devices are beneficial for increasing work productivity, remote control and modernization of industrial processes, monetization of data by companies. However, the very large number of connected devices leads to a major security risk by increasing the attack area and the high probability of infection with computer viruses.
Once under the control of hackers, IoT devices can be used to launch attacks against other entities, they can be disconnected, they can cause immense damage by interrupting business processes.

The main reasons why security problems may arise in the case of IoT are:

- Most of these devices have limited computing power, so the operating system has a minimal structure, and installing powerful antimalware software is difficult.
- IoT releases are made in haste, without support from security specialists - serious security tests and advanced protection options are generally missing.
- Hackers can take advantage of vulnerabilities in the IP protocol that allows communication between various devices.

Attacks against semi-autonomous vehicles will develop in 2024 simultaneously with the evolution of technology. In 2024, it is estimated that 80% of new vehicles will be connected to the Internet.

For cyber attackers, this technological evolution in the automotive field becomes a new opportunity to exploit system vulnerabilities and steal sensitive data or even endanger traffic participants.

Cyber attacks against mobile devices
Mobility is the new driver in connectivity and IT: 95% of mobile device users will use mobile broadband in 2024. Even if mobile threats are not yet as visible as those in the PC area, the growth of mobile threats is real and accelerated:

Source: https://www.pwc.com/cz/cs/cyberandprivacy/Cloud%20security%20report_EN.pdf

- 263% increase in mobile malware in the last 12 months,
- 75% of mobile security breaches are the result of misconfiguration of applications,
- 80% of employees use personal mobile devices for business and 82% of companies reported security problems in the mobile area due to employees.

The main concerns in the mobile area:

- Data loss due to lost or stolen devices
- Mobile malware
- Lack of data protection and the possibility of information leaks
- Bring-Your-Own-Device policy and legal liability issues involved
- Enforcing acceptable usage policies for mobile devices in an organization.

In 2024, ensuring security in the case of Cloud services is a priority

The cloud is revolutionizing the way business is done. Companies no longer have to invest in on-premises, inflexible and expensive IT solutions, a cloud solution saving time, money (hard, software, maintenance) and resources.

Where no economy should be made is cloud security. For example, moving information and sensitive operations to an external data center is important not only from an economic point of view, but also from a security point of view. Not only IT professionals understand how important it is to choose a cloud service provider - a reliable partner becomes not only a competitive advantage, but also a crucial component of the business.

Data protection is the main priority when discussing about cloud security. The security constraints of cloud services are: compliance (legal, regulations), integration with the current IT environment, fear of too much dependence on the cloud provider. Data protection in the cloud is achieved through backup and recovery services, encryption, data loss prevention (DLP - data lost prevention) and database activity monitoring (DAM - database activity monitoring).

8. Business Internet Security – Insights and Findings

Business Internet Security (BIS) is a Managed Security Service offered by Orange Business available for medium and large companies, that analyses more than 11 million security threats each month within our customers' security infrastructures. We gather anonymized relevant data from companies across industries such as public services, retail, transportation, and energy. Data obtained is then processed through InfraAI, our Big Data Security Analytics in-house developed platform, to correlate and enrich the business intelligence we provide our customers for insights and actionable intel. Data for this report is generated by correlating anonymized information from multiple security systems deployed within our Service Premises, such as NG-Firewalls, Web and Email Security Gateways, DDoS mitigation systems, Intrusion Detection Systems, or Web Application Firewalls, and statistical data gathered from pen testing and security audits performed for our customers.

The information gathered from our Cyber Security Sensors is enriched in InfraAI through multiple Threat Intelligence Feeds. The information presented herein represents all findings from Q4 2022 up to Q3 2023.

a. Distribution of Threats by Business Vertical

Threat distribution by business vertical in Romania closely resembles the wider, international distribution, published through open sources. Our State-of-the-Art MSSP Platforms, enrich our existing Customer Data with Business-relevant Context, such as Industry Verticals, or Geographical reach. Compared to our 2022 reporting, we've noticing an overall increase in volumes of the threats and attacks detected and blocked by BIS.

Our 2023 analysis reveals that the Energy Sector was hit the worst, amongst our B2B and Public Sector Customers Base, and this year, resembling the past two reporting periods, ransomware is the main culprit. The transportation sector is second in line, with upwards of 22% of all detections through BIS.

Although the motivations, techniques and procedures of attackers are usually difficult to observe and relay, there are a possible number of reasons for this shift in targeting, compared to what we previously observed in our reporting: a consistent move toward the developing and release of user-facing digital tools, for consumers and prosumers in the Energy sector has allowed customers to quickly be onboarded by their energy providers. Furthermore, advances in integrating new IT tools in the operations stack of many players in the Energy Sector, has led to the increase of the addressable attack surface and has made key players in this sector, a very tangible target for malicious actors.

Percentage of All Blocked Threats in BIS

Energy	31.06%
Transportation	22.36%
Govt. and Public Services	19.70%
Retail	16.42%
Health	10.46%

b. Distribution of Threats by Region

Within a nation-wide customer base, we gathered information related to attacks across-industries and the Bucharest region was the most targeted, with 39.92% of all detected threats targeting assets geographically located to our Capital's City Region.

Coming in second is Sud-Est region with 27.13% of all threats distributed across-industries and on third place is the Banat region with 16.27% of all threats.

