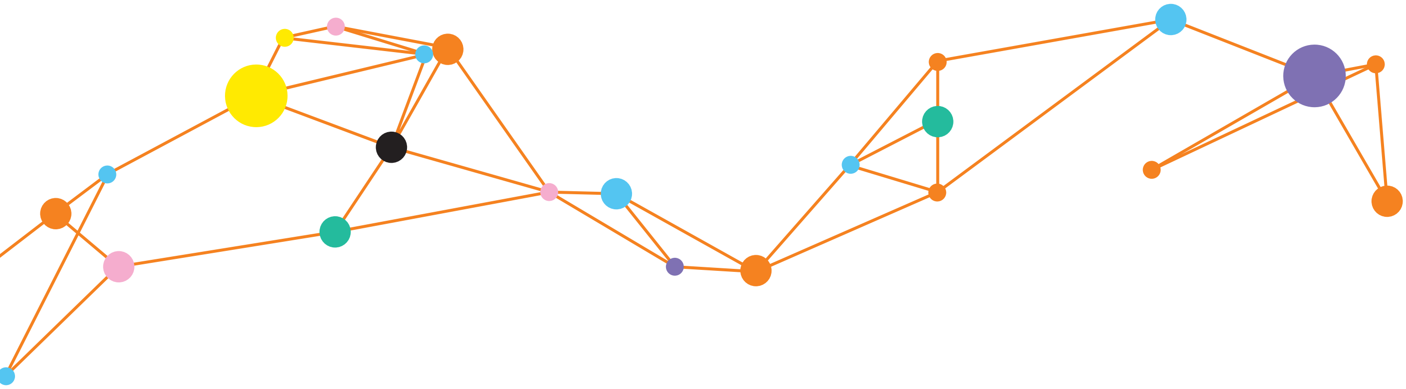
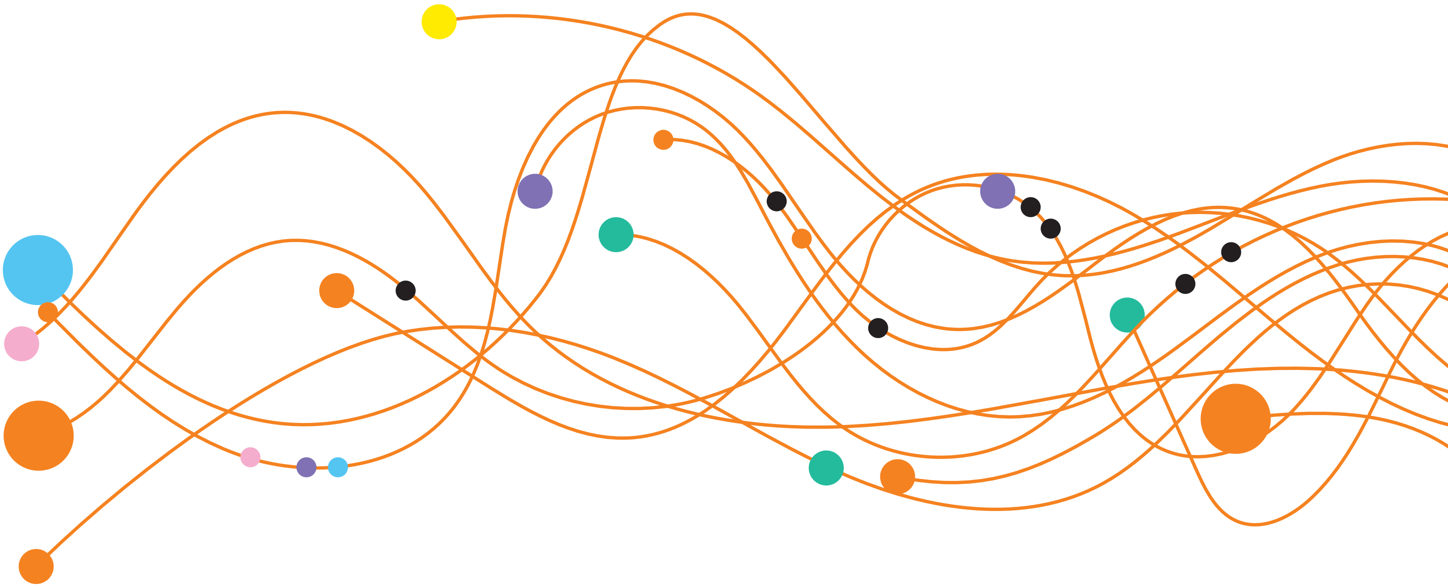
Business
Services

Business Internet Security Report

4th edition, 2021



Contents



Business Internet Security report 2021

Cybersecurity has been a hot topic in the last few years as the number of cyberattacks kept increasing and as hackers found new ways to challenge the IT infrastructures and the security systems of individuals, institutions and companies alike. With the emergence of COVID-19, companies and institutions tried to quickly adapt to the new reality by adopting online services more than ever before and by moving most of their employees in remote or hybrid work. This has created the perfect opportunity for hackers to manipulate or steal data and to exploit vulnerabilities of organizations' security infrastructure that the shift to remote work has exposed.

Now, almost two years in the pandemic, security and risk management are more than ever a top priority for organizations and as the number and complexity of cyber-attacks keep rising, security is placed at the forefront of business decisions. This has also become increasingly a matter of getting and maintaining your customers' trust. Digitalization has been given a tremendous push over the recent period, which goes in pair with enhanced exposure and security concern.

In this challenging digital landscape education, increased awareness and proactive measures are the key to protecting personal as well as business data. In this regard, we remain committed to support education through partnerships with universities all across the country and joint collaborations in our EU research and innovation programs, all with the aim to grow new experts in this field. That is why we are testing interactive cyber-security focused learning and practice platforms such as CyberEDU that has been used to stage ”Unbreakable Romania” as well as the RO-CSC – Romanian Cyber Security Challenge National Competition. Another example is our initiative to engage students and teachers in education through gamification, by piloting UNBreakable Romania, a first of its kind CTF (Capture The Flag) competition in cyber security for all pupils and students. In addition, partnerships and collaborations with startups through programs such as Orange Fab are key for the development of new technologies, business and cyber security awareness in Romania.

