orange™ Business

Business Internet Security Report

5th edition, 2022

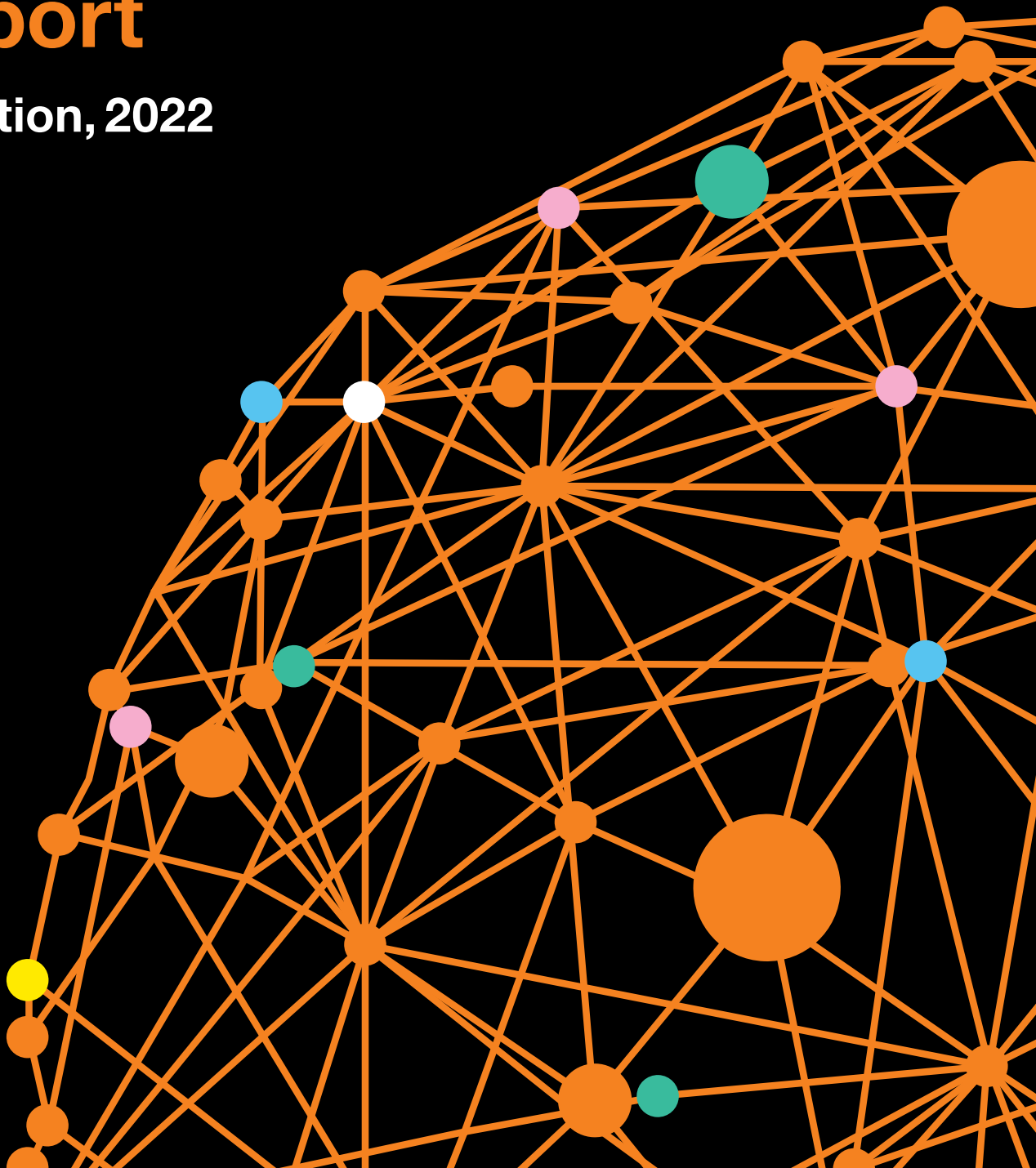


Table of Contents

2022: The year we all came under attack 6

Malware 2.0 7

Timeline of events 8

Cybersecurity on the rise: the NIS directive 14

Security Operation Centres in the NIS directive context 17

Security – from question mark to certainty 19

Empower employees to securely access apps remotely 22

Vulnerability management 24

Business Internet Security – insights and findings 25

Federating threat detection & response: next wave of security operation centres 30

- On the opportunity of a Security Operations Centre within a university 31
- Challenging the future of cyber security 33

Education, innovation and research 35

- UNBreakable Romania 35
- Innovation in cyber security – Orange Fab 36
- Research – Horizon 2020 and Horizon Europe projects 37

Bring your own device and mobile security 39

Predictions for 2023 41

Glossary of terms 42

We are quickly approaching the end of 2022, a year unlike any other, in which the world seems to do a high-risk balancing act, oscillating between great technological advances and unique opportunities on one side, uncertainty and economic turmoil on the other. Thus, after two very atypical years marked by the COVID-19 pandemic, in which companies had to reinvent themselves and embrace the digital transformation of their business, we now face new challenges.

As many companies migrated to hybrid or remote work, the number and complexity of cyber-attacks amplified. In fact, in the past year, we saw that cybersecurity threats have grown exponentially and, in an ever-increasing connected world, the internet has become not just the place that connects us, but also the new battlefield.

While there is no shortage of challenges ahead, one cannot help but be hopeful as cybersecurity and risk management are quickly becoming top of mind for businesses and public institutions alike. This is why having a prepared and safe infrastructure is critical, and Orange Business is now a trusted partner and an able provider of security services focused on delivering solutions that map customer needs and address requirements arising from the current socio-economic context. Customers can take comfort in knowing that they have the support and expertise of dedicated teams of experts as well as a wide array of robust, mature and high-quality services, all supported by the best network infrastructure in Romania.

At the same time, proactive measures such as education along with constant research and innovation are just as powerful in protecting personal and business data. In 2022, we expanded our partnerships with universities all across the country as well as joint collaborations in our EU research and innovation programs. In addition, we continue to build a strong ecosystem of startups through programs like Orange Fab, that support the growth of cyber security solutions.

In our 2022 Business Internet Security Report you will find a comprehensive analysis of the security threats that shaped the digital world this year, useful insights, and predictions for the year to come. We hope it brings you value, a better understanding of the importance of cybersecurity and growth to your business.

Marius Maican
Chief Technology Officer
Orange Romania

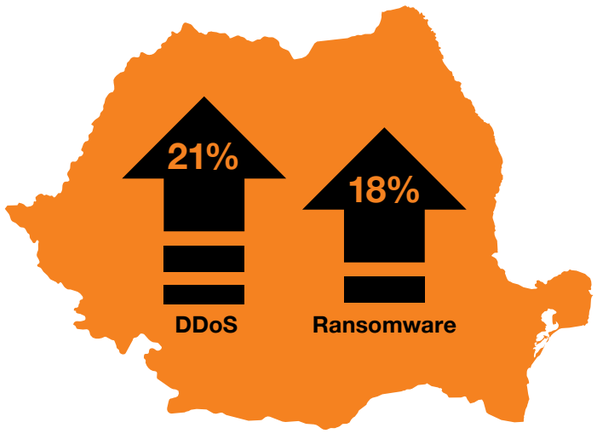
2022 – The year we all came under attack

The end of 2021 had most of us backpedalling through the aftershock of Log4J, with the worst out of the way. This was probably the aftershock no one accounted for, of the past 2 years of large shifts in ITC infrastructures due to COVID and its immense impact on cyber security. Log4J reminded us, people working in cyber security that we're far off from securing infrastructures "by design", while architectures remain reliant on ubiquitous software still prone to zero-day exposures.

Then early 2022 brought an onslaught of cybercrime and cyberattacks. Building atop what proved to be an ongoing war in Ukraine, state actors, various hacktivist groups and freelancers, alike, unleashed a series of high-gain, high-visibility attacks on targets of political and social importance with DDoS becoming a constant topic for most news outlets and other, more impactful attacks, targeting critical infrastructures, news & media, healthcare institutions and a plethora of Government websites and applications.

Private companies were alike targets of these groups' arsenals, more sophisticated attacks stemming from zero-day exploits in various software being used to gain access or exfiltrate data.
For the better part of 2022, most of these high-visibility attacks had low yield to target infrastructures, such as the DDoS attacks of April and May against various civilian and Gov't websites. Most targets were quick to recover from the DDoS while many had in-place protection against such unsophisticated, brute force attacks. But this did add to the news & media pressure of constant reporting of the various state-actors targeting the assets of politically or ideologically opposed countries, which unsurprisingly brought forward an increasing level of awareness to the tactics, technologies, and outcomes of the attackers.

Notable increases in the use of **ransomware** are a key to 2022 trends in cyber-attacks, with some **18%** YoY reported for the Romanian threat landscape, from our Business Internet Security services intelligence, while DDoS attacks saw an **21%** increase over the previous year.



Cyber-attacks increase in Romania

2022 brought some very interesting zero-day vulnerabilities, with researchers still looking for the associated exploits or attacks in the wild and some spectacular hacks and data leaks as well, some of these orchestrated by internal threat actors or through complex Social Engineering and authentication bypassing scenarios.

Malware distribution frameworks and "hacked" exploitation tools such as Cobalt Strike saw great increase in use of their target-side components (such as the Beacon backdoor) so did mobile-based attacks, with the likes of Pegasus' Spyware and the zero-click exploits it enables.

2022 has been a challenging year for everyone in cybersecurity from CISOs to SecOps. On the optimistic side of things, we've gained posture and resilience by dealing with large-scale attacks. The pessimists could argue that there are still some 2 months left of 2022.

Malware 2.0

The idea of Malware has been -to a great extent- on a slow and predictable evolutive slope, for the past 40-some years. Diversity and usage show incredibly strong growth, year over year, with some industry-actors referring to more than 1 billion variants, in the wild, as valid datapoint.

Considering a stable 15% growth in variants, year over year, one could easily predict what the landscape might be, in terms of volumes and diversity, in short and medium term. Worryingly, an estimated total cost of cybercrime (as a phenomena) which includes malware-based attacks, is skyrocketing to some 10 trillion dollars by 2025.

$ 10 trillion
estimated total cost of cybercrime by 2025

While the focus of many ventures in cyber security analytics, has been to monitor diversity and growth, the past few years brought an interesting shift towards the evolution of malware. The need to discuss "Malware 2.0" stems from the development of very prolific ventures offering Malware-as-a-Service.

Cobalt Strike, a commercial product for automation of exploitation has been in used since 2012 to recreate the techniques used by malicious actors and is a go-to tool for pen testers and red team specialists, part of one's offensive security toolset. Over the few years attackers have had access to leaked copies of the source code of both server-side components of Cobalt Strike and its frontend(s) and managed to pirate fully working versions of the suite, enabling to a limited extent, access to "Beacons" – i.e. – registered and monitored back-doors deployed on unsuspecting targets' infrastructures. The incredibly detail-rich community generated content, on how to access, deploy and use such tools have made it easy for attackers to use Cobalt Strike as a stop-gap tool for malware-based attacks. Furthermore, various marketplaces selling configurations, payloads and backdoors have appeared as a lucrative business for threat actors.