Percentage of Total Attacks Blocked by BIS

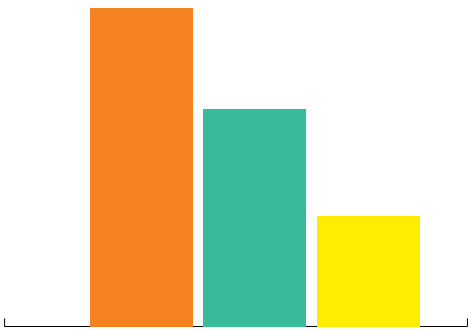
Bucharest	39.92%
South-East (Dobrogea)	27.13%
Banat	16.27%
Other regions	16.68%

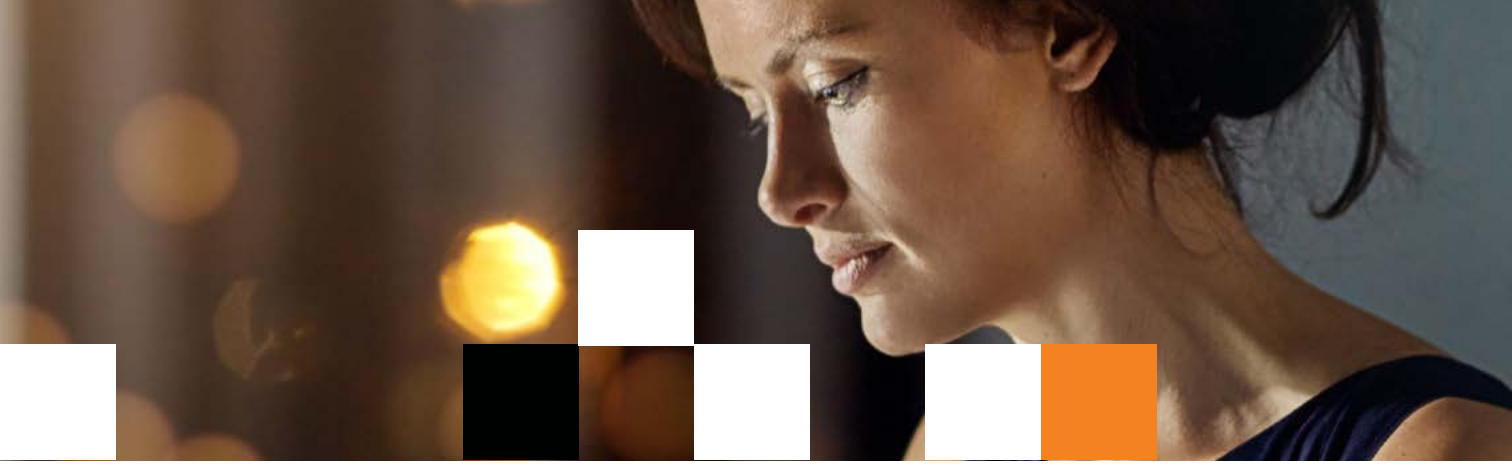
As for the most affected cities in the past 12 months, Bucharest is in first place with an average of 980.000 attacks prevented each month, across our customer base located there, with Constanţa coming in second with on average 670.000 attacks blocked each month and Timişoara counting for third place with almost 340.000 threats detected and blocked, each month.

We have developed and automated an enrichment method for enabling precise localisation of the various infrastructure and digital assets, under BIS' protection, in our customer premises. The process relies on targeting and consolidating data from our CRMs, related to association of IP addresses, ASNs and on the ingestion of client-specific onboarding data, to refine the positioning of the assets to a certain geography. This enables our InfraAI platform to pull relviable data, and to provide analytics on threats, actors, and targets across Romania, and with precision information regarding the association to the different branches and Points of Presence of our BIS Customers.

Avg. number of blocked attacks, monthly

Bucharest	980.000
Constanţa	670.000
Timişoara	340.000





c. Distribution of Threats by Type

2023 was once more a year of the Ransomware. Multiple campaigns had affected hundreds of millions of assets, with losses totalling in the tens of billions USD. Many new malware species have been detected to provide their operators with cryptography-based attacks capabilities. We've seen Ransomware spread through the usual vectors – emails, social media, unsafe downloads, in principle, with some interesting new-comers to our BIS Customer premises, such as Browser-based attacks.

There were numerous ransomware incidents in Romania targeting across the spectrum of industries, with malicious actors engaging Generative A.I.-tools to create obfuscation of their codes and to generate "digital noise".

Phishing Attacks comes in second, 3 years-in-row, continuing to cause disruption to business and people, with large scale reporting of many incidents, from bulk email and SMS campaigns to targeting of victims. We've monitored multiple campaigns through 2023 and noticed a shift of the content to pressing social issues with widespread audiences such as the war in Ukraine, economic struggles such as rising inflation or the various viral campaigns of late 2022 and early 2023, specifically the falsified drafting orders being seemingly send by the Local Military Offices to conscripts of age. Unfortunately, such campaigns have their large share of victims, with many failing to address the truthfulness of the messages, in principle due to a lack of awareness.

Percentage of All Threats Detected in BIS

Ransomware	34.62%
Phishing	31.19%
DDoS Attacks	27.07%
Others	7.12%

d. Distribution of Threats by Country of Origin

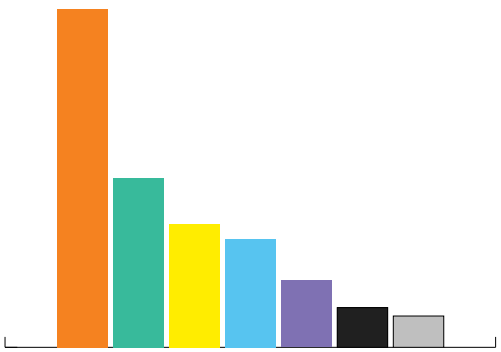
Keeping in line with our previous reports, most of the sources of the attacks detected by our security solution use spoofed IP addresses so it is difficult to precisely identify the 'true' geographical source of an attack.
To circumvent this limitation, we are using several enrichment methods to determine a more precise localization for some of the principal threats we are seeing attacking our customer base.

We report on the mean number of unique offender IP addresses hitting BIS each month and we use several intelligence methods and techniques to pinpoint these IoCs (Indicators of Compromise) to specific locations.

The past 12 months show an uptick in malicious traffic stemming from IPs in the Russian Federation and China.

Unique Offender IPs (Rounded up Avg./ Month, past year)

United States	810.000
Romania	405.000
China	295.000
Russia	260.000
France	160.000
United Kingdom	95.000
Brazil	75.000



e. Distribution of Threats by Criticality

Our risk-based assessment model follows Mitre CVSS 3.0 rankings for each exploitable weakness.
This scoring system assigns a criticality level for CVSS value ranges as follows – critical level for values in the range of 9.0 to 10.0, high level for values 7/0 through 8.9, medium for 4.0 to 6.9, Low being 0.1 to 3.9 and finally – Informational representing a ranking of precisely zero.