Our annual Business Internet Security Report offers a holistic overview of the main cybersecurity threats, the challenges of the past year as well as predictions for 2022. I hope you will find it useful and that it will bring value to your business.

Emmanuel Chautard - Chief Technology Officer,
Orange Romania

2021 highlights

2021 continued the trends set forth by the changes brought on by the Pandemic in 2020. The remote-friendly model and the fast-pace adaptation of remote-everything solutions added to the narrative that is becoming mainstream - cybersecurity threats are exploiting the ”new normal” and this ”new” normal means increased attack surface.

Businesses continued their transition to cloud services and cloud infrastructures and are becoming more reliant on A.I.-enabled monitoring and performance optimization solutions.

Cyber criminals are becoming more interested in the supply chain paradigm as are the ”blue” teams. Potential catastrophic failures in supply chains with the extreme impact of the possible cascading effects of such failures lead to a 2021 filled to the brim with call to actions on improving resilience and response capabilities for critical infrastructures, from both governments and private institutions.

Notable outcomes of this complex ecosystem of threats and defenses have materialized in the realization of the importance of communications, cooperation and communities in dealing with cybercriminals.

Targets have been a mixed bag of companies and individuals across most business verticals but there has been a more consistent focus on transportation and the healthcare sector, two of the principal infrastructures influencing the outcome of the ongoing pandemic.

Ransomware had its big comeback with an entire business model of Ransomware-as-a-Service (RaaS) being adopted to scale. Ransomware has been used, in 2021, to inflict compromise on sophisticated supply chain attacks, such as the Colonial Pipeline attack during the summer of 2021. Managed service providers were still prime targets for ransomware but so did healthcare facilities with some **82 incidents** tracked to US healthcare providers alone, by mid-2021. This is not to say other verticals were neglected by Ransomware - the public sector and national or regional government organizations were, again, prime real estate for RaaS groups. Romania saw at least 4 publicized incidents - fortunately - with a low overall impact.

Phishing is still the principal vector of compromise for most types of threats, from malware and ransomware to data stealing or crypto jacking and most businesses are still far from the necessary level of employee awareness to mitigate this important way-in for malicious actors and malicious code. As a matter of fact, a Phishing-as-a-Service model is gaining prevalence, offering easy onboarding and deployment for all cybercriminals and wannabes. What was true for DDoS orchestration, back in 2015, is now true for actors wanting to conduct Phishing Campaigns - they rent or subscribe to services that allows them to easily architect, launch and monitor campaigns and even balance their earnings through integration with crypto-payment portals or scammer call centers tools.

DDoS on shifting targets - IoT is of special interest to DDoS C2C controllers as the sheer diversity of manufacturers, models, firmwares and communication protocols make this category of devices into a robust, powerful and non-discerning botnet. As these devices gain on intelligence through iteration, so is the gain in communication capabilities - more and more are enabling high-bandwidth comms and this transforms our benign home gateway into a 1 Gbps-capable DoS-inducing machine. 2021 saw increasing interest from C2C herders and controllers to home IoT devices and there has been prevalent interest in ICS-class devices, although it remains an obfuscated affair for most cybercriminals.

Managed Security Services Evolve with The Pandemic

The pandemic situation that burst almost one year and a half ago with no clear horizon to end has profoundly impacted the workplace reality for many companies. Many organizations have been facing a new business and operational agenda, including topics related to cybersecurity issues affecting security system deployments, artificial intelligence and other emerging technologies, remote work strategies with a new focus on the employee experience in the workplace and disruptions in the business continuity.

Today, however, the COVID-19 pandemic has forced many companies to scramble into alternative business operations and execute many decisions unexpectedly. Many technologies that were initially used on-prem have embraced the cloud-based model and started to be delivered as managed services, including security.

Simultaneously, other factors such as socio-economic and political unrest, cybersecurity developments and privacy laws can complicate security planning. Lastly, at the beginning of the pandemic, some companies found themselves unprepared to assess technology in a meaningful way. Many of them embraced new technologies with little planning, but there were also happy cases when the adoption led to solving immediate business needs, thus improving the companies' ability to respond to the new challenges.

Now more than ever, operations, IT and security professionals are working to find ways to address these concerns and leverage various technology solutions that will help them secure and scale their operations. Many end-users are working closely with a managed service provider as an extension of their in-house teams to help identify the best and most effective solutions, including the partial or full outsourcing of the security functions.

Remote VPN connections, instant expansion of bandwidth to support increased digital and collaboration applications, deployment of secured WAN services to pop-up instant networks across locations, contactless access control systems and temperature monitoring solutions are just a few examples of technologies delivered under the managed service model.

The Covid pandemic opened up the Pandora of MSP (Managed Service Providers) as trustworthy partners to be considered even from the initial technology deployments. Migrating to the cloud and setting up cloud networking requires advanced skill sets and experience in order to right-size and optimize. Rather than waiting until the network is up and running to bring in an MSP for maintenance and management purposes, organizations are seeing the benefit of including them during the initial planning and migration.

Security, as a managed service, is also increasing in popularity, allowing organizations to maintain exceptional security posture while still being able to dedicate IT resources to other priority areas. With more remote workers and constantly evolving cybersecurity threats, there's a greater demand for advanced protection. That's driven the rise in adopting managed security services in several areas such as SIEM (Security Event Management System) as a Service, SOC (Security Operation Center) as a Service, Firewall as Service or Remote Managed Endpoints.

Laurentiu Popescu, Security Product Manager, Orange Business Services

My business aplications are always protected

Disaster Recovery: a solution for data recovery after major incidents

You have easy and fast access to the data and business applications prior to the cyber attack.

More details on
www.orange.ro/business

Business
Services

orange™

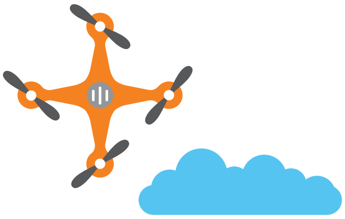
Timeline of events

September 2020

■ Norway's parliament attacked by hackers - A "vast" cyberattack targeted the Norwegian Parliament, in September 2020, attackers gained access to emails of Members of the Parliament and employees. An undisclosed number of accounts **have been compromised** and the attackers exfiltrated "various quantities" of data.