Malwares such as IcedID or Trickbot and FluBot serve as malware distribution platforms for the discerning customer. Having reached widespread distribution on infected PCs and devices, some actors begun cross-weaponizing these types of malwares into sorts of "Malware Content Distribution Networks (CDNs)" through which various types and variants of other malware are distributed on unsuspecting victim computers, allowing the attackers to reach highly granular distribution of malware according to their scope or objectives.

Flubot, on one hand has reached such a wide distribution pattern and had gained highly diverse payloads and specific settings accounting for a large range of banking services, that has become a banking malware distribution platform through which attackers can target certain banking apps, frontends and interfaces accounting for regionality, language and services offerings available to the customers of various financial institutions.

Moving through 2022, Ransomware shows clear signs of acceleration and it's likely to remain one of the principal threats to cyber security for the short to mid-term future. What is an addition to an otherwise well-known technique is the consolidation of features to Ransomware Distribution and Management-Like Platforms, enabling threat actors to deliver a pay-as-you-use Service for attackers wanting to encrypt data and/or extort unsuspecting victims.

We've seen threat actors crafting their own ransomware variants to exploit internet-facing services, sometimes by using large windows of opportunity and even zero-day attacks, or other purchasing access to target systems already compromised in previous attacks, by the selling party. It is these niche cases that makes attribution extremely difficult and are limiting cyber defenders in their capacity to pinpoint the sources of attack.

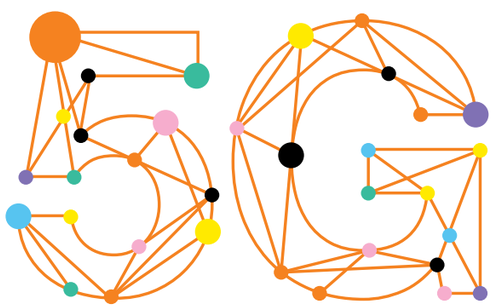
Ransomware variants actively weaponized into Ransomware-as-a-Service (RaaS) include some of the most infectious and effective ones, such as Conti or REvil (accounting for more than one third of all Business Internet Security detections).

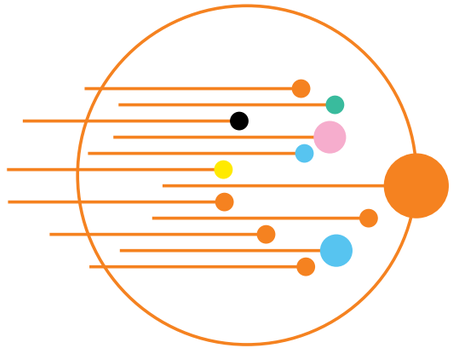
While the business model has been validated and threat actors are reaching to even more customers willing to buy RaaS access, the short-term outlook reveals that attackers are more likely to gain access and consolidate existing access to large enterprises, to maintain their service as in-demand and enable various parties to launch high-gain extortion attacks on their victims.

Timeline of events

September 2021

- A data breach exposed more than 61 million records and user data, from a various fitness trackers and medical devices. Data includes personal identifiable information and health metrics and data. The leak source is a company specialized in offering unified access to a wide range of health and fitness monitoring platforms.
- Hacker claims has stolen private data of more than 7 million Israeli citizens, from the databases of a websites used by public municipalities. The attackers has published samples of the alleged hack which – if confirmed – will prove to be the largest data breach in Israel's history.
- Hackers leak 0.5 million login credentials from vulnerable Fortinet VPN Servers. The hackers seemingly exploited a known vulnerability (CVE-2018-13397) to scrape these credentials covering some 500.000 users across approximately 13.000 devices. There are evidences suggesting the attackers have used this leak to promote (and enable distribution) of the RAMP Ransomware.





October 2021

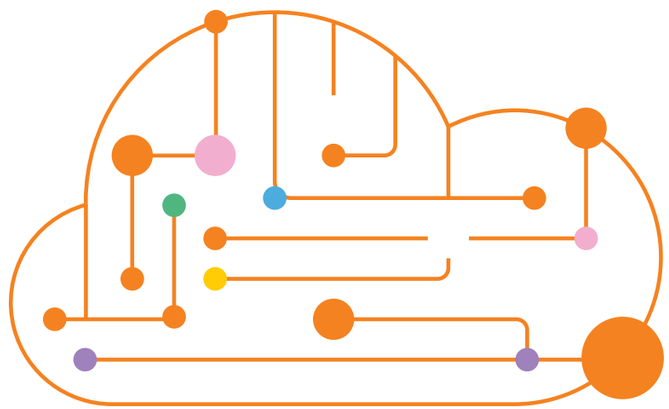
- Department store Neiman Marcus hacked by unknown party; more than 4.5 million records stole containing personal identifiable information of more than 4.6 million customers. Hacked supposedly happened in 2020.
- The Telegraph newspaper leaked some 10 TB of logs and subscriber data from an unsecured Elasticsearch instance. The cluster has been freely accessible to anyone wishing to interrogate and pull data, without any authentication in-place.
- Amazon's Twitch streaming platform specialized in e-sports content, reported a data breach happened in October without providing any further details. Independent outlet Video Games Chronicle reported, however, that some 125GB of data was leaked including highly sensitive financial information about the content creators who stream on this platform.

November 2021

- Personal data of more than 5.9 million Singaporean and South-East Asians customers of hotel booking site RedDoorz was leaked in Singapore's largest data breach to date. Records included names, e-mail addresses and itinerary info. Many Indonesian customers were among the 5.9 million victims.
- bZx, a De-Fi protocol used by many Crypto investors, has been hacked and assets up to $55 million in value have been drained from its liquidity pools. Attacked was based on threat actor gaining access to a Private Key used to control some of the protocols' smart contracts.
- Around 6 million customers of Sky Broadband located in the UK have been exposed to a critical vulnerability – a DNS rebind flaw – that could have been easily exploited by malicious actors, to gain access to the user's private home networks. The window of opportunity for such attacks closed 17 months after initial notification of the provider.

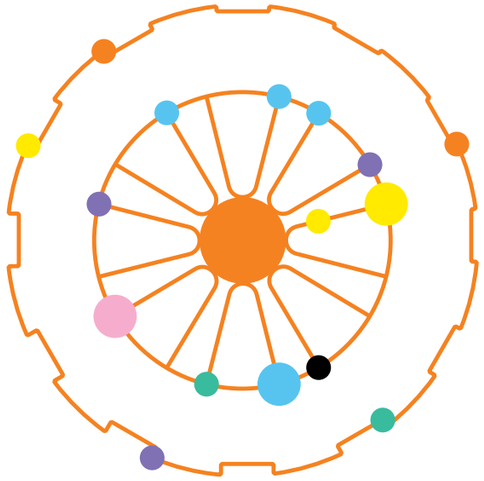
December 2021

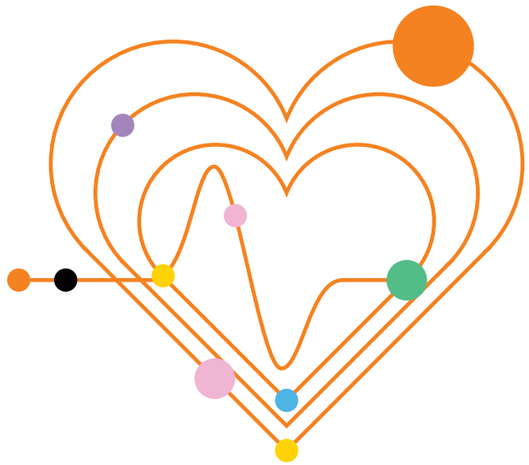
- A critical vulnerability in Java Logging Library, ApacheLog4J which is ubiquitous in most modern ITC infrastructures, could have allowed malicious actors to execute remote commands on the targets and subsequently gain access to the vulnerable machines and networks. Malicious activity triggered by the automated scanning and exploitation of this vulnerability has been recorded by many threat researchers, MSSPs and Cyber Security firms as early as December 1st, 2021. Log4j has been – and still is – one of the most impactful threats to ICT infrastructures.
- Brazil's Ministry of Health's websites attacked with ransomware by Lapsus$ Group, claimed to have exfiltrated then encrypted some 50TB of data pertaining to COVID vaccination records of 212 million Brazilians.
- The Belgian Ministry of Defence has suffered a cyberattack after malicious actors exploited one of the vulnerabilities in Log4j. The attack marks the first occasion that a NATO country's defence ministry has fallen victim to these types of attacks.



January 2022

- Crypto.Com was hacked with some 500 wallets targeted. The malicious actors used a 2FA authentication attack to gain access. The hackers stole 33$ Million in cryptocurrency. While they initially called it an ‘incident’, Crypto.com later retracted their statement and confirmed the theft and subsequent reimbursement of the victims.
- Some 39 million purported patient records from Bangkok’s Siriraj Hospital have been offered for sale on a dark web forum in what appears to be one of the largest breaches in Thailand’s history. The attacker followed up by posting on raidforums.com with a sample file.
- A „highly sophisticated” attack compromised The International Committee of the Red Cross servers, attackers compromised data of more than 515.000 “highly vulnerable persons” including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention.





February 2022

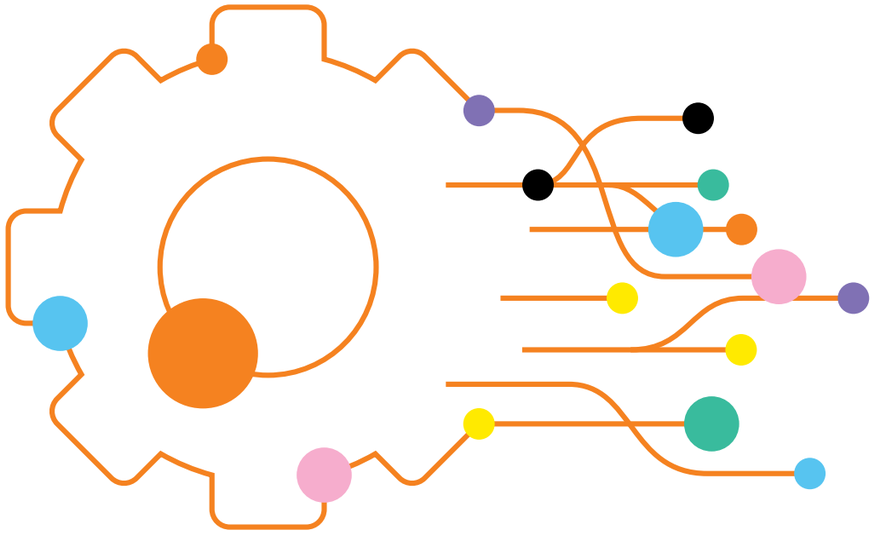
- A large telecommunications company in Portugal was victim of a cyberattack which affected service availability across most of their commercial mobile networks along with fixed data, fixed and mobile voice and SMS services.
- Swissport, an important aviation operations company which provides services to many airports across Europe has been hit with ransomware in an attack that caused flight disruptions for at least 22 scheduled flights.
- Credit Suisse were victims of a data leak, with confidential information on more than 18.000 bank accounts amassing some 100$ Billion in wealth, was leaked to a German Newspaper by a whistle-blower. The attack brought into focus the importance of insider threats monitoring and security.