Percentage of all vulnerabilities

Critical	9.12%
High	11.57%
Medium	7.82%
Low	56.08%
Informational	15.41%

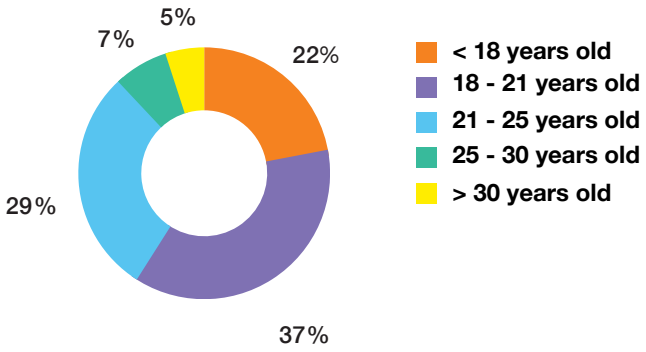
9. Education, Innovation and Research

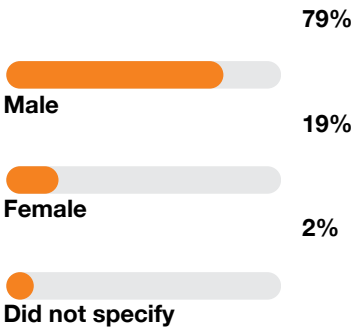
Education through Gamification - UNbreakable Romania

UNbreakable Romania – UNR23, in short, for most participants – has become the principal reference to Capture-the-Flag competitions in Romania, available for students of all ages. This years' edition was by far the most successful since the beginning of our programme, with 900+ participants registered in the competition, representing 62 high schools and 29 universities across 38 counties.
Nearly 30% of all participants have played at least in one of UNR's previous competitions.

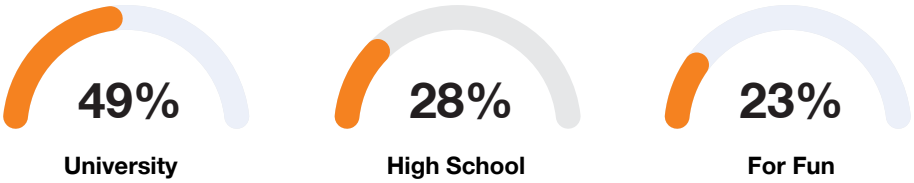
UNR23 consisted of 2 CTFs, one with individual scoring and a second, team-based competition.
For a comprehensive report on all results, check out the skills mapping section on Threatmap.ro and visit Unbreakable.ro for up-to-date results and infographics.

Participants distribution
622 participants





Team distribution
85 teams



The Romanian Cyber Security Challenge

2023 was our second year of promoting UNBreakable as part of the selection process for RoCSC – The Romanian Cyber Security Challenge, a national effort supported by partners from the public and private sectors to search for, and train #TeamRomania, a group of 10 individuals representing Romania to the European Cyber Security Challenge. We've weighted the results of the participants to UNR23 as a criterion for the selection of the Top-30 players, further advancing to an on-site CTF competition organized in late July. The top 20 scorers continued to a 5-days Boot-Camp held at Bran in mid-August, which yielded a Best-10 who got to represent Romania in the European Cyber Security Challenge 2023.

This road led us to Hamar, a beautiful inner town of Norway, some 120 km north of Oslo, where we competed in the ECSC 2023 Finals, during a 3-days CTF competition. The event consisted of a 2-day Jeopardy-style CTF and a one-day Attack and Defence event.

#TeamRomania finished the competition in 8th place out of the 30+ participant countries, on a highly competitive and tight scoreboard. This has set a natural goal of reaching Top-3 for the 2024 edition to be held in Italy.

Innovation in Cybersecurity - Orange Fab Startups

Orange Fab Romania is part of the Orange Fab international network of accelerators, currently operating in 20 countries across the globe. In Romania, the programme started in 2017 and, from the very beginning, had a dedicated Security track.

Orange Fab offers innovative startups access to:

- Orange 5G Lab, with the newest technology and equipment
- Mentoring and on-demand learning opportunities
- Clients and pilot projects supported by Orange
- National and international exposure

Security Startups from Orange Fab

Pentest Tools - Online framework for automation of penetration testing and security assessment where the users obtain a detailed list of vulnerabilities which they can remediate before being hit by cyberattacks.
pentest-tools.com

Dekeneas - Web Security solution using artificial intelligence to address some of the most complex and hard to tackle computer threats: browser-based attacks.
dekeneas.com

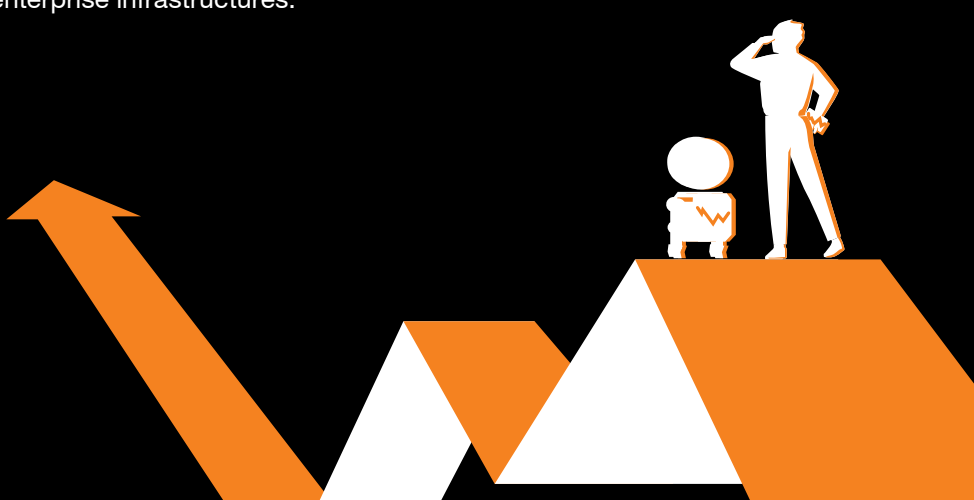
Siscale - A highly experienced integration company offering services and products in fields like infrastructure & security, data services and AIOps adoption.
siscale.com