■ Newcastle University, victims of an Ransomware attack - Newcastle University was another victim in the ongoing Ransomware epidemic that started in early 2020. The DoppelPaymer group had breached the University's systems on September 4, 2021 causing **large-scale disruption** of services availability in the wake of the start of a new school year.

■ Public Health Wales accidentally publishes 18,000 coronavirus patients' data - Public Health Wales has confirmed that it accidentally published the personal data of 18,105 people who tested positive for coronavirus. The information was accessible on a publicly accessible server for 20 hours on 30 August. In most cases, patients' initials, dates of birth, geographical area and gender **were exposed**, which fortunately presents little risk.



October 2020

■ Massive Nitro data breach impacts Microsoft, Google, Apple, more - On October 21st, Nitro Software issued an advisory to the Australia Stock Exchange, stating that they were affected by a "low impact security incident" but that no customer data was impacted.Further investigations by CyberSecurity outlet, Cybel, confirmed one user was selling 1TB worth of PII, documents and databases for **USD 80.000**.

■ Enel Group hit with ransomware - After being affected by the Snake ransomware, in June 2020, Enel Group was the target of an attack by Netwalker with a ransom tag of USD 14M. The malicious group published screenshots showing several TB of data supposedly stolen from **Enel**.

■ Chinese Hackers Steal Personal Data of Half of Taiwan's Workforce - Chinese hackers have allegedly stolen data of nearly six million Taiwanese. The largest data breach in the country's history, Chinese hackers targeted a Taiwanese job bank and sold the data on the dark web as per authorities. Taiwanese official stated the data repository was some **9 years old**.

November 2020

■ Personal data of 21.000 British Motorist exposed on-line - Personal information, including driving licence numbers and phone numbers, of 21,000 British motorists have reportedly been stolen by cyber criminals and put up for sale on dark web marketplaces.The breached data includes full names, addresses, phone numbers, dates of birth, email addresses and driving licences of **motorists living across the UK.**

■ Capcom ransomware attack leaves 350.000 people at risk - In a press release, the developer of such hit games as “Resident Evil” and “Street Fighter” confirms that it not only fell victim to a ransomware attack but that the **malicious hackers** accessed sensitive personal data of up to 350,000 people.

■ Hosting Provider Exposed 63M records - Security Expert Jeremiah Fowler exposed a data leak of more than 60 million records by Cloud Clusters Inc., an IaaS cloud provider. The security researcher discovered an unprotected database containing data backups, monitoring and security logs across the 4 data center locations used by **Cloud Clusters**.

December 2020

■ T-Mobile Data Breach exposes 2M records - According to T-Mobile, its security team (...) discovered "malicious, unauthorized access" to their systems. After bringing in a cybersecurity firm to perform an investigation, T-Mobile found that threat actors gained access to the telecommunications information generated by customers, known as CPNI. The information exposed in this breach includes phone numbers, call records, and the number of lines on **an account**.

■ Brazilian aero-space industry giant, Embraer, targeted by hackers - In a statement published in December, Embraer officials cited malicious activity from hackers which gained access to company data in the form of a single archive. This breach had a temporary effect on the **company’s operations**.

■ Transform Hospital Group victim of ransomware attack - REvil group posted in one of their leak sites that they gained access to some 600GB of PII, including photographs of patients. Officials of Transform Group later confirmed the attack stating that payment details of its customers have not been divulged although “some (...) personal data” had been **accessed**.

January 2021

■ Database Leak in Brazil exposes personal data - The information contained in the compromised database includes the name, date of birth and CPF of almost all Brazilians, including authorities. The leaked data contains detailed information on 104 million vehicles and about 40 million companies, potentially vulnerable to the entire population of Brazil.

■ British Mensa Website Hacked - British Mensa, the society for people with high IQs, failed to properly secure the passwords on its website, prompting a hack on its website that has resulted in the theft of members' personal data.

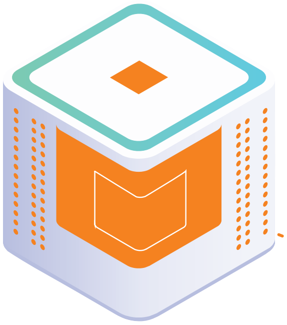
■ SonicWall allegedly hacked by zero-day in its own products - The Network Devices Maker announced on their website that zero-day vulnerabilities in certain products have been exploited in a "highly coordinated attack". The company listed some of their Secure Remote Access solutions as impacted.

February 2021

■ Biochemical Systems Labs at Oxford hacked - Oxford confirmed to Forbes that back in February 2021, malicious activity had been detected in systems used by their Division of Structural Biology who were studying, among other things, the complexities of COVID-19 disease.

■ Brazilian Telcos hacked, 100+ million customers' data leaked - Malicious actors operating outside of Brazil claimed they have personal data of some 102 million people, after a leak from two of the largest telcos in Brazil - Vivo and Claro. A formal investigation has been started by the National Data protection agencies.

■ Romania's largest Real-Estates portal breached - Up to 200.000 records containing personal information have been leaked from an AWS Bucket used by imobiliare.ro, our country's largest real-estate web-portal. Leaked contains full names, phone numbers, addresses, emails and CNPs of users.

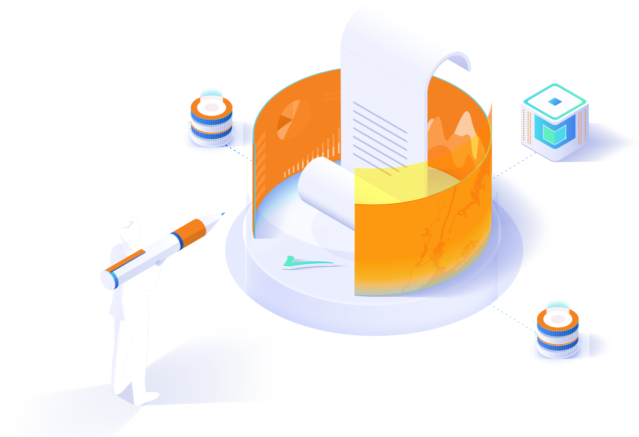


March 2021

- Malaysia Airlines hacked, frequent flyer info compromised - Frequent Flyers of Malaysia Airlines have been informed that their data may have been leaked in an 9-years ongoing attack, from 2010 up to 2019. The Airline urged its customers to secure their accounts by **changing their passwords**.