March 2022

- Apple and Meta, two of the Worlds’ largest private entities fell victims to hackers impersonating law enforcement officers, gave user data upon response to forged requests. It is believed that some of the actors who gained access to the Law Enforcement Agencies’ Systems, to be part of the Lapsus$ Group.
- Hackers leaked large collection of data exfiltrated from Samsung Group’s Systems, including source code of applets and system components in use in sensitive “TrustZone” Environments, and source code of Qualcomms’ components.
- On March 17, it was revealed that the accounts of 19 healthcare staff had been hacked, causing the details of at least 510.000 people to be stolen. France’s Caisse nationale d’assurance maladie (Cnam) health insurance body, which has now made a formal complaint, explained that “unauthorised people” had connected to the “Amelipro accounts” of the healthcare workers whose “email addresses had been compromised”. Data stolen include the names, surnames, date of birth, social security numbers, GP details, and levels of reimbursement for at least 510.000 people.

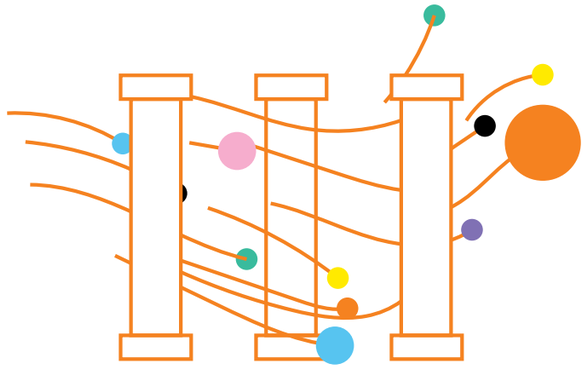
April 2022

- Hacktivists claim to have wiped nearly 65TB of data from Rosaviatsia’s (Russian Civil Aviation Authority) servers, including e-mails, aircraft registration and maintenance data. The Agency denied the attack took place, stating there was a downtime caused by a scheduled maintenance window.
- Large scale DDoS attacks caused downtime of some of Finland’s Ministry of Defence websites. This is one of the many brute-force DDoS attacks launched during the month of April 2022, by both Russia and western actors alike, against public websites. In most cases, the unsophisticated attacks caused minor availability issues for the web portals, and the operators managed to restore their websites in short time.
- Russian State-Sponsored group targets Ukrainian infrastructure with new variants of the Pteredo backdoor. According to a report by Symantec, who tracks the group as Shuckworm, the actor used at least four variants of the “Pteredo” malware, also tracked as Pteranodon.



May 2022

- A dataset containing user data for more than 21 million users of several VPN services, was leaked on Telegram. The data contains names, usernames, hashed passwords and e-mail addresses of GeckoVPN, SuperVPN and ChatVPN clients.
- Hackers claim to have personal identifiable information of more than 22 million Malaysians. A post on a Malaysian forum by the alleged hackers, is listing the dataset as for sale for some 10.000 $.
- German Library Service crippled by ransomware, in an attack orchestrated by the Lockbit ransomware group, who then published the data they exfiltrated during the attack, claiming their ransom requests have not been met.



June 2022

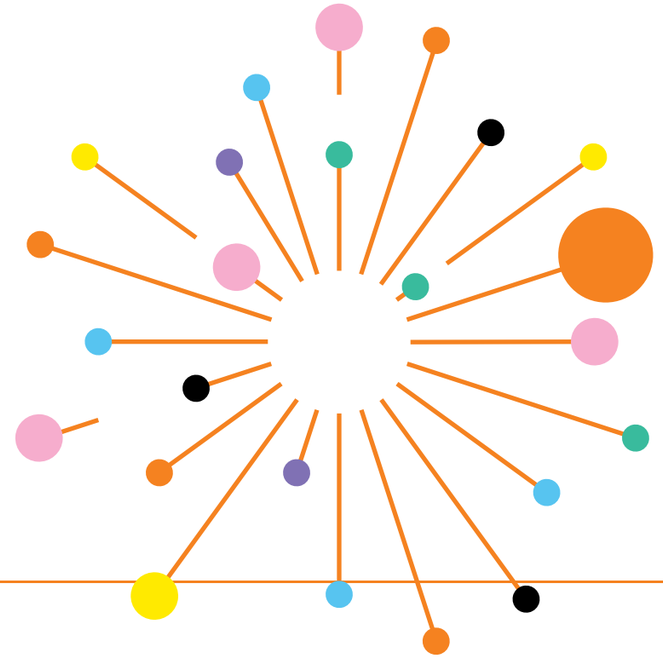
- OpenSea, the NFT marketplace, suffered a data breach after an employee of the company's email delivery vendor, "misused their employee access to download and share email addresses provided by OpenSea users… with an unauthorized external party".
- An unsecured AWS Bucket used by Pegasus Airline, exposed 6.5 TB of data consisting of personal information of flight crews. The EFB bucket was misconfigured to allow open access from the internet.
- Costa Rica's Public Health services offline after ransomware attack. The Hive Ransomware was the culprit, with initial breach happening some 3 days before the report was publicized. The employees of the Public Health agencies targeted by the ransomware were instructed to "unplug their computers" in order to prevent the malware from spreading through their networks.

July 2022

- Twitter was breached using a Zero-Day Vulnerability in their software stack, allowing the attackers to associate usernames with e-mail addresses and registered phone numbers. The hackers generated a dataset of more than 5.4 million affected user profiles.
- Uber acknowledged a 2016 data breach that exposed the personal information of more than 57 million of their customers. The company allegedly paid 100.000$ as ransom to the attackers and had failed to report the incident.
- Virtual pet website Neopets suffered a data breach exposing a database containing personal information of 69 million users. The website reported that the attackers exfiltrated source code of its software products.

August 2022

- A breach involving a partner of privacy messaging app Signal has exposed about 1.900 phone numbers used to create an account with the app. Twilio, the company that provides Signal with phone number verification services, suffered a phishing attack. Signal says that only a very small percentage of its user base was impacted and that no information beyond phone numbers was exposed.
- A hacker claims to have obtained the personal information of 48.5 million users of a COVID health mobile app run by the city of Shanghai, the second claim of a breach of the Chinese financial hub's data in just over a month. The hacker with the username as "XJP" posted an offer to sell the data for $4,000 on Breach Forums.
- An automotive supplier was hit with ransomware by three different attacks, all exploiting a misconfiguration exposing RDP through a border firewall. LockBit, Hive and BlackCat – the three culprits – have encrypted files (some files were encrypted at least 3 times each), the attack lasted for more than 2 weeks.



Cybersecurity on the rise: The NIS directive

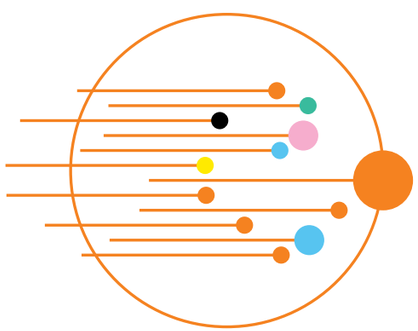
Network and information systems support many of the essential services so therefore it is highly important to protect these assets from the continuously evolving threat landscape. The European Commission elaborated the Network- and Information Security (NIS) directive applicable to all EU Member States.

The directive provides legal instruments enhancing the security of network and information systems underlying essential services in the EU for three strategic axes:

- improved cybersecurity capabilities at a national level
- increased EU-level cooperation by establishing the CSIRTs Network and the Cooperation Group
- defined security requirements and incident notification obligations for Operator of Essential Services (OES) and Digital Service Providers (DSPs)

The NIS Directive was adopted and put into force by the European Parliament in 2016 while the Member States were obliged to transpose it into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018.

In Romania it has been transposed through Law no. 362/2018 and has been effectively applied starting from July 2020 after Gov Order no. 119/2020 has been released. The technical rules needed for law's requirements implementation has been elaborated under the Gov Order No 1.1323/2020. DNSC is the local entity responsible for NIS Directive implementation.



NIS1 applicability

The NIS Directive defines security requirements and notification for OES and DSPs.

- Operators of Essential Services - OES is a public or private entity, which provides an essential service for the maintenance of critical societal and/or economic activities.
- Digital Service Providers - DSP means a service offered at a distance by electronic means at the request of a business organization or of an individual recipient of services.

It is understood that the directive is applicable for OES that depends on networks and information systems to deliver its services. A cyber incident affecting such systems may have an impact producing significant disruptive effects on its ability to provide its service.

For easier identification of OES's and DSP's, DNSC elaborated documents available in the same repository mentioned above.

To comply with the NIS Directive, OES and DSPs must take appropriate and proportionate technical security measures to minimize the risks of incidents affecting the security of network and information systems underlying their services.

Directive provides a comprehensive framework involving four pillars:

1 Governance at Member State level and cooperation among them

2 Security Requirements for OES and DSPs

3 Impact Assessment based on specific criteria

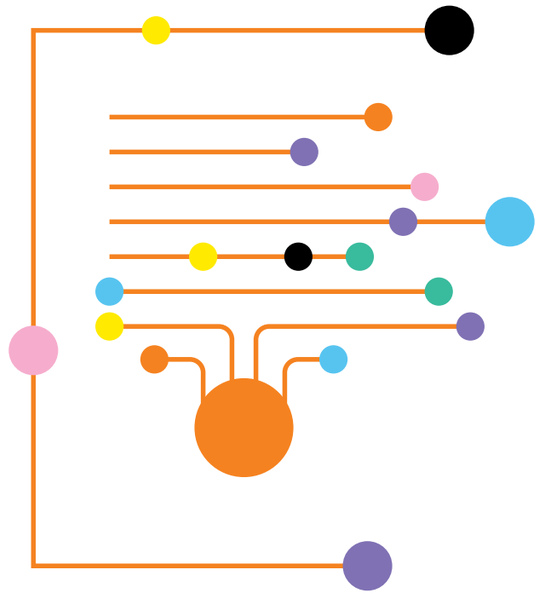
4 Incident Notification obligations for OES and DSPs to relevant NCAs or CSIRTs

Cyber capabilities

The technical measures to be implemented by organizations to prevent and minimize the impact of the security involves multiple cyber security capabilities. Most frequently these capabilities are elaborated under a technical roadmap followed for building them and for enhancing the maturity of OES and DSPs in alignment with the NIS Directive.