Rungutan – A disruptive load testing platform available as a service, offering rich technical features useful for simulating application traffic spikes, up to the point of simulating denial of service scenarios.
rungutan.com

CyberEDU - With hundreds of hands-on exercises mapped against industry standards, CyberEDU offers a powerful learning tool for individuals or teams that want to reach the next level of mastery in offensive or defensive cybersecurity.
cyberedu.ro

Core Antivirus – Next-generation AV solution, offering advanced real time protection against cyber-threats in a fast, ultra-performant package. Core Antivirus offers protection of local and Cloud environments and can be configured and deployed remotely.
corecyberdefense.com

StageOne – Disruptive Purple Teaming and Red Teaming Platform built to simulate complex adversarial techniques and procedures against enterprise infrastructures.
stageone.ai



Research and Innovation Projects

Orange Romania is one of the most active participants in Research and Innovation Actions funded through the European Union, with an impressive track record on delivering advanced capabilities for experimentation and validation of Use-Cases. Our 5G Lab Facilities in Bucharest and Iaşi, provide State-of-the-Art and Beyond-State-of-the-Art services for developing, testing and technical and business validation of new technologies in the complex domains of Networks of The Future, Compute Continuums, Communications Continuums, Cyber Security and Advance-IoT.

During the past 12 months we onboarded 14 new Research and Innovation Projects, on multiple topics in the Horizon Europe and Digital Europe Programme calls, and on the National Resilience and Recovery Plan.

The topics range from Beyond-5G Networks to Cyber security in the EDGE-Cloud-IoT Continuums and are expected to deliver platforms, frameworks, and best-practices, promoting the development of new capabilities and Use-Cases for the European Networks of the Future.

5GASP

5GASP (5G Application & Services experimentation and certification Platform) aims at shortening the idea-to-market process through the creation of a European testbed for SMEs that is fully automated and self-service, to foster rapid development and testing of new and innovative Network Applications built using the 5G NFV based reference architecture. Building on top of existing physical infrastructures, 5GASP intends to focus on innovations related to the operation of experiments and tests across several domains, providing software support tools for Continuous Integration and Continuous Deployment (CI/CD) of VNFs in a secure & trusted environment for European SMEs capitalizing in the 5G market. 5GASP targets the creation of an Open-Source Software (OSS) repository and of a VNF marketplace targeting SMEs with OSS examples and building blocks, as well as the incubation of a community of Network Applications developers assisted with tools and services that can enable an early validation and/or certification of products and services for 5G. We focus on inter-domain use-cases, development of operational tools and procedures (supporting day-to-day testing and validation activities) and security/trust of 3rd party IPR running in our testbeds.

The 5GASP Project started in January 2021 and will continue until the end of 2023. Orange Romania's objective is to validate the usage of the 5GASP Platform for the delivery of 5G Network Applications, through our facility in Bucharest and to create a community of developers of 5G-enabled applications.

This project has received funding from the European Union's Horizon 2020 research and innovation programme (5GASP H2020 – ICT- 2020). Grant agreement ID: 101016448

5gasp.eu/

VITAL-5G

The VITAL-5G (Vertical Innovations in Transport And Logistics over 5G experimentation facilities) project has the vision to advance the offered transport & logistics (T&L) services by engaging significant logistics stakeholders (Sea and River port authorities, road logistics operators, warehouse/hub logistic operators, etc.) as well as innovative SMEs and offering them an open and secure virtualized 5G environment to test, validate and verify their T&L related cutting-edge Network Applications. The combination of advanced 5G testbeds (offered through participating MNOs / vendors) with vertical specialized facilities and infrastructure (offered by participating key logistics stakeholders) through an open service validation platform (repurposed and created by the project) will create a unique opportunity for third parties such as SMEs to validate their T&L related solutions and services utilizing real-life resources and facilities, otherwise unavailable to them. The platform will provide to 3rd party experimenters, the necessary testing and validation tools, offering them a trusted and secure service execution environment under realistic conditions that supports multi-tenancy. Such an elaborate validation mechanism will allow for the further refinement and fine-tuning of the provided services fostering the creation of new services and the evolution of existing ones, while boosting the SME presence in the emerging 5G-driven logistics ecosystem.

The VITAL-5G project plans to showcase the added-value of 5G connectivity for the European T&L sector by adopting a multi-modal approach containing major logistics hubs for freight and passengers (sea ports, river ports, warehouse / logistics hubs, highways, etc.) as well as the respective stakeholders (road operators, port authorities, 3rd party logistics (3PL) operators), thus creating an end-to-end chain of connected T&L services accommodating the entire continent.

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 101016567.

vital5g.eu/

RIGOUROUS

RIGOUROUS project aspires to identify and address the major cybersecurity, trust and privacy risks threatening the network, devices, computing infrastructure, and next generation of services. RIGOUROUS will address these challenges by introducing a new holistic and smart service framework leveraging new machine learning (ML) and AI mechanisms, which can react dynamically to the ever-changing threat surface on all orchestration layers and network functions.
In brief, RIGOUROUS targets the following key objectives:

- Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management
- Human-Centric DevSecOps
- Model-based and AI-driven Automated Security Orchestration, Trust Management, and Deployment
- Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies
- Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

RIGOUROUS is funded by the European Union's Research and Innovation Programme Horizon 2020 under Grant Agreement no. 856709.

rigourous.eu/

DYNABIC

The strategic objective of DYNABIC is to increase the resilience and business continuity capabilities of European critical services in the face of advanced cyber-physical threats. This objective will be pursued by delivering new socio-technical methods, models, and tools to support resilience through holistic business continuity risk management and control in operation, and dynamic adaptation of responses at system, human and organization planes.

DYNABIC sets forward a set of specific objectives, aimed to deliver the DYNABIC Framework for ensuring increased resilience of critical systems, while assuring the continuity of business and operations through smart dynamic adaptation of the system, human and organization responses.