- E-Ticketing business “Ticketcounter'' targeted by complex attack - the e-ticketing operator confirmed a breach leading to exfiltration of nearly 1.9 milion e-mail addresses. The vector was an unsecured staging server. The attackers later advertised the database for sell, on a **darkweb forum**.

- COVID-19 test results leaked online - TheHealth and Welfare Department of West Bengal, India confirmed a potential data **leak of more than 8 million COVID-19** test results from samples collected from all the province’s residents. The mishap, in the form of an unsanitized URL has been fixed.



April 2021

- Yet another Facebook leak - Phone numbers of nearly 0.5 Billion users of the Social Network were leaked online to a publicly accessible forum. The data dump contained phone numbers of users who chose to hide this information from their public profile. Facebook announced that it was, in fact, ”old data” previously leaked in the 2019 data dump **incident.**

- University of Portsmouth hit with ransomware - The University of Portsmouth had to close their campus in early-April, due to t**echnical conditions** to their IT infrastructure, likely believed to be caused by a ransomware attack. Students and Faculty were advised to work from home as the IT Systems were restored.

- Reverb, a marketplace for musical instruments leaked 5.6M records of musician’s data - Security researcher Bob Diachenko, investigated a possible **data leak** from an unsecure Elastic instance of Reverb, containing personal information of its users. Reverb, in turn, sent notifications to its users urging them to change their passwords, without giving details on how the breach occurred.

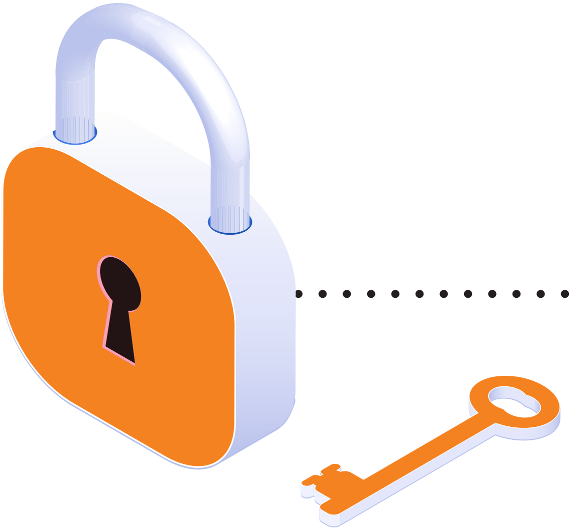
May 2021

- Cluj City Council Website hit with Ransomware - The Website of the Cluj City Council was defaced with an announcement stating that the attackers had dumped remote databases and encrypted the websites files, asking for 100 USD worth of BTC, in return for the decryptors and the **encryption keys**.

- NHS Website misconfiguration leaks COVID-19 vaccination data - The website used by UK residents to book COVID-19 jab appointments, run by NHS Digital, allows anybody in possession of other people's basic personal information to see whether they are vaccinated or not. Although this does not expose sensitive medical records, the failure to secure the functionality of NHS's platform **might have enabled** anyone with basic info on any person to check whether they got the shot or not.

June 2021

- Colonial Pipeline halts operations due to ransomware - The large infrastructure operator had to shut down its operations including fuel transport capacity to the East-Coast of the U.S., in order to contain a ransomware attack from spreading through their ICS & OT Infrastructures. In a further notice sent to the public, the Company confirmed they paid up to 4.5 Million USD in ransomware in order to restore operational capacity. This has been one of the most important cyber attacks in recent history, the first of its kind by ability to **affect a large population** in a developed country.



- Electronic Arts hit with breach, loses IP - Hackers have breached EAs systems and exfiltrated up to 700 GBytes of data, including source code to some of the publisher's most popular titles, such as "Frostbite", the engine that powers FIFA, Madden or Battlefield video games. Spokespersons for the company claim **no personal data has been accessed**.

- McDonalds hit with data breach, customers personal data exposed - Customer's data in South Korea and Taiwan has been exposed in an incident, after some malicious activity has been detected in McDonalds systems. The Company stated they managed to secure access and **contain the breach**.

- Fujifilm hit with ransomware, refuses to pay demand - Japanese multinational conglomerate Fujifilm said it has refused to pay a ransom demand to the cyber gang that attacked its network in Japan, in June 2021, and is instead relying on backups to **restore operations**.

July 2021

- Iberic Telco MasMovil hit with ransomware - REvil Ransomware group claims it had exfiltrated databases of Spain's 4th largest Telco, MasMovil, including customer data. Proof of the breach has been published on a dark web forum powered by REvil and the telecommunications operator confirmed the attack although stating they were yet to **receive a ransom demand**.

- PDS of Tamil Nadu Region in Bangalore breach - Records of more than 4.5 million residents of the Tamil Nadu Region **have been exposed** from the Public Distribution Systems of the State, including names, social security numbers and phone numbers. A sample of the dataset has been published to data sharing platforms.

- Municipality of Oradea, Romania, hit by ransomware - The operations of the Municipality of Oradea have been suspended due to the spread of **ransomware malware** in their systems. The City's representatives noted, however, that a complete restoration from backups was ongoing and that the service disruption was to be contained shortly.

August 2021

- T-Mobile Data Breach of more than 50M customers - an ongoing investigation into a data breach revealed that hackers accessed personal information of more than 53 million customers of the third largest US wireless carrier. T-Mobile said that personal data of more than 40 million former and prospective customers **was stolen** along with data from 7.8 million existing T-Mobile wireless customers.