Usually, the technical measures are at the top of the actions taken by the organizations including capabilities covering Infrastructure Protection, Vulnerability Management and Cyber Incident Response.

Other important capabilities following these measures are Cyber Risk Management and Compliance; Cyber Training, Education and Awareness; Information Privacy and Protection and Security Operations Centre.



Key facts

According to ENISA's Threat Landscape Report, 2021 the estimated direct cost of a major security incident affecting OES/DSP at EU level is 100.000 EURO on median, with the banking and healthcare sectors experiencing the highest such costs of 300.000 EUR and 213.000 EUR respectively. The primary cost factors include costs related to revenue losses and data recovery or business continuity management.

On a global level, information security budgets seem to be increasing, although information security is still widely recognized as an exclusive IT discipline.

Skills shortages persist as an issue for information security staffing: skills in risk management, service management, incident response, threat intelligence, data science / analysis and coding are all expected to be in growing demand soon.

The NIS2 Directive

The coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation of societies around the world. During this unprecedented situation, there has been an increase in malicious cyber-activity across Member States, as revealed by a recent Europol report.

To respond to the growing threats posed with digitalization and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements. The Commission presented on 16 December 2020 a proposal for a directive on measures for a high common level of cybersecurity across the Union (NIS 2). The new act will oblige more entities and sectors to take measures and would assist in increasing the level of cybersecurity in Europe in the longer term. The proposed directive aims to tackle the limitations of the current NIS1 regime.

General objectives

- Increase the level of cyber-resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society, are required to take adequate cybersecurity measures. For instance, the proposal significantly extends the scope of the current directive by adding new sectors such as telecoms, social media platforms and the public administration.
- Reduce inconsistencies in resilience across the internal market in the sectors already covered by the directive, by further aligning:
  - the de facto scope
  - the security and incident reporting requirements
  - the provisions governing national supervision and enforcement and
  - the capabilities of the Member States' relevant competent authorities
- Improve the level of joint situational awareness and the collective capability to prepare and respond, by:
  - taking measures to increase the level of trust between competent authorities.
  - by sharing more information, and
  - setting rules and procedures in the event of a large-scale incident or crisis.

Orange Romania's cybersecurity capabilities

Managed Cyber Defense
SIEM & SOC Services
UEBA - User and Entity Behavior Analytics
Incident Response
Risk Monitoring Services

IOT Security
Operational Technology Monitoring
Industrial Network Protection

Endpoint Security
Client Protection and Monitoring
Endpoint Detection & Response (EDR)

Private Cloud And Data Security
Cloud access security broker (CASB)
DLP & DRM - Digital Rights Management
Key Management

Governance, Risk & Compliance - GRC
ISMS - information security management system
Risk Management
GDPR Compliance
Security Architecture Consulting
Security and Defense Management

Network security
Network Gateway Protection (NG-FW, IPS)
Content Security (Web Security & Mail Security)
Advanced Analytics
DDoS Protection
NAC - Network access control

Security Testing
Penetration Testing
Vulnerability Scanning
Patch Management
Secure Application Development

Business Application Security
Portal Security
Databases Security
Fraud Prevention

Identity & Access Management
Authentication
Access Management
ID Management
PKI & Certificates
Privileged Account Security

Security Operation Centres in the NIS Directive context

The Network & Information Systems (NIS) Regulations, aimed at raising levels of cyber security and resilience of key systems across the EU, came into force in Romania in January 2019.

The Emergency Ordinance no. 119 of July 22, 2020, for the amendment and completion of Law no. 362/2018 on ensuring a common high level of security of networks and IT systems enforces that each OES must implement appropriate and proportionate technical and organizational measures to meet the minimum-security requirements.

From the above the NIS directive enforces a set of specific requirements for the Information Security Incident Management Area for the OES:

- To implement appropriate measures to prevent and minimize the impact of incidents affecting the security of networks and IT systems used for the provision of essential services, with the aim of ensuring the continuity of those services.
- To establish the permanent means of contact and to designate those responsible for the security of networks and IT systems in charge of monitoring the means of contact.
- To immediately ensure the response to the incidents that have occurred, to restore the operation of the service to the parameters before the incident as soon as possible and to carry out the security audit.

In the above context the existence of a SOC (Security Operational Centre) facility at OES level becomes mandatory. Orange Business SOC (Security Operational Centre) covers the following requirements within NIS directive:

Tăslăoanu Cătălin
Cybersecurity Operations Manager
Orange Romania

Control indicator	Description	Art.
SIENIS	**SIENIS** - system for recording events at the level of networks and computer systems	Art. 29 - Registration of events [C121]
SIEM	**SIEM** - management of monitoring, research, and rapid identification of the main causes of security breaches, as well as breaches of security policies	Art. 29 - Registration of events [C122]
SCAJ	**SCAJ** - correlation system and journal analysis	Art. 30 - Logging and ensuring the traceability of activities within networks and IT systems [C13]
SMMEIS	**SMMEIS** - security events and incidents monitoring and management system.	Art. 31 - Response to security incidents [C212]
SIDGI	**SIDGI** - dedicated computer system for incident management	Art. 31 - Response to security incidents [C213]

Orange Business Security Operations Centre solution is designed to protect a company's business from the risk that information, applications, databases, servers and workstations, data and systems are modified, copied, or destroyed. The service is responsible for identifying, investigating, prioritizing, escalating, and resolving issues, which most of the time, are generated intentionally or accidentally by the human resource.

The mission of SOC solutions is to provide customer organizations with a highly mature detection and response capability designed to mitigate threats that endanger their most critical business assets. Security Operation Centre (SOC) services define security operations to respond to emerging and ongoing cyber threats.

SOC solutions ensure your compliance with data protection standards and security of national and EU networks and IT systems: GDPR, NIS-D with measures specific to each stage:

- prevention: advanced systems based on predictive algorithms used for early identification of new attacks.
- detection: Threat Intelligence, Threat Hunting, SIEM Security Information & Event Management).
- response: incident response, IT forensics, malware analysis.

In brief, a SOC solution:

- unifies and coordinates an organization’s security tools, practices, and response to security incidents.
- simplify and strengthen an organization’s compliance with industry, national and global privacy regulations.
- provides a centralized, complete, real-time view of how the entire infrastructure is performing from a security standpoint.
- detect, identify, prevent, and resolve issues before they cause damages for the business.

How does it work?

To monitor the Customer's systems, networks, applications and services, Orange Romania will first perform a security assessment on the Customer's infrastructure, then integrate the systems and services into the security monitoring and incident management (SIEM) platforms.
The Pre-onboarding and Onboarding stages include the technical evaluation, definition and configuration processes of the systems and services that produce events, logs and indicators that will be monitored through the SIEM (security Information and Event Management) platform.
First, the recording must be activated on the systems and applications so that they can then produce the set of data, logs, events, attacks that will be monitored through the specific detection and monitoring platforms.

“We are living in a digital era who brought us many rewards and as many challenges. Cybersecurity operations are transforming as we speak, to keep the pace with increased attacks seen on last years.

When discussing about SOC (or MSSP) maybe you are thinking to people who stay in front of big screens and check for all the events which are about to affect a company. While such view isn’t far from reality it is a bit outdated as our processes and tools are continuously evolving and heads to even more changes in the future.

We already started to add Public Cloud to our monitoring, the AI/ML is already assisting analysts in the triage and investigation, and, not at least, we are part of communities to exchange information. All these are the base of the future Autonomous SOC which is built on Data (ability to collect data from entire organization), Analytics (empower analysts with AI/ML-based analytics) and Community (intelligence sharing).

For all companies, small or big, essential services providers, or not, we are recommending implementing a cybersecurity program to increase protection against any business disruption which is easier than ever to appear from online. “

Security – from question mark to certainty

”

Innovation is everywhere around us; we have the latest smartphones that makes our lives better, smart cities with more and more digitalized services and facilities, smart agriculture, and farming with lot of sensors and data collection for a better and healthier food, manufacturing and production with robots and AI for faster and seamless products, but what about security? Do we have it, do we need it?

Now I must say that few years ago, when we thought about this word, we associated it with physical security in most cases, but this perception has changed over the years. Nowadays when we think about security, we extend this notion from a materialistic term to a more virtual one.

We are using more and more AI and connected tools at home and work, we must admit that we became technology dependent, therefore the concept of virtual or cyber security is not just a word anymore, it is a link to our material and emotional safety.

Today, we must watch over everything that goes online, that goes over the internet, that used data, in virtual ground. To have or not to have a security umbrella for our digital lives is not a question anymore, it is a must have, a certainty.

Whether we like it or not, the investment in a security solution will not just save our money and time, but also will generate safety for our partners and our businesses. We've upgraded to latest technologies, we embraced innovation, it’s time to upgrade our security solutions also, it is not a question it is a requirement. Threats have become more sophisticated than before and with the arrival of the internet of things (IoT), increased the need to secure networks and devices. A key element in protection is represented by the automation of cybersecurity that has become an integral component to keep companies protected from the growing number of cyberthreats.

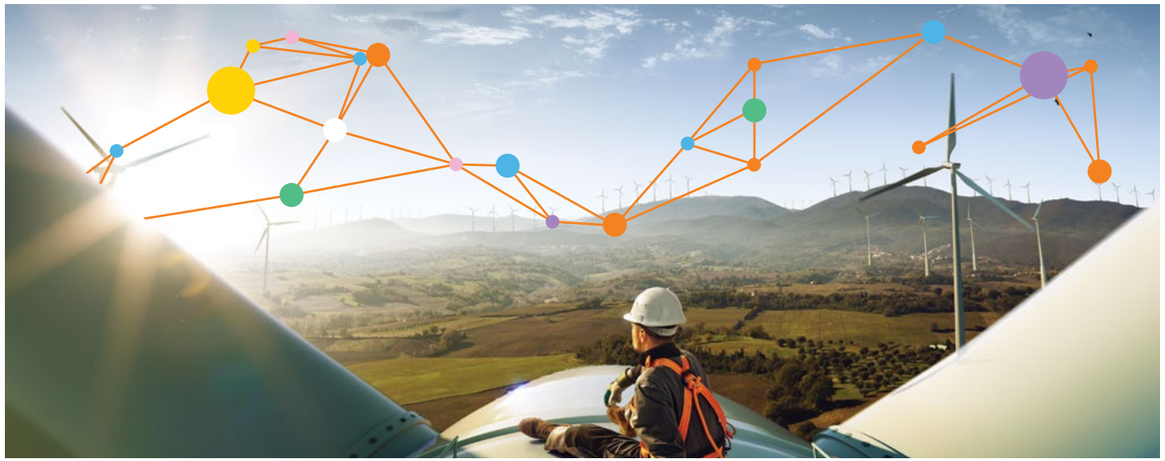
Ştefan Tarisnyas
Fixed Data Product Manager
Orange Business

When threats are all over the place it is more than clear that we need to secure our digital life and we've answered to that first question do we need it. Now the next question would be: there are a lot of things that needs to be protected, so what should I protect first? The answer is very simple: You need to protect everything, but this answer needs to be detailed! First, you should be aware that everything that goes online and uses a connectivity represent a possible target, therefore make sure your connectivity is safe. If it's not, then this is the first step to do for you or your business, make it safe, make it trustable.