This will enable Operators of Essential Services to Predict, Quantitatively Assess and Mitigate in Real-time Business Continuity Risks and their potential cascading effects, using a new breed of methods and tools that Enable Disaster Preparedness in Critical Infrastructures and Improve the Prevention of business continuity risks in cross-organization and cross-domain incidents and attacks.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070455.

dynabic.eu

EU-CIP

The main goal of EU-CIP is to establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs).
In this direction, the partners have already established the European Cluster for Securing Critical infrastructures (ECSCI), which brings together 22 projects that collaborate in CI Resilience EU-CIP will leverage the capacity, organization, community, and achievements of the ECSCI cluster towards establishing an EU-wide knowledge network with advanced analytical and innovation support capabilities.
EU-CIP will offer advanced information analysis capabilities for evidence-based policy making and innovation support services for exploiting and commercializing research outcomes.
To maximize the impact of its activities, EU-CIP will establish and grow a vibrant ecosystem of interested and committed stakeholders around the project's information analysis and innovation support services.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

eucip.eu/

ADROIT-6G

The goal of ADROIT6G is to demonstrate low-TRL applications for the upcoming 6G network using a new, cognitive approach based on distributed AI. The project aims to improve performance and control in digital service interactions, and support future-looking applications.

The project goals will be achieved through the implementation of three use-cases:

- PoC 1 Immersive eXtended Reality (XR)
- PoC 2 Industrial IoT (IIoT)
- PoC 3 Collaborative robots (cobots) in construction

ADROIT6G project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grand Agreement No 101095363.

adroit6g.eu/

TrialsNet

The TrialsNet project vision is to enable the realization of compelling societal values through the implementation of 5G and beyond applications, which will be demonstrative for the transition towards the next generation of mobile networks. TrialsNet, through its large-scale trials with verticals in the three domains of i) Infrastructure, Transportation, Security & Safety, ii) eHealth & Emergency, and iii) Culture, Tourism & Entertainment, will be the means of connecting the digital with the physical and natural worlds.
There will be 13 use-cases that will cover the

three earlier mentioned domains and that will be developed in four countries. In Romania, in Iaşi, we will host 2 of 13 use-cases, one regarding Smart Crowd Monitoring and another one related to the development of a Smart Traffic Management solution.

The TrialsNet project has received funding from the European Union's Horizon-JU-SNS-2022 Research and Innovation Programme under Grant Agreement No. 101095871.

trialsnet.eu/

6Green

In the scope of the 6Green project we've committed the target to reduce the computed carbon footprint, relatively to 5G, by a factor of 10.
The efficiency comes from the extended usage of cloud-native solutions that place the business and consumer applications at the edge of the network, closer to the end-users, and are able to autonomously and proactively decide how to steer the user traffic in an efficient manner and how to scale down the resources that are not utilized.
The future 6G networks will also be aware of the carbon emissions related to the automatic computational decisions that it can take, so that it uses energy in the most efficient manner.
All these actions will be possible with the extended usage of ML algorithms that will actively learn from the network's operation and will take decisions based on the input from all the related stakeholders (MNOs, business, and commercial applications owners).

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101096925.

6green.eu/

SOCCER

The project "Security Operation Centres Capacity building for European Resilience - SOCCER", established to answer the European call DIGITAL-ECCC-2022-CYBER-03-SOC - Capacity building of Security Operation Centres (SOCs) - brings together a consortium of cyber and technology experts from Germany, France, Hungary, and Romania.

Over the period of 36 months our proposal seeks to:

- Develop and implement cutting-edge technologies for secure access to data (Security Hub) and the sharing of threat intelligence signals (TIS) across European entities, allowing for reinforced capacities to monitor and detect cyber threats
- Interconnect and strengthen advanced Security Operation Centres (SOCs) ecosystems in Germany, Hungary, and Romania, with the goal of enhancing cyber security resilience at both the national and EU levels

This project has received funding from the European Union's Digital Europe Programe under grant agreement No 101127847.

CYRESRANGE

The project addresses concerns and European directives in the field of cyber security, following the fulfilment of synoptic requirements at the EU level expressed through the EU Cyber Strategy presented by The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to "build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies" where "the EU's technological sovereignty needs to be founded on the resilience of all connected services and products."

The architecture of the project consortium and the participation of a cluster of excellence in cyber security with a wide representation at national and European level ensures the fulfilment of a premise of the EU strategy in cyber security: "All the four cybercommunities – those concerned with the internal market, with law enforcement, diplomacy and defence – need to work more closely towards a shared awareness of threats. They should be ready to respond collectively when an attack materializes, so that the EU can be greater than the sum of its parts."

Our project proposal addresses the first objective to build capacity of cybersecurity actors to react in a coordinated way to large-scale cybersecurity incidents, while fostering the role of CSIRTs, the CyCLONe network and considering the Blueprint. Our project will provide stakeholders a set of structured methodologies, vulnerability databases and forensic tools, and automated content delivery aims and tools.

The project focuses on the creation of new paradigms regarding the creation, interconnecting and strengthening cybersecurity ranges at national and regional level with great capabilities in the European realm, including critical infrastructures, not limited only to sectors covered by the NIS Directive.

This project has received funding from the European Union's Digital Europe Programe under grant agreement No 101128088.

iSEE-6G

iSEE-6G extends beyond JCS (Joint communication and sensing) and propose a Joint Communication, Computation, Sensing, and Power transfer (JCCSP) unified radio platform, which includes all support elements of the proposed solutions in future 6G networks. By integrating, exploiting, and supporting 6G key enabling technologies, iSEE-6G offers:

- JCCSP-oriented novel intelligent reconfigurable surfaces (RIS) and agile beamforming array solutions
- JCCSP-optimized physical layer design including waveform design, frame structure design, channel modelling, precoding/beamforming with respect to open radio access network (O-RAN) architectural paradigm
- JCCSP-enabled cross-layer schemes design under new capabilities in terms of service-oriented network architecture
- JCCSP-implemented system-level solutions for providing new functionalities towards a cell-free 6G network

The iSEE-6G Proof-of-Concept (PoC) focuses in JCCSP use cases in aerial corridors, where UAVs with various roles providing different services coexist and coordinate with each other. In Orange Romania's testbed 5G waveforms based JCCSP exploits the KPI collection capabilities of it. The operation of the testbed will be extended at an outdoor venue, where UAVs and IoT devices will be deployed to test the Wireless Power Transfer (WPT) capabilities. Edge computational power is used for Public Protection and Disaster Relief (PPDR) monitoring and JCCSP-as-a-Service implementation.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101139291.