- Taiwanese computer hardware vendor Gigabyte, hit with ransomware - A spokesperson for the company stated that a no production systems have been hit, but only a small number of servers in one its headquarters, although posts on the darkweb states that up to 112GB **of company data** is up for grabs.

- L.A. man steals 600k photos of iCloud Users through phishing - A Los Angeles County man broke into thousands of Apple iCloud accounts and collected more than 620,000 private photos and videos in a plot to steal and share images of nude young women, federal authorities say. The man admitted that he impersonated Apple customer support staff in emails that tricked unsuspecting victims into providing him with their Apple IDs and passwords, according to **court records**.

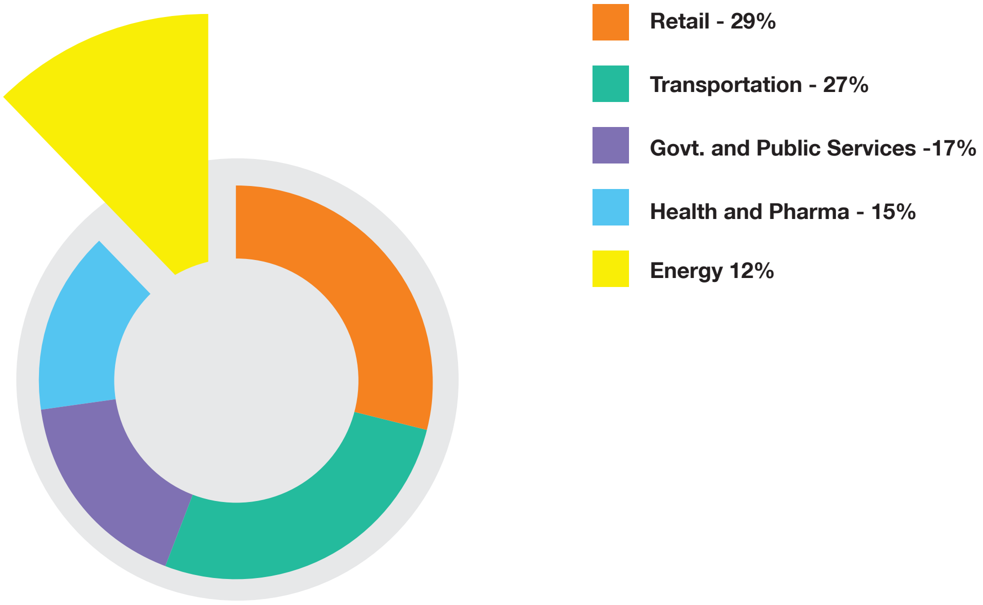
Business Internet Security

Insights and Findings

Business Internet Solution (BIS) offered by Orange Business Services, available for medium and large companies, analyzes more than 8 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, in order 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 2020 up to Q3 2021.

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 our previous reporting period, there have been noticeable changes in the overall volumes of the threats detected and the most exposed verticals. For 2020, Transportation was the worst hit industry in Romania, mostly through phishing attacks and crypto malware. For 2021, the Retail industry was the most exposed to such attacks:



The **Retail industry** was worst-hit by cyber threats in the past 12 months with malicious actors closely monitoring the widespread and rapid transition to on-line, due to the COVID-19 Pandemic. More companies are opening up e-shops and online PoPs, while fast-tracking through the development, testing and validation phases. For some of these customers, ready-made one-click deployable solutions are, in some cases, sufficient to accommodate their business models but others are relying on DIY-solutions such as open-source content publishing platforms with e-shop plugins to go, all hosted on third party services. This, in turn, opens the door to multiple vulnerabilities and misconfigurations doubled by the lack of proper cyber security processes for development, integration, deployment and security monitoring.

2021 was prolific for actors searching for low-hanging fruits such as out-of-date e-commerce platforms, misconfigured hosting services or unsecured admin areas. This, in turn, led to malware being spread through compromised websites, data leaks of customer databases, large scale email phishing campaigns or full-on DDoS attacks.

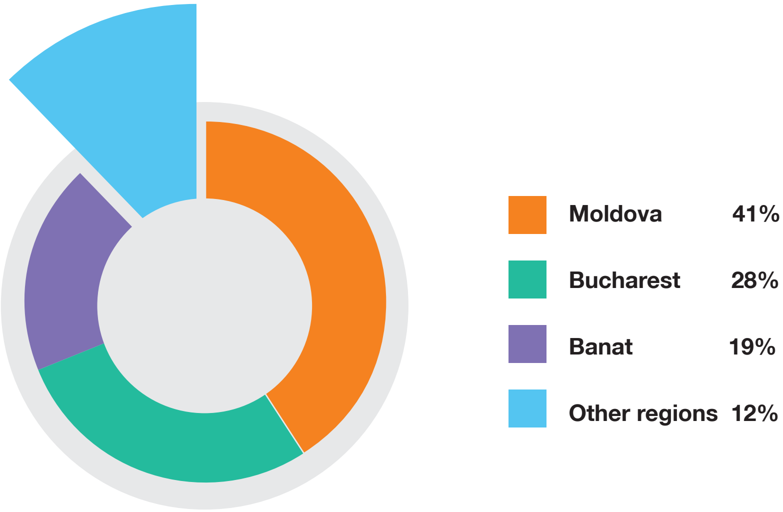
2021 saw the emergence of phishing campaigns targeting retail stores customers, with several such examples being monitored and exposed by national authorities.

In the past 12 months we have blocked, through BIS, several types of attacks targeting Retail customers, from DDoS attempts to intrusion attempts, e-mail phishing attacks and website cloning.