Most of all cyber-attacks happen when your connectivity has weaknesses that you are not aware of, therefore contact your provider and ask for your security umbrella. Second, check your machines, your tools, your software and make sure they are running latest security versions, certificates, and updates. It is very important that you keep up the pace with the rest of the world. Be late and you'll become vulnerable, that's exactly what hackers are waiting. Last, but not least, protect your data and your data base. Make sure everything is safety saved, backed-up, encrypted and protected against any type of threats.

Another logical question that you may ask would be: where should I go to get my cyber security and what are the costs? Now when we want to answer this question, we need to look at the security market. There are lot of security providers out there, but do they give you everything you need for your business as an end-to-end solution? The answer is no, they give you only a small part of what you need, for example they don't offer you a connectivity solution nor a single point of contact for everything you need, that's why more than ten years ago IT and security suppliers embraced telecom providers to better respond to market needs creating more suitable offers for clients. Bundles have been created in collaboration between IT companies and telecom companies, each side knowing better own strengths with years of experience behind. In this regard, connectivity with security tools, security platforms responded better to market request, these partnerships have led to competitive bundling with overall lower costs.

For Orange, excellence in the delivery of complete solutions has always been in the foreground. Many years of experience, partnerships, highest standards, and skills delivered many end-to-end solutions and transformed Orange from a telecom provider to a multirole operator. Iaas, SaaS, PaaS are just few of our implemented solutions that meet most demanding requirements with cyber security being always the basis of everything. Our message for everyone is that future businesses can't exists without cybersecurity and the good news is that upgrading your safety you'll be able to upgrade your business model also, delivering better, fasters, safer.



Empower employees to securely access apps remotely

Companies around the world adapted to ever changing circumstances like work done from virtually anywhere, maintaining efficiency and at the same time staying connected with business partners and clients all this under the risk of cyberattacks and phishing or ransomware. An accelerated digital transformation must be taken into consideration to become more resilient, and companies should have more and more security as top of mind.

Microsoft gathers data insights including the cloud, endpoints, and the intelligent edge from over more than 24 trillion signals from a diverse set of products, services, and feeds around the globe. per day. For example last year in June, Microsoft reported to have blocked 9 billion endpoint threats, 31 Billion identity and 32 Billion e-mail threats.

Also, thousands of Microsoft security experts across 77 countries interpret and contribute to the insights gained from the advanced engineering and threat signals to come up with recommendations, analysis, and new solutions.

So, if we are to follow best practices for securing remote workforce the approach would be to start focusing and embarking into the Microsoft Zero Trust journey. Zero Trust is based on the principle: never trust, always verify! Treat each access request as though it originated from an uncontrolled network.

Every access request must be strongly authenticated, authorized within policy constraints, and inspected for anomalies before access is granted. Everything from the user's identity to the application's hosting environment must be verified to prevent any breach.

By Verifying identity and implementing an MFA policy (multi-factor authentication) you can prevent 99% of credential theft and the company is one step ahead in the security environment.

This can be done either using smart cards to control administrative access to servers or verifying the users' identity in multiple steps like login credentials. By Verifying devices, it takes another step toward enrolling into a device-management system and controlling who has access to what on specific devices. By Verify access into the network it must convey that employees use VPN and automatically route users and devices to appropriate network segments.

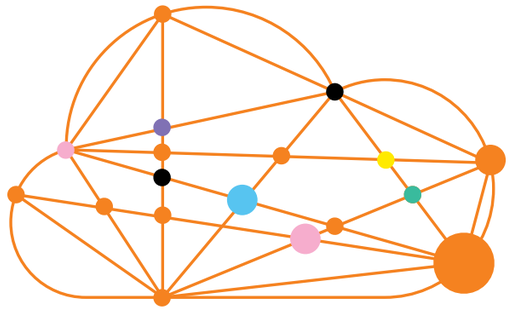
The environment will force companies more and more to evaluate such risks, and then set the appropriate goals. For conditional access, to focus on most used applications to ensure maximum coverage they should start with simple policies for example like device health enforcement, device lock or password complexity.

Also run pilots and rollouts, monitor VPN traffic to understand internal dependencies, assign performance indicators and goals for all workstreams and elements including employee feedback. User experience has shown to be critical to productivity and more over key to user adoption of security procedures and policies.

These recommendations are meant to minimize impact of risks and companies must learn to practice good cyber hygiene and implement architectures to support the principles of Zero Trust.

Soon companies should consider integrating cybersecurity into business decision making to protect from threats because at some point they will face cybersecurity threats. This could be from small actions like employees accessing unauthorized work data from personal devices to the most sophisticated ones.

So, they must be prepared! Every leader in the organization should consider how they enable employees and customers to have a better digital experience, while also considering what's needed to mitigate the associated risks.



Vulnerability Management

Organizations are unclear about whether they are successfully identifying breaches and incidents. The increasingly complex security services cause companies to turn to security professionals due to the lack of internal resources specialized in these areas. Compliance requirements in the field of cyber security (for example, the NIS Directive, GDPR, etc.) will lead to an increase in investments in this field, especially in managed services.

The outsourcing model of security services is recommended by the most prestigious analysis companies (IDC, Gartner, Forster) and is growing in popularity.

Vulnerability Management is quickly becoming a stop-gap solution for companies with an online presence that are not willing or capable of investing in high-cost or complex cybersecurity tools and services, Vulnerability Management platforms work by actively scanning a company's public assets, finding threats, ranking them and being capable of export to a SIEM or a SOC.

The benefits of adopting a vulnerability management platform:

- **Enhanced Reactivity:** You reduce the risk of potential exploitation of your security flaws by hackers through a proactive vulnerability assessment
- **Operational Efficiency:** The assessment of the vulnerability list helps IT security experts, to remediate the most critical security threats first and address the minor ones later.
- **Fast Reporting:** Cut off operational workload to report and prioritize security threats and comply with internal and external regulations.

Vulnerability Management platforms, implemented alongside other security tactics, are vital for organizations to minimize attacks and prioritize possible threats.

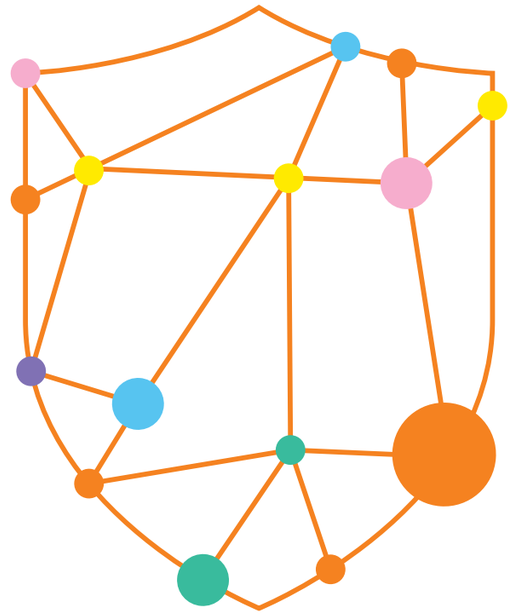
Cristian Turcin
Cloud & Professional Services Product Manager
Orange Business

Business Internet Security – insights and findings

Business Internet Solution (BIS) offered by Orange Services, available for medium and large companies, analyses more than 9 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 was 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. This report was generated by correlating anonymized information from multiple security systems deployed within our solutions such as NG-firewalls, web and e-mail security gateways, DDoS mitigation systems, intrusion detection systems and statistical data gathered from pen tests and security audits performed for our customers.

The information gathered from our Cyber Security Sensors is enriched in InfraAI through multiple Threat Intelligence Feeds, both commercial and open source. The information presented herein represents all findings from Q4 2021 up to Q3 2022.



Distribution of threats by business vertical

Threat distribution by business vertical in Romania closely resembles the wider, international distribution we can access from open sources. Compared to previously released data, there has been a substantial increase in overall volume of threats, across industries with significant detections happening in the Health and Pharma and Government and Public Services sectors. Public attribution through Open-Source Intelligence, reveals many of the attacks have been opportunistic, and triggered by the massive geopolitical unrest brought forward by Russia's invasion of Ukraine.

Distribution of threats by industry

Health and Pharma	32%
Govt. and Public Services	23%
Energy	22%
Retail	16%
Transportation	7%

Health and Pharma and the Government and Public Services infrastructures protected by BIS were the primary targets for large-scale, brute force, unsophisticated attacks like DDoS. More complex threats were detected and blocked, aiming to cripple Public Services systems, with ransomware a key threat for this year's campaigns.

The attacks were opportunistic, in their nature and seemingly (unsuccessfully) targeted high-visibility websites or webapps, aiming to affect availability and cause downtime and to a lesser extent, poking to find exploitable vulnerabilities in Internet-facing assets.

By correlating the business vertical data with source / origin information and open and custom Threat Intelligence, we established that many of the large-scale DDoS attacks were orchestrated from Russia and China and run through botnets.

Distribution of threats by region

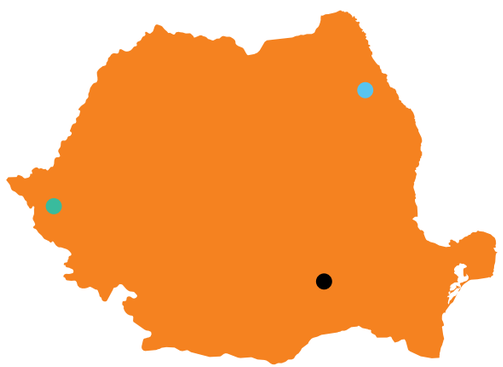
Within a nation-wide customer base, we gathered information related to attacks across-industries and distributed the volumes of attacks to the geographical localization of the targeted assets.

Bucharest was the worst-hit region, accounting for nearly half of all the attacks (48%), followed by Banat and Moldova.

Distribution of threats by region

Bucharest	48%
Banat	25%
Moldova	16%
Other regions	11%

As for the most affected cities in the past 12 months, Bucharest is in first place with an average of 970.000 attacks prevented each month, across all our customer base located there, with Timişoara in second place, on average with 260.000 attacks blocked each month and Iaşi counting for third place with almost 170.000 threats detected and blocked, each month.



Bucharest	970000
Timişoara	260000
Iaşi	170000

Distribution of threats by type

For the second year in row, Ransomware is still the principal culprit for the attacks detected and blocked by BIS, with DDoS coming in second and Phishing in third.

The volumes of DDoS attacks were normalized and distributed over a 12-months period, given that the months of April and May of 2022 brought large-scale DDoS activity from botnets with global coverage, used by hacktivists and state actors as cyberweapons during the Russian invasion of Ukraine.