6G-PATH

The path towards 6G is beginning now that 5G matured and is being deployed worldwide both publicly and privately. While 5G brought a step up in many fields, such as performance and efficiency, more is always expected in terms of efficiency by the overall community and in terms of performance by industry and technology providers who want to further increase their offerings and products. Continuous demands for higher throughput, lower latency and more energy efficient communications needs to be supported by relevant use cases that can claim and demonstrate the needs for these requests.

6G-PATH goal is to help foster the further development and integration of new and improved tools and products from EU companies with 5G/6G, while also measuring relevant KPIs and KVIs. To achieve this, some testbeds will be part of the project consortium, which will be used by corresponding use cases spread across four key verticals: Health, Education, Smart Cities and Farming.

6G-PATH plans to work closely with other ongoing/starting Stream-B and Stream-C projects in a feedback loop, where the innovations that partners are achieving in other projects can be deployed and further tested by our pool of use cases and Open Calls, while sharing our results and outcomes to further cement the innovation being made.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101139172.

6G-INTENSE

The 6G Smart Networks of the future will provide the high-performance and energy-efficient infrastructure on which next generation internet and other services can be developed and deployed. 6G will foster an Industry revolution and digital transformation and will accelerate the building of smart societies leading to quality-of-life improvements, facilitating autonomous systems, haptic communication, and smart healthcare.
To achieve the objectives in a sustainable way, it is well understood that new approaches are needed in the way the telco infrastructures are architected, federated, and orchestrated.

These new approaches call for multi-stakeholder ecosystems that promote synergies among Mobile Network Operators and owners of all kinds or computational and networking resources that will share the extraordinary costs of yet another generation upgrade from 5G to 6G, while facilitating new business models. It is clear that the new architecture paradigms bring unprecedented complexity due to the sheer scale and heterogeneity of the orchestration domains involved, that should be matched by equally capable automation capabilities. Thus, 6G is aiming for the “holy grail” of pervasive AI-driven intelligence, termed as Native AI. However, the multi-stakeholder infrastructures foreseen in 6G as per the “network of networks” concept, will add a level of unprecedented management complexity due to the sheer scale and heterogeneity of the orchestration domains involved.

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101139266.

6G-MUSICAL

6G-MUSICAL is a ground-breaking project that merges radio sensing and communication technologies to create new paradigms in RF communication. It aims to equip edge infrastructure nodes of 6G with integrated RF/radar-based radio-sensing elements that co-work with communication components. This enables localization, object tracking and 3D imaging, with CM-level precision and resolution. As such, the project will investigate new spectrally and energy efficient system architectures and signals, to facilitate high-rate communication across multi-frequency bands integrated with accurate sensing and localization.

In the wireless domain, the project will define new waveforms suitable for radio-sensing and communications, exploit compressive sensing techniques and define cooperative multimode sensing and localization algorithms. In the network domain, focus will be on procedures for synchronization/calibration among edge nodes and on compression techniques to enable low overhead transport to a data fusion center of the collected information.

This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No 101139176.

10. Predictions for the Evolution of Cybersecurity Threats in 2024

Cybersecurity is a dynamic field, where the landscape is constantly evolving and threat actors are becoming increasingly sophisticated. As we approach 2024, it is essential to anticipate the potential directions in which cybersecurity threats might evolve.

1. AI and Machine Learning in Cyberattacks

Prediction

In 2024, we can expect to see an uptick in the use of artificial intelligence (AI) and machine learning (ML) by cybercriminals. These technologies will be employed for more sophisticated attack strategies, including advanced social engineering, targeted phishing, and the development of polymorphic malware.

Analysis

AI and ML enable threat actors to automate attack processes, improve evasion techniques, and analyse vast datasets for identifying potential targets. As AI and ML adoption increases, cybercriminals will capitalize on these tools to make their attacks more effective and difficult to detect. This evolution will require cybersecurity professionals to develop AI-driven defence strategies to counter AI-driven threats.

2. Supply Chain Attacks on the Rise

Prediction

Supply chain attacks will become more prevalent in 2024. Attackers will target third-party vendors and software suppliers, exploiting vulnerabilities in the supply chain to compromise organizations downstream.

Analysis

The SolarWinds and Kaseya incidents in recent years have exposed the potential impact of supply chain attacks. These attacks are difficult to detect because they compromise trusted sources, making them a highly effective method for threat actors. In 2024, organizations will need to strengthen their supply chain security and conduct thorough risk assessments to mitigate this growing threat.