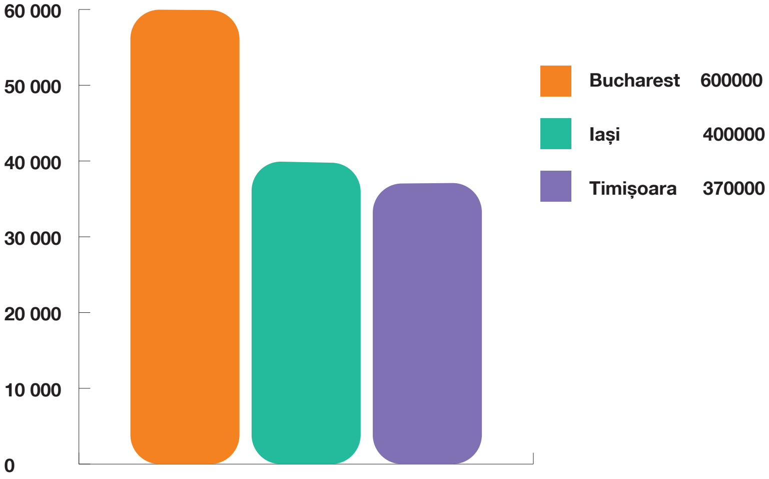
Distribution of threats by region

Within a nation-wide customer base, we gathered information related to attacks across-industries and the Moldova region seems most targeted, with 41% of all detected threats.

Coming in second is Bucharest region with 28% of all threats distributed across-industries and in third is Banat with 19% of all threats.



As for the most affected cities in the past 12 months, Bucharest is in first place with an average of 600.000 attacks prevented each month, across all our customer base located there, with Iasi coming in second with on average 400.000 attacks blocked each month and Timisoara counting for third place with almost 370.000 threats detected and blocked, each month.



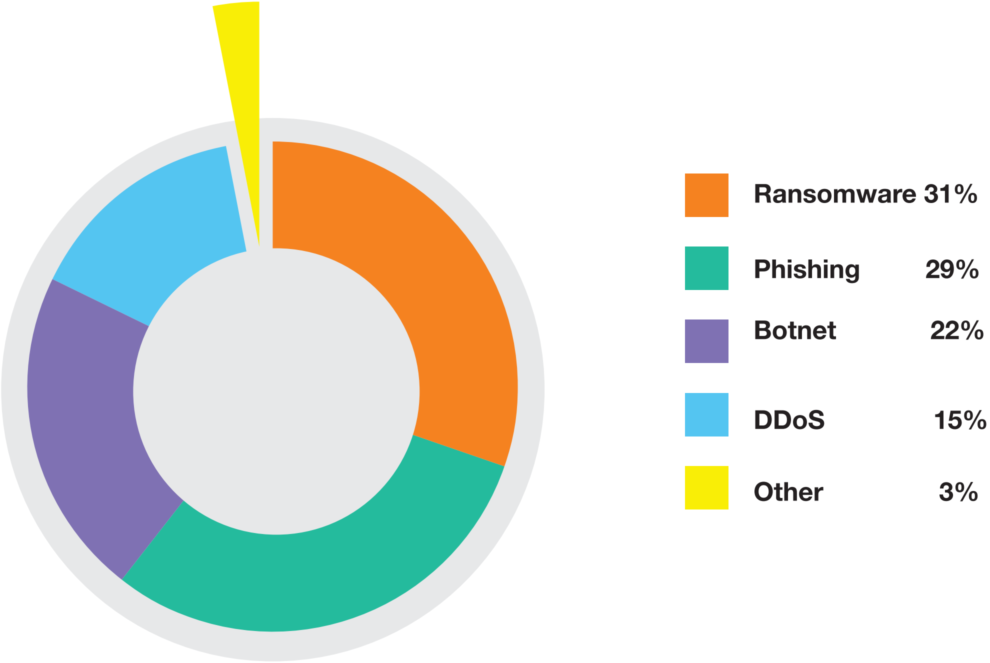
Distribution of threats by type

The TL;DR of 2021 when it comes to prevalent threats is - Ransomware is still king of the hill.

2020 was a prolific year for Ransomware with multiple global campaigns affecting tens of millions. This trend will continue in 2021 and our findings from BIS are consistent with the reports of global organizations and cyber security outlets. There was not one single month of the past 12, without at least one ransomware attack making headlines and the principal targets were, again, large companies across industries and public sector organizations such as municipalities, hospitals and schools. Romania was by no means kept safe from these developments with numerous incidents reported in 2021. Hospitals and public institutions were chief among the victims but as these organizations rely heavily on paper-backups and alternative workflows and to a lesser extent on end-to-end digital infrastructures, the impact was not substantial. Nevertheless, the volume of blocked attacks in our BIS service was impressive.

In second place, phishing attacks continue to disrupt businesses and people, with multiple incidents reported at large scale, through Romania, ranging from email campaigns to SMS and Whatsapp campaigns. Prime targets for these attacks are customers and/or users of services provided by banking institutions or retailers and the attackers tend to be focused on information gathering rather than malware deployment.

Botnets are in third, with most of the zombies continuing to beacon to C2C servers without being detected by the victims. We have blocked communications between run-of-the-mill Windows PCs and C2C servers and those between Gateway-class devices and malicious command/control centers. Connected video cameras and Smart Home Gateways are beaconing as more than 5% of all Botnet communications detected and blocked through BIS.