Ransomware, however, is still the favourite among hacker groups and individuals as Ransomware-as-a-Service is becoming de-facto for launching cryptographic malware attacks, given the abundance of potential targets exposed on the Internet. BIS, however, uses state-of-the art detection and blocking capabilities to protect against some of the prolific variants and distribution platforms out there, maintaining an up-to-date threat detection capability leveraging high-end Threat Intelligence.

Distribution of threats by type

Ransomware	35%
DDoS	25%
Phishing	21%
Other	19%

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.

Distribution of threats by criticality

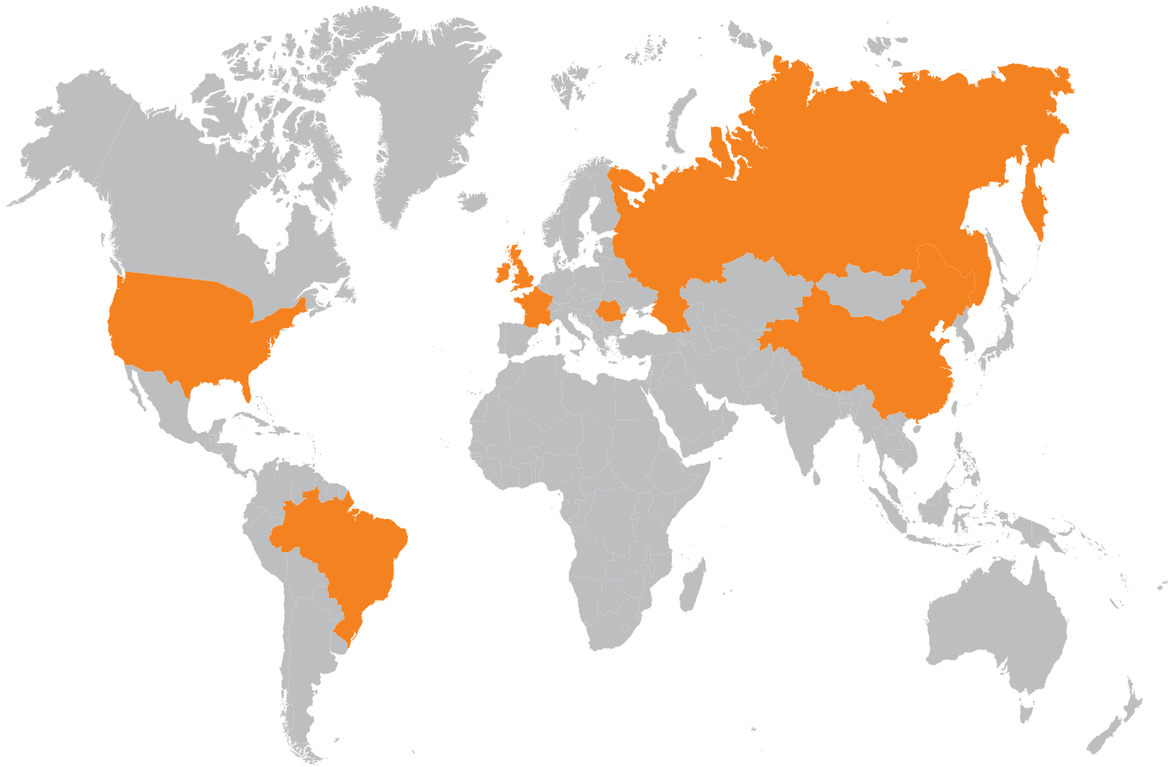
Critical	31%
High	16%
Medium	24%
Low	27%
Informational	2%

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 this info to specific geographies.

Source of attack by country and unique offenders



420.000	320.000	310.000	280.000	145.000	64.000	42.000
China	Romania	Russia	United States	United Kingdom	France	Brazil

Federating threat detection & response: next wave of Security Operation Centres

Pushed forward by the rise in volume and complexity of cyber threats, there is a real and immediate need to better integrate Cyber Security operational capabilities across societies – organizations and jurisdictions – in the private and public sectors. We, at Orange have strived to offer a holistic approach to Cyber Security for our customers and partners, with an end-to-end approach to proactive cyber security and operational cyber security. While the MSSP approach can -and does- offer a consolidated services offerings to customers looking for basic, perimetral security to more complex, threat management solutions, it lacks in the ability to scale to more federated needs.

Building a strong partnership between Academia and Private sector, on cyber security, has been a defining objective for several of Orange Romania's initiatives, such as Orange Education Program, the Orange 5G Lab and the researched performed in the various projects and programmes, and UNBreakable Romania, a first-of-its-kind national CTF competition for high-school and college-level, and University Students. For the past two decades, Orange has actively participated in providing the students of top-tier Universities in Romania, with up-to-date, hands-on knowledge and experimentation for new technologies and concepts, on topics of current and future generation communication networks, Internet of Things, Entrepreneurship, and Cyber Security.

Our logical follow-up to the existing initiatives in these partnerships is to advance the knowledge transfer on cyber security from Orange Romania's experts to the partner Universities and to provide them with a flexible toolset capable to be integrated in their Curriculum, to support the teaching of Cyber Security at a Bachelors' or Masters' level. We are doing this by providing content and a platform-as-a-Service for CyberEDU, a state-of-the-art virtual cyber range platform developed by one Orange Fab Start-up. By using CyberEDU, Universities can access pre-existing content, on cyber security topics and create their own content, and can make use of virtual laboratories for hands-on practice. Furthermore, CyberEDU allows individual performance monitoring for each student and handily integrates any Continuous Formation, Continuous Education processes and software platforms.

One key area of interest for our partnership is to develop regional and sectoral operational capabilities, to detect, response and recover from cyber security threats. Since the knowledge on how to design, build and run Security Operational Centres, is a subset of the common-core information we are transferring to our university partners, through our education programmes, our focus is now shifting towards helping to provide the technological stack and the processes required to create and operate SOCs, together with partner Universities.

To this end, we developed an approach to have partner Universities, from Romania, hosting and running Security Operations Centres, build on Open-Source technology to promote the capabilities to offer threat detection and threat response to regional beneficiaries from the private sector and the public sector. This approach enlists a technology stack delivered to a partner University, by Orange and key partners in the cyber security operations business, and to perform a strong integration of the University Curriculum on cyber security, with our continuous learning and virtual laboratory platform (CyberEDU). Once this technology stack is fully deployed, on-premises in the partner Universities, a knowledge transfer process is initiated, to ensure a fast capabilities build-up, for the analysts to operate at L2 levels.

As soon as the initial capabilities have been reached, the regional SOC can provide Managed Detection and Response services to private and public entities in their respective geographical (or administrative) regions.

The high-level architecture for these SOCs is based on continuous intelligence sharing between the regional SOCs and relevant national public entities, as such as DNSC and CyberINT. This enables a reliable and near real-time coordination to anticipate incoming threats and to pro-actively assign a protective posture and relies on real-time sharing of Indicators of Compromise and more complex, detailed, intelligence collected or generated within the SOCs.

As these SOCs will have an in-build capability to communicate with each other and "learn" and adapt to threats, incidents and scenarios as they are detected, this will enable an federated operational model, through which resources such as Threat Intelligence can be shared or consolidated, as needed.

We envision an initial deployment of 5 SOCs, in each of the social-economic regions of Romania, piloted with the top tier Universities.

On the opportunity of a Security Operations Centre within Ovidius University of Constanţa

Over the past two years, the context of the COVID pandemic has exposed several critical issues that public and private organizations have been forced to navigate in real time. Nowhere is the need for adaptation more compelling than in the world of cyber security. The year 2022, with the emergence of the armed conflict in the Ukrainian space, has further complicated the field of cyber security, affecting government institutions, public utility companies, banks, large corporations, and hospitals, producing chaos and endangering the health and even the lives of patients affected by blockages in many developed countries of the world, not least at the individual level.

Unfortunately, cyber-attacks and breaches are big "business" – malicious actors, state or otherwise, with a large stream of destructive motives populating the Internet, ready to attack insecure data and immature security practices.

Romania, and in particular Dobrogea, attracts the attention of attackers due to the presence of NATO bases and multinational companies that carry out activities here. The Cernavodă Nuclear-Electric Power Plant, the Constanţa commercial port, the Midia refinery, companies that drill in Romanian territorial waters, domestic and foreign banks, multinational military bases, all can be vulnerable to cyber-attacks.

Prevention and protection against cyber-attacks is a very topical issue at the international level. International security organizations, such as the National Security Agency (NSA), support the development of education in the field of Cybersecurity, by establishing and supporting academic centres of excellence, in which bachelor's and master's programs aimed at advanced training in the field of information security are held.

In a region heavily tested by the existence of ongoing or frozen military conflicts, the Ovidius University of Constanta is a constant promoter of democratic values and the rule of law, a benchmark for the entire Black Sea basin. Political, military, economic, resource and environmental regional security issues are the subject of existing study programs within the university. The interdisciplinary approach, from the perspective of political sciences, of sustainable development in terms of environmental protection and the promotion of democracy and social justice goes beyond the limited space of the lecture halls and spills over the many international scientific events that are organized every year on the shores of the Black Sea.

Ovidius University of Constanţa, is a public higher education institution which provide a constant pool of talented students, with innovative ideas in very diverse fields of study, including informatics/computer science as well as the priority sectors of the region. In particular, the expertise in cybersecurity should be emphasized, as the university will

Alexandru Bobe
Vice-Rector
Ovidius University of Constanţa

provide a high-level design of a Security Operations Centre architecture, to be initially piloted with one partner and then replicated across SE Romania.

The mission of the Cyber Innovation Hub technological transfer platform is to facilitate innovation in the field of cyber security and to accelerate the technological transfer of Ovidius University of Constanța (OUC) specialists and those of partner institutions to public and private institutions, to implement the regional development strategy. The expected impact will be to strengthen the procedures and technology used in the protection of data and IT systems in the south-eastern region of Romania, positively affecting the regional partners, but also those from the entire area of the Black Sea and the south-eastern flank of NATO, also contributing to the development of mechanisms for informing and raising awareness of society regarding good cyber security practices.

An important achievement of the UOC is the alignment with the European Union's digitalization priorities. In this regard, the university submitted a funding application for the digital innovation centre (DIH) CiTyInnoHub, established in 2017, and which in 2018 was selected by the European Commission as one of the 5 digital innovation centres in Romania. Its selection in the European Commission's Smart Factories in New EU Member States training and technical assistance program, provided by PwC and Oxford, funded by Horizon 2020, enabled staff training and an action plan for digital transformation to be drawn up. Based on these reasons, CiTyInnoHub has become a digital innovation centre orchestrated by UOC in partnership with local authorities, the Chamber of Commerce, employers' associations, and companies with experience in the field of consulting and digital transformation. The development of the centre allowed the elaboration of a strong application in the national competition launched in 2020 by the Romanian Digitalization Authority, resulting in the fact that the Digital Innovation Centre orchestrated by UOC was selected to enter the European competition to become a European Digital Innovation Hub. To ensure a broad collaboration framework, as well as coherence and complementarity in priorities, CiTyInnoHub has joined the Association of Digital Innovation Centres in Romania (RO-DIH) and in June 2022 has gained the competition and now is a European Digital Innovation Hub having cybersecurity as the main component.