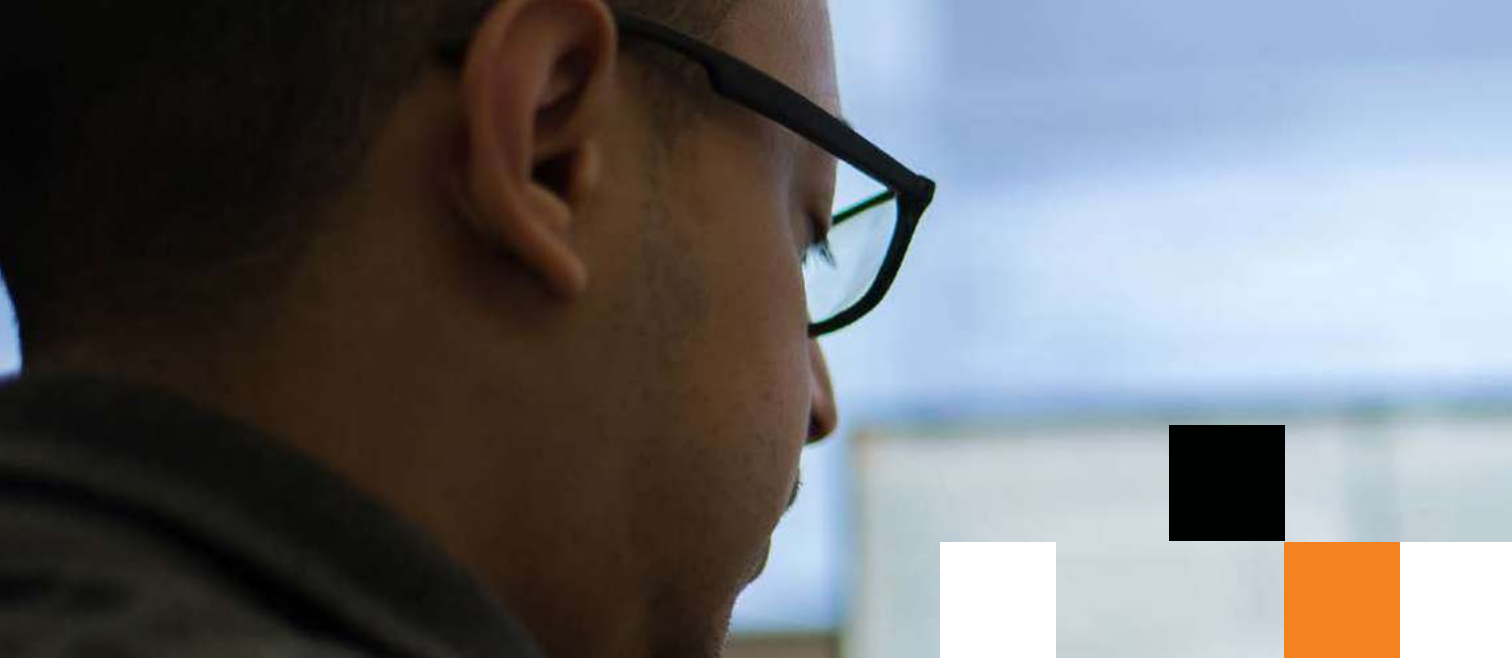
3. 5G Network Vulnerabilities

Prediction

With the widespread adoption of 5G networks, new vulnerabilities and attack vectors will emerge. In 2024, we can anticipate an increase in attacks targeting 5G infrastructure, IoT devices, and the potential exploitation of network slicing.

Analysis

5G networks offer faster speeds and lower latency, making them integral to the growth of IoT devices and critical infrastructure. However, this also introduces new security challenges. As 5G networks become more prevalent, attackers will look for weaknesses in these networks to compromise devices and disrupt critical services. Securing 5G infrastructure will be a top priority for organizations and governments.



4. Quantum Computing Threats

Prediction

Quantum computing, while promising for various applications, will pose a new set of challenges for cybersecurity in 2024. Quantum computers will have the potential to break widely used encryption algorithms, threatening data security.

Analysis

Quantum computing's ability to factor large numbers quickly jeopardizes encryption methods that rely on the difficulty of factoring large primes, such as RSA. In 2024, organizations will need to adopt post-quantum cryptography and quantum-resistant encryption methods to secure sensitive data. It's crucial to stay ahead of the curve to ensure data remains protected.

5. Ransomware X.0

Prediction

The evolution of ransomware will continue in 2024, with attackers adopting more sophisticated tactics. We can expect to see further exploitation of double extortion, targeting critical infrastructure, and the use of decentralized and privacy-focused cryptocurrencies.

Analysis

The ransomware threat is not going away; it's becoming more refined. Attackers will increasingly target critical infrastructure, adding additional leverage to their extortion attempts. Furthermore, they will focus on evading law enforcement by using cryptocurrencies that provide greater anonymity. Organizations must improve their incident response and disaster recovery capabilities to mitigate the impact of ransomware 2.0.