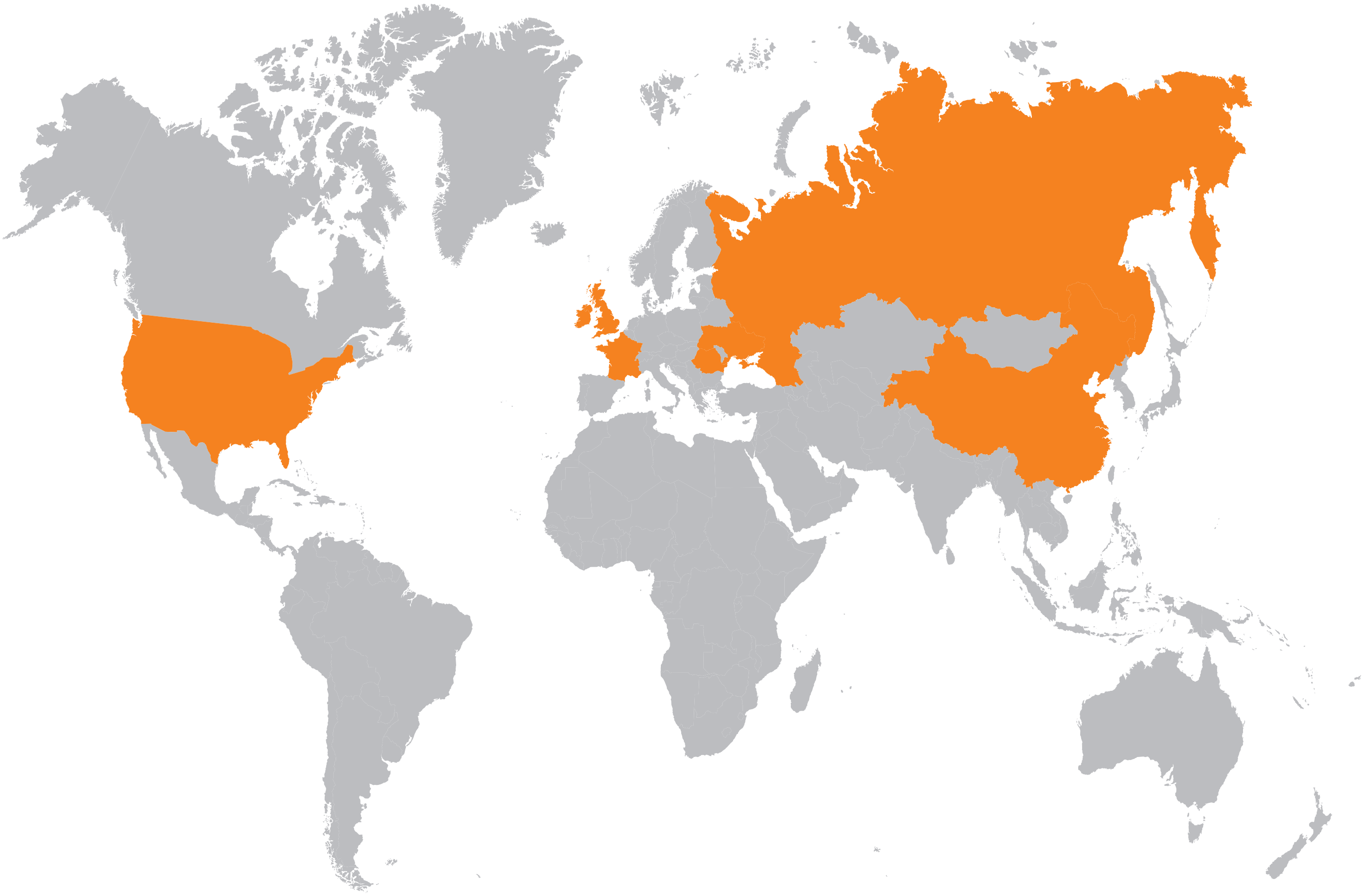


Distribution of threats by country of origin

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 pin-point these IoCs to specific geographies.

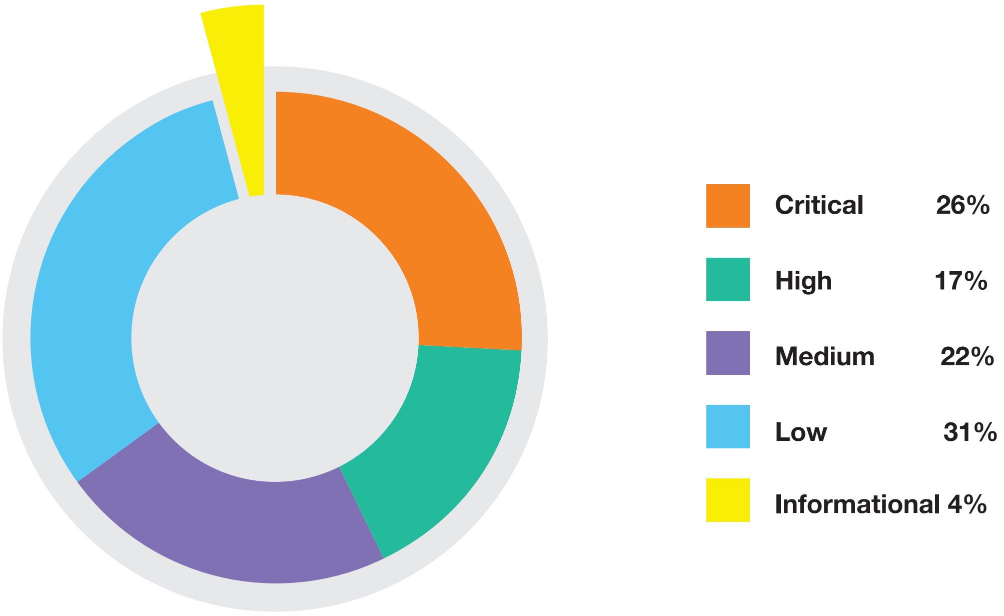
Source of attack by country and unique offenders



550.000	320.000	190.000	180.000	120.000	80.000	25.000
United States	Romania	United Kingdom	China	Ukraine	Russia	France

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.



Disaster Recovery Features for Ransomware Resilience

Ransomware continues to cause headaches, sleepless nights, disruptions, and heavy financial losses to organizations around the world. What makes ransomware so different and more challenging than other types of malware is its ability to severely disrupt the operations of the organizations it hits. By removing access to data, ransomware is halting IT operations and all the systems that rely on them. The only effective response is a disaster recovery solution that can bring the data and the operations it enables back online as quickly as possible and with the least amount of data loss.

Key Disaster Recovery Features You'll Need to Beat Ransomware

These seven key features of Disaster Recovery for ransomware resilience can help you prevent, prepare, and recover. Because ransomware is a disaster scenario, our solution provides data protection that is perfectly suited for minimizing the disruption caused by any ransomware attack and delivering the very best recovery time objective (RTO) and recovery point objective (RPO) possible. These seven features assist not just in recovering from a ransomware attack, but also in hardening systems and backups to prepare for and prevent ransomware attacks.

RPO – Recover data with only seconds of loss – Disaster Recovery's continuous data protection (CDP) uses journaling technology to allow you to rewind the state of your workloads to seconds before an attack took place, minimizing data loss and reducing the impact of the attack. Not only can Disaster Recovery maintain the journal locally for instant restores, but the same workloads can simultaneously be replicated to a warm recovery site (or to the cloud) using our unique one-to-many capability to provide additional options for recovery.