The selection of the CiTyInnoHub as European Digital Innovation Hub was also based on existing previous collaborations. Ovidius University of Constanța, along with the Romanian Intelligence Service's National Cyberint Centre, Romanian National Security Incident Response Team, and Orange Romania have been partners of Ovidius University in the HCOP 2014-2020 project Pro-Info, which had as key objectives to provide a training program in cybersecurity and to create a Cyber Lab.
Therefore, it is natural to consider an investment in human resources, as a central element in increasing the level of security at the level of society, whose benefits and effects will be felt at all macro and micro levels of society.

We can encounter into university environment, among the multitude of types of attacks, such as: phishing, compromising accounts and computer systems, illegal downloading of software or files, attacks on databases and activity logs, use of computer systems or networks for the purpose of generating spam, the possible use of computer systems on university campuses in DDoS attacks, or even theft of identity data or intellectual property.

It is necessary for it to have both a team of trained cyber security professionals and the necessary technical architecture, organized in the form of a SOC. Only in this way, the university will be able to respond to possible cyber risks and threats, on the one hand, but also to contribute to increasing the level of education of the entire academic community, on the other hand. At the same time, educational institutions must adopt administrative measures and security policies to maintain a balance between the need for free access into IT systems and services and ensuring cyber security at one acceptable level.

Therefore, at the level of our university, it is necessary to improve actual strategy, to plan, implement and realize a Security Operations Centre (SOC). The objectives of this component are to address operational cybersecurity needs, minimize cybersecurity costs, and protect institutional assets using IT infrastructure and network defence capabilities, as well as train students in the best practices of cyber security, which can then be transposed to society.

In our view, the present project proposed by Orange Romania is ready to assume the responsibility of this investment, by involving the participating university centres, specifically in the exact sciences of mathematics, informatics, computers and information technologies, in the training of specialists who can form the basis of selection for governmental or non-governmental institutions (economic entities), in the improvement of cyber security culture at mass level, in the development of cooperation between the public and private environment, in order to ensure cyber security, through the education of human resources, the exchange of information and good practices.

Challenging the future of cyber security

Andrei Mihai Crăciun
Head of Digital Transformation and Data Analysis
West University of Timişoara

It was no later than 9 PM the day I started to write this article and, all over the world, more than 16.2 million cyber-attacks were identified and publicly exposed by the live threat map maintained by a global CyberOps supplier (CheckPoint). The top 3 targeted industries are Education, Healthcare, and different Governmental facilities. Between 2020 and 2021, the attacks on educational infrastructure have risen by 75%, according to the same source. Fortinet's live Threat Map was also full of DDOS and Remote execution attacks.

Daily, tens of millions of threats catch the specialized organizations' eyes, as cyber criminals are accessing and creating complex tools to plan, direct and execute their attacks. The highest impact malware types are adware, phishing, and exploited backdoors, ways in which cybercriminals are controlling technology to reach their goals.

If we are analysing from a wider standing point, malware does not work alone, rarely are their threats that are not controlled remotely, that is, not sending and/or controlling/ingesting data into a victim system. You need tools, servers/data clusters, practically entire attack frameworks, and deployment networks. These infrastructures are completely controlled, work systematically, and often are extremely hard to defend.

If we are talking about targeted industries, it is safe to say that Education is at the top. Usually, in education, you get a lot of equipment - diverse tech, connected usually via the best high-speed bandwidth routes. If the pandemic years taught us something, that would be the fact that we need to learn and adapt at a fast pace; but to reach far, we need to keep a close eye on the security of our infrastructures.

There is a catch here though, related not necessarily only to people and salaries, not only to top tier tech involved but, more importantly, how you can shift organizational focus from a reactive to a proactive digital security approach. Organizations need to embrace new relevant strategies that are heading beyond only monitoring, and towards actively blocking attacks and hacking attempts at the source before they can do any kind of damage.

Education has a central role and a huge opportunity at its doorsteps. Cyberspace stopped being a buzzword a long time ago. Fostering talent able to develop, integrate and monitor their own digital ecosystems and data networks is no longer a choice for universities, but a mandatory landmark.

Nevertheless, there is much more on the horizon. Universities need to develop real and active partnerships with organizations that not only hold the best expertise on the current technologies and cyber threats but can see beyond the obvious toward emergent challenges.

Advanced security, monitoring, and intervention is not a simple task, and the full stack range of Orange services helped us understand how you can balance and protect your data systems and develop advanced tools to best optimize your workflows. From an active cybersecurity standing point of control, public-private partnerships is the only approach that makes sense. Operating a security advanced node/

cluster implies, in addition to good hardware infrastructure, an extremely well-balanced team of highly skilled professionals with a comprehensive set of software and hardware tools to back up their work. It might just be the perfect mix, the emerging talent from Universities, the skills, experience, procedures, and active knowledge of well-established professionals. It might just be the right answer to the dilemma: how do we improve overall security within educational infrastructure and promote and deploy best practices?

The next 5-7 years will bring a generational shift in technology, tools, and advanced public services. Data-related security, availability, and preemptive forensics will transform and augment further the role of education in society. There is a simple approach to this that holds an easy choice: wait for “something to be done, somebody to bring the next” or build the tools, frameworks, and security within a relevant partnership. The goal should not be to lower the number of attacks but to better protect all relevant ecosystems, not only the critical ones.

Midnight summed up, more than 21 million attacks identified at a global level. But still, I estimate tens of thousands of command-and-control frameworks are waiting for the next victims. Let’s not give them the opportunity to operate.

Education, Innovation and Research

Education through Gamification - Unbreakable Romania

UNbreakable Romania is the end-to-end Cybersecurity Educational Program for High schools and University students from Romania. It offers a detailed landscape of cybersecurity skills at national level and aims to identify and encourage talents as to mitigate the skill gap in the cybersecurity field and supporting organisations and institutions to build strong defences.

The main goal is to increase cybersecurity expertise at a national level and provide guidance for young talents interested in pursuing a career in the industry.

The vision behind UNbreakable is to have ongoing competitions, split between two seasons, starting in early-spring, and hosting the second season in late-autumn.

The participants go through an informative journey of boot-camp themed training sessions on multiple topics then move on to participate in Capture-The-Flag competitions, in both individual and team settings.

The participants gain access to trainings and webinars on Network Tools, Cryptography, Web Applications Security, 5G and Wireless Security, Cloud Security, Forensics and Computer Investigations, Reverse Engineering, through and extensive 30+ hours of online tutoring conducted by leading industry experts.

We launched this competition in 2020 through two pilot CTFs for participants of all ages, high-school, or University students. The results encouraged us to continue to invest in further developing UNbreakable, through partnerships with leading Romanian Academia – Universities and High-Schools, and to offer a content-rich, informative, and lucrative tutoring concept for all participants.

In 2021 UNBreakable transformed into a year-round competition, with two seasons of qualifiers and play-offs, to better suit the Gamification concept and to allow individuals and teams to train and practice through a curriculum aligned with their school schedules.

We created two ‘seasons’ – spring-summer and autumn – winter, and we invited guest lecturers to disseminate their expertise in Bootcamp-like training sessions, on topics of up-to-date interest: cryptography, reverse engineering, web security, network security, mobile networks, and mobile devices security etc.

During 2022 we further consolidated the scheduled into a single competition, this to better align with the school and University calendars which were still recovering from the disruption COVID brought on.

593 individuals participated in the competition, representing 40 of the 41 Counties in Romania, Students of 35 Universities and 75 High-Schools and Colleges. The numbers are impressive and representatives for the popularity of UNBreakable among participants, and it is well reflected in the results obtained by the players, where double-digit percentage increases are visible, from the 2021 results in most of the categories of challenges played in the CTF.

As in the previous years, each participant had received their individual performance evaluation, post-competition, a detailed report on how their skills is progressing from season to season and how they rank up to other players in the CTF.

2023 will start a new season, with registration to open in Early March and the CTF to be scheduled by late-April / early May.

Aggregated performance indicators and information is available on Orange Threatmap in the RoCyberEDU Skills Sections.

Innovation in Cybersecurity - Orange Fab startups

Orange Fab Romania is part of the Orange Fab international network of accelerators, currently operating in 18 countries across the globe. In Romania the program started in 2017 and, from the very beginning, had a dedicated Security track.

Orange Fab offers innovative start-ups 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 Start-ups from Orange Fab

StageOne

StageOne is a disruptive tool that allows employing complex adversarial techniques against the target infrastructure in order to find vulnerabilities and helps mitigate them before an actual attacker can manipulate them. The tool prepares the organizations to face advanced cyber-attacks demonstrating the (in)effectiveness of their security program.

www.stageone.ai/

Dekeneas

Web Security solution using artificial intelligence to address some of the most complex and hard to tackle computer attacks: watering holes and crypto jacking.

www.dekeneas.com

Rungutan

Rungutan is 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.

www.rungutan.com

Siscale

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

www.siscale.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.

www.cyberedu.ro

Core AntiVirus

Core AntiVirus - is a state-of-the-art product that uses a minimal range of resources, offers realtime protection, manual and scheduled scans, Cloud protection and an interface for remote configuration. Using advanced Artificial Intelligence, it instantly detects and blocks the latest threats before they cause damage to the device.

/www.corecyberdefense.com

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.

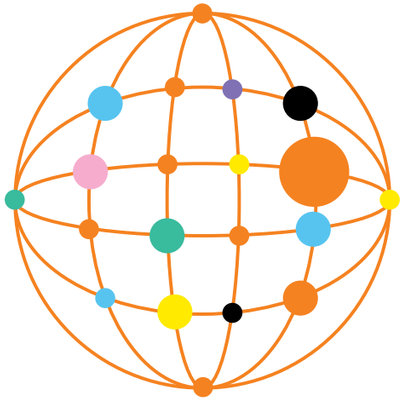
www.pentest-tools.com

Research - H2020 and Horizon Europe Projects

What is Horizon 2020? - Horizon 2020 was the biggest EU Research and Innovation programme ever with nearly €80 billions of funding available over 7 years (2014 to 2021) – in addition to the private investment that this money will attract. It promises more breakthroughs, discoveries, and world-firsts by taking great ideas from the lab to the market. By coupling research and innovation, Horizon 2020 is helping achieve this with its emphasis on excellent science, industrial leadership and tackling societal challenges. The goal is to ensure Europe produces world class science, removes barriers to innovation and makes it easier for the public and private sectors to work together in delivering innovation. Its high-level goals are being continued through Horizon Europe.