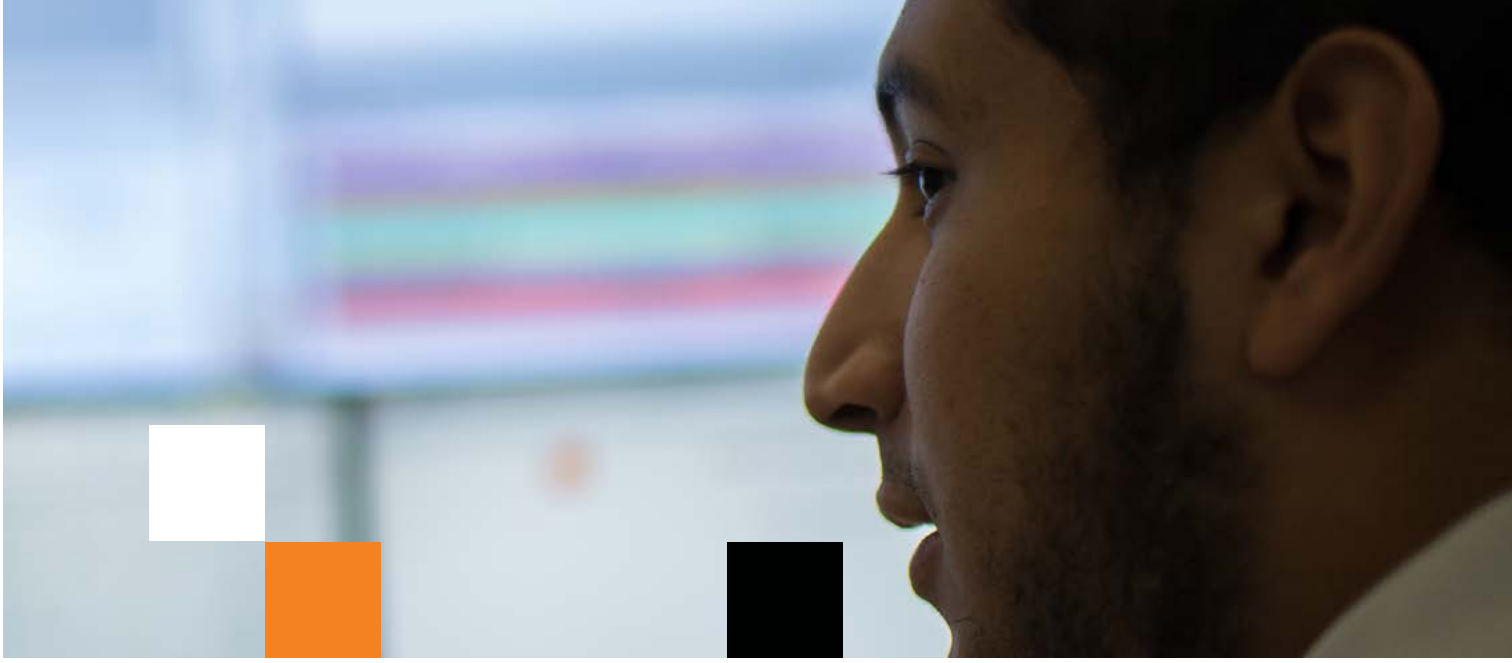
6. IoT Device Vulnerabilities

Prediction

The proliferation of Internet of Things (IoT) devices will continue to introduce new vulnerabilities. In 2024, we anticipate a surge in IoT-related attacks, with threat actors exploiting these devices for various purposes, including DDoS attacks, data exfiltration, and lateral movement.

Analysis

IoT devices often lack robust security measures and are typically connected to the internet, making them easy targets for attackers. As the number of IoT devices grows, they provide a larger attack surface for cybercriminals. Organizations and manufacturers need to implement better security practices for IoT devices and consider them in their overall security strategy.



7. Zero-Day Vulnerabilities and Exploits

Prediction

Zero-day vulnerabilities and exploits will continue to be an asset for cybercriminals in 2024. Their use will increase, particularly in targeted attacks, with the potential for the sale of exploits on the dark web.

Analysis

Zero-days are vulnerabilities unknown to software vendors and, as such, lack patches. These exploits are highly sought after, making them a valuable commodity. Attackers will actively look for and exploit zero-days to infiltrate systems and deploy malware. Organizations need to focus on proactive threat hunting, and software vendors must improve their patching processes

8. Advanced Persistent Threats (APTs)

Prediction

APTs will persist and evolve, becoming more elusive in 2024. They will focus on espionage, data exfiltration, and long-term persistence within compromised networks.

Analysis

APTs are highly targeted and well-funded threats that often remain hidden within networks for extended periods. They pose a severe threat to governments, critical infrastructure, and large enterprises. APTs will continue to evolve, using advanced techniques to maintain access and steal sensitive data. Organizations need to prioritize threat detection, incident response, and network segmentation to counter APTs.

As we look ahead to 2024, the cybersecurity landscape promises to be as dynamic and challenging as ever. Cyber threat actors will leverage emerging technologies and exploit vulnerabilities across diverse attack vectors. To defend against these evolving threats, organizations must remain vigilant, invest in cutting-edge cybersecurity solutions, and prioritize cybersecurity training and awareness. Staying ahead of the ever-changing threat landscape is essential to secure sensitive data and critical infrastructure in the years to come.

11. Glossary of Terms

Cyber Security - Computer security or IT security is the protection of computer systems from the theft and damage of their hardware, software, or information, as well as from disruption or misdirection of the services they provide.

Cyber threats (Threats) - The possibility of a malicious attempt to damage or disrupt a computer network or system.

Managed Security Services - In computing, managed security services (MSS) are network security services that have been outsourced to a service provider. A company providing such a service is a managed security service provider (MSSP).

IDS - An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

IPS - Intrusion prevention systems (IPS) are network security appliances or virtual appliances that monitor network or system activities for malicious activity, log information about this activity, report it and attempt to block or stop it.

WAF - A web application firewall (or WAF) filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF can filter the content of specific web applications while regular firewalls serve as a safety gate between servers. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

SIEM - Security Information and Event Management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

Ransomware - is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Crypto mining - in cryptocurrency networks, mining is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward.

Malware - (short for malicious software) is any software intentionally designed to cause damage to a computer, server, or computer network. It can take the form of executable code, scripts, active content, and other software. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, besides other terms.

Botnet - A botnet is several Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attacks (DDoS attack), steal data, send spam, and allow the attacker to access the device and its connection. A Botnet is controlled by a Command-and-Control Centre, operated by the owner.

DDoS - In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), The incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

Malvertising - (a portmanteau of "malicious advertising") is the use of online advertising to spread malware. The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but can inter-operate within the existing Internet infrastructure.

(Home) Router - A device that allows a local area network (LAN) to connect to a wide area network (WAN) via a modem (DSL or cable), a broadband mobile phone network, a general-purpose optical network or other connection.

Java Script - Alongside HTML and CSS, JavaScript is one of the three core technologies of the World Wide Web. JavaScript enables interactive web pages and thus is an essential part of web applications. Most websites use it, and all major web browsers have a dedicated JavaScript engine to execute it.

(Malware) Payload - The payload is the part of transmitted data that is the actual intended message, or, in the context of a computer virus or worm, the payload is the portion of the malware which performs malicious action.

Phishing - is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy website, communication typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern.

Exploit - An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behaviour to occur on computer software, hardware to gain control of a computer system, allow privilege escalation, or execute a denial-of-service (DoS or related DDoS) attack.

Public-key cryptography - Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

CVE - The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Eavesdropping (attack) - Network eavesdropping is a network layer attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information.

Bring Your Own Device Policy (BYOD) - Bring your own device (BYOD)—also called bring your own technology (BYOT), bring your own phone (BYOP), and bring your own personal computer (BYOPC)—refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smartphones) to their workplace, and to use those devices to access privileged company information and applications.

SQL injection - SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Cross-site scripting - Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

Windows PowerShell™ - PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language. It can be used in a cyber-attack to execute commands and copy or modify information on the victim's computer.

The Team
Ioan Constantin, Cyber Security Expert
Cristian Paţachia, Development & Innovation Manager
Alexandra Stanciu, Business Services Marketing Manager
Mădălina Pavel, Business Services Marketing Manager
Cristina Ilisei, Brand & Communication Team
Ştefan Buzea, Graphic Design & DTP