What is Horizon Europe? - Horizon Europe is the EU's key funding programme for research and innovation with a budget of almost 100 billion Euros. It tackles climate change, helps to achieve the UN's Sustainable Development Goals, and boosts the EU's competitiveness and growth.

The programme facilitates collaboration and strengthens the impact of research and innovation in developing, supporting, and implementing EU policies while tackling global challenges. It supports creating and better dispersing of excellent knowledge and technologies. It creates jobs, fully engages the EU's talent pool, boosts economic growth, promotes industrial competitiveness, and optimises investment impact within a strengthened European Research Area.



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 5G 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 5G 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 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.

https://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 (5G 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.

www.vital5g.eu/

EU-CIP

The main goal of European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (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 operators, authorities, and innovators. EU-CIP is due to start in Early October 2022 and will continue for 3 years, up to 2025

Bring Your Own Device (BYOD) and mobile security

Personal smartphones and mobile devices permit employee access to corporate email and network resources but add a vulnerable entry point that can be exploited. Additionally, document sharing enables mobile devices to further proliferate corporate resources outside of a potentially compromised network infrastructure.

Bring Your Own Device (BYOD) and Corporate Owned Personally Enabled (COPE) strategies accelerated during the COVID-19 pandemic. While enterprises enjoyed the productivity of continuous connectivity, IT admins on the other hand were blind-sided with protecting corporate owned devices from the massive amounts of insecure personal data employees began keeping on their phones. With both BYOD/COPE and cyber-attacks increasing, the scramble to analyse the facts and figures ensued in hopes of finding a way to manage the escalating problem.

Enterprise data is finding its way on employee smartphones as the new norm for corporate efficiency. Corporate smartphones have increased productivity by placing work and personal data on the same device but has compounded enterprise security exponentially. Mobile devices expose numerous pathways through which sensitive data can be stolen (sharing data with untrusted third-party applications, device theft, intentional rooting, misconfigured, or vulnerable enterprise applications). These vulnerabilities grow exponentially across an organization, when hundreds or even thousands of devices require secure management, configuration, and deployment.

Samsung Knox enhances your business workflow, providing IT admins with comprehensive solutions to make managing the entire device life cycle simple, secure, and efficient. The Knox Platform provides a robust set of features to fill security and management gaps, resolve pain points identified by enterprises, and meet the strict requirements of highly regulated industries.

Hardware-backed security

The Knox Platform defends against security threats and protects enterprise data through layers of security built on top of a hardware-backed trusted environment.

- Trusted environment — A trusted environment separates security-critical code from the rest of the operating system. This strategic separation ensures only trusted processes that are isolated and protected from attacks and exploits can perform sensitive operations, such as user authentication and key encryption and decryption. Trusted environments perform integrity checks prior to executing any software. These checks detect malicious attempts to modify the trusted environment and the software running on the device.

- Hardware-backed — A trusted environment is hardware-backed if hardware protections isolate the environment from the rest of the running system. This isolation ensures that vulnerabilities in the main operating system don't directly affect the security of the trusted environment. The environment also ties integrity checks of the software running in the trusted environment to cryptographic signatures stored in the device hardware. Hardware-backed integrity checks prevent an attacker from exploiting software vulnerabilities to bypass protections and load unapproved software into the trusted environment.

The Knox Platform uses a hardware-backed trusted environment, and the specific components depend on the device hardware. For example, ARM processors provide a Trusted Execution Environment (TEE) that leverages components such as the ARM TrustZone, ARM Hypervisor Mode, and Embedded Secure Elements. Knox features that use the trusted environment include Real-time Kernel Protection (RKP), Trusted Boot, Device Health Attestation, Certificate Management, Sensitive Data Protection (SDP), and Network Platform Analytics (NPA).

Furthermore, the Knox Vault introduced with the Samsung Galaxy S21 offers an isolated, tamper-proof, secure subsystem with its own processor and memory. Knox Vault operates completely independently from the primary processor running the Android OS, and guards against attacks that exploit shared resources, such as software side-channel attacks that can compromise other software executing on the same processor. This separation means Knox Vault protects sensitive data even if the primary processor itself is completely compromised.

App isolation

The Knox Platform uses app isolation to prevent

rogue apps from intentionally or inadvertently accessing unauthorized data. The Knox Platform provides several forms of app isolation to create a protected app container space on Samsung devices. Each option is based on the same core isolation technology called Security Enhancements for Android (SE for Android.) SE for Android is an integration of SELinux and Android, expanded to cover Android components and design paradigms. The Knox Platform offers these options:

- Android Enterprise on Samsung devices — Android Enterprise provides app isolation through work profiles, which provide basic isolation of enterprise apps from personal apps. When using Android Enterprise on Samsung devices, Knox provides features like Real-time Kernel Protection (RKP), secure enterprise apps, and hardware-backed storage of certificates and keys, making Android Enterprise even better on Samsung devices.

- Separated Apps — For enterprises that need full control over a corporate-owned device, while still enabling authorized third-party business apps, Samsung exclusively offers Separated Apps to isolate third-party apps in a sandboxed folder.

- SE for Android Management Service (SEAMS) — With SEAMS, you can isolate a single app or small set of trusted apps, to lock down the apps in the same container. SEAMS containers have no special GUI. Apps in a SEAMS container appears with the rest of the apps on the device but are differentiated with a shield badge to show that they're isolated and protected from apps not sharing their same container. You can create as many of these SEAMS containers as you want on-the-fly.

Data protection

Enterprises can protect personal and enterprise data on mobile devices using a rich set of Knox features:

- User authentication — Samsung Knox devices support not just password, PIN, and pattern authentication but also the latest biometric authentication such as ultrasonic fingerprint sensors. Options are available for both device lock screen authentication as well as work profile authentication. Through the Knox Platform, you can enforce two-factor authentication or enterprise AD credentials for the work profile to ensure stronger data protection.

- Encryption of device data — Samsung Knox devices provide data encryption through Sensitive Data Protection, which binds to the hardware-backed Root of Trust and user authentication. This encryption ensures data is decrypted only on the device where the data is stored, and only by the device owner. DualDAR Encryption offers two instances of encryption to achieve an even higher level of reliability.

- Encryption of network data — Samsung Knox devices offer the widest selection of advanced VPN features, providing the ability to configure a separate VPN for individual apps to reinforce data isolation even further. Knox also offers always-on VPN, on-demand VPN, on-premises VPN bypass, HTTP proxy over VPN, multiple active tunnels, strict data leakage controls, and VPN chaining or cascading.

- Device tracking, locking, and erasing — Samsung Knox devices offer the ability to track, geofence, and automatically lock devices based on events and security policies. For example, a device that leaves a specified geographic perimeter is locked, wiped of data, or reset to factory defaults.

Knox is the most comprehensively secure and manageable mobile device solution for enterprises large and small. Samsung continually works with global government organizations and international regulatory bodies to meet a wide range of certification requirements designed to protect public safety and consumer privacy. Find out more about the Knox ecosystem on **docs.samsungknox.com.**

Predictions for 2023

Our predictions on what to watch for in 2023 and beyond stem from the Global unrest led by the geopolitical factors – the war in Ukraine, the rising tensions in the Pacific and in the Middle East, and by the normalization in post-pandemic societies. There is a clear, in plain-sight deviation from the evolutionary path of cyber threats of before 2020 which leads to a better pronounced malicious activities targeting of Critical infrastructures and a dominance of high-profile, high-gain state actors sponsored attacks. Unfortunately, it is our take that these are going to be the highlights of next year as it has been for the better part of 2022.

IoT / ICS vulnerabilities and Attacks – IoT is becoming mainstream in homes and small business while ICS is more visible to attackers and defenders, alike, due to its role in Critical Infrastructures. We believe 2023 to bring forward new vulnerabilities, across the stacks of IoT/ICS in both commercial-grade platforms and highly specialized ICS platforms. The red line bordering IT and OT is going to become faded as malicious actors with great technical and tactical capabilities are going to increase their probing and testing of such systems. Cyberwarfare is going to be part of the news cycle, with critical infrastructures targeted across the globe, with limited success.

On the personal use and home-front, IoT are becoming widespread, with reports estimating the total number of IoT-class devices up to 65 billion in 2025. As these devices generally have a less security compared to smartphones or computers, we expect it to become a favourable target for attackers and to further expand the attack surface of individuals or households and SMEs.

Cyberwarfare – there is going to be a visible and worrisome increase in state-sponsored or state-regulated cybercrime against other states, private companies, and public institutions. The motivation will probably stem from the current geopolitical tensions and the tools and techniques to be used are going to be increasingly high-end. The (virtually) unlimited resources put at the disposal of such malicious actors, by powerful nations means that current defences are going to have to keep up with an increasing volume of Zero-Day attacks, targeted Social Engineering, attacks to ICS/Critical Infrastructures and a very large volume of disinformation and fake news spread through social networks and state-run media outlets.

Cyberwarfare has clear advantages over traditional, kinetic warfare, in terms of economics, and (lack) of policies or it can benefit from ambiguous policies. This adds to the attractiveness of such involvement, from state-actors otherwise involved in traditional wars. Given the capabilities of distributing at large-scale, coordinated and targeted attacks over ultra-high speed, low latencies connectivity, cyberwarfare will impact societies for the foreseeable future.

Adversarial Artificial Intelligence – Machine Learning (ML) has become an established process in most cyber security areas. In defensive cyber security we extensively use ML to better understand the context of an incident and to identify patterns. The using of ML is becoming ever more predictive in nature, as we're looking forward to build capabilities of automated detection and response, based on the anticipation of attacks. The reversal of this is that A.I. will become an adversarial tool which can be used by defenders and attackers alike, to either anticipate attacks or to anticipate defensive techniques. We expect malicious actors to increase their usage of Artificial Intelligence methods and tools to further develop their capabilities of targeting of assets, to generate new malware variants and to create new methods for obfuscation of malware and detection prevention.

Furthermore, as there is a growing interest in using threat-as-a-service platforms, from malicious actors who wish to automate their activities and leverage operational efficiency, we believe that these so-called platforms to better enable the usage of Machine Learning, to add to their efficiency.

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.

IoT 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.

Visual Basic™ Macro A Visual Basic Macro is a type of computer code widely used to automate repetitive tasks in working with multiple data inputs from applications such as Microsoft Excel and Microsoft Word. When used in a cyber-attack it can execute malicious code on the victim's computer.

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
Andreea OCHIANĂ, Business Communication Specialist
Miruna PREDA-ŞINCA, Business Services Marketing Manager
Ştefan BUZEA, Graphic Design and DTP

Orange Fab

Startup accelerator program

orangefab.ro

Apply for Orange Fab if you are a technology researcher or innovator, and you can get access to:

- **Orange 5G Lab with the newest technology and equipment**
- **Mentoring to turn youe ideas into sustainable business**
- **Clients & pilot projects supported by Orange**
- **National and international exposure**