RTO – Resume operations within minutes of an attack – When ransomware hits, time is of the essence, and response time matters not only to stop the spread of encryption across the network, but also to minimize the disruption to your business. Local systems and backups can be compromised, making remote recovery the only option left. With Disaster Recovery, failover of an entire site can be performed within minutes to a remote site, where data can be recovered quickly from a point in time of your choice.

Recovery in an isolated network – When data hit by ransomware is recovered, it may still contain malware, so you don't want to recover the malware directly back into the production environment. Disaster Recovery enables a test recovery into an isolated network allowing the opportunity to validate the recovered data and check for malware before recovering the data back to the production network environment.

Multiple copies of data for recovery – Ransomware relies on recovery being more costly than paying the ransom, and ransomware can attack local backup copies and snapshots to prevent recovery. With Disaster Recovery, you can create multiple copies locally or remotely to ensure there is a clean copy to recover from quickly and with minimal data loss. More copies across recovery sites mean more recovery options when needed.

Immutable data copies – As ransomware may target backup or replica copies, it is possible that even remote recovery data could be targeted by ransomware. Disaster Recovery provides the option for immutable replicas that cannot be encrypted or corrupted by ransomware and are always available for recovery. When all hope seems lost, immutable recovery data can always save the day.

Non-disruptive DR testing – You've implemented a solution, hardened it, made a plan for recovery, but how can you be sure it will work? Testing is vital to any recovery plan and with Disaster Recovery, testing can be done quickly and without disrupting production environments. By doing a failover and recovery test into an isolated network in a sandbox environment, the recovery plan can be tested as often as needed to give you the confidence that it will work when it is needed.

On-demand sandboxes for system hardening and malware scanning – With Disaster Recovery, you can create an on-demand sandbox replica of your production environment quickly and non-disruptively. Hardening systems by keeping them up to date with the latest patches and detecting malware before an attack happens are both important in preventing ransomware attacks. Ransomware attacks can lie dormant on systems for days, weeks, or months before attackers decide to activate the malware and they often target known vulnerabilities. Being able to quickly and non-disruptively test security patches and scan for malware in on-demand sandboxes helps you accelerate your preventative measures to keep your systems free of ransomware.

Is Your Organization Ransomware Resilient?

The threat of ransomware is looming over every organization today. Don't let your organization fall victim because you failed to deploy the right solution to eliminate that threat when it attacks. With these seven powerful features from Disaster Recovery, you can defeat any number of ransomware attacks quickly and with minimal cost.

Cristian Turcin, Cloud Services Product Manager
at Orange Business Services

Education, Innovation and Research

Education through Gamification Unbreakable Romania

2021 marks the first year of Unbreakable Romania, a first-of-its-kind initiative from Bit-Sentinel Security and Orange Romania.
UNbreakable Romania is the end-to-end cybersecurity educational program for high schools and university students from Romania. It offers an x-ray and visualisation of cybersecurity skills nationally with the sole purpose to identify and encourage talents in order to decrease the impact of the cyber security skills shortage and supporting organisations and institutions to build strong defenses.

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.

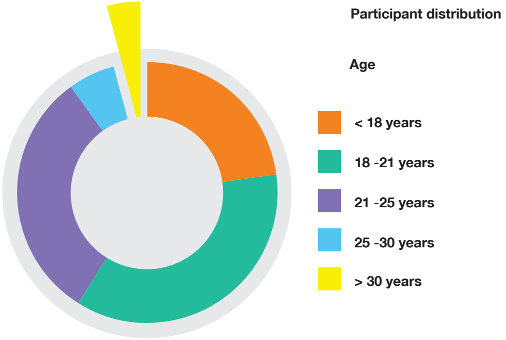
The vision behind UNbreakable is to have ongoing competitions, split between two seasons, starting in early-spring and hosting the second season in late-autumn. The participants go through an informative journey of boot-camp themed training sessions on multiple topics then move on to participate in Capture-The-Flag competitions, in both individual and team settings.

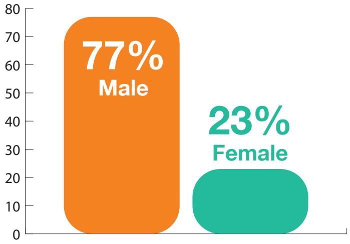
The participants gain access to trainings and webinars on Network Tools, Cryptography, Web Applications Security, 5G and Wireless Security, Cloud Security, Forensics and Computer Investigations, Reverse Engineering, throught and extensive 25+ hours of online tutoring conducted by leading industry experts.

The first season of Unbreakable Romania started with two pilot editions in late 2020, with competitions centered around the incentive of introducing CTF-Style Challenges to the participants. These two pilots netted more than 400 participants from Romania, challenging over 30 exercises from a diverse topics pool. These two pilots were primed to beta-test CyberEDU, the online learning platform developed by Bit-Sentinel for all-around cybersecurity training, learning and knowledge management.

This year's first Season of UNbreakable Romania debuted in Spring with 877 participants from across Romania. 54% of all participants were students in Romanian Universities while 28% were highschool students. The remaining 18% participated for fun, without scoring in the overall leaderboard.

Leading presence among the participants which scored during the CTF were from the University of Bucharest and POLITEHNICA University of Bucharest, netting around 5000 points each, with "Alexandru Ioan Cuza" University of Iaşi scoring third, with approx. 4500 points.





During the 24hrs timeframe of the CTF, 9.181 flags were sent by the participants and the challenges were solved 438 times.

The "Reverse Engineering" category proved to be the most challenging for the participants with only 7.5% of all solutions.

The second Season of UNbreakable Romania is due to start in Late October 2021, with webinars on a wide range of topics and a 24-hours CTF on December 3rd for individual players while a teaming CTF is to be held on December 10, 2021.

All participants will receive an individual performance report at the end of the competition, no later than December, 15.

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 startups access to:

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

Security Startups from Orange Fab

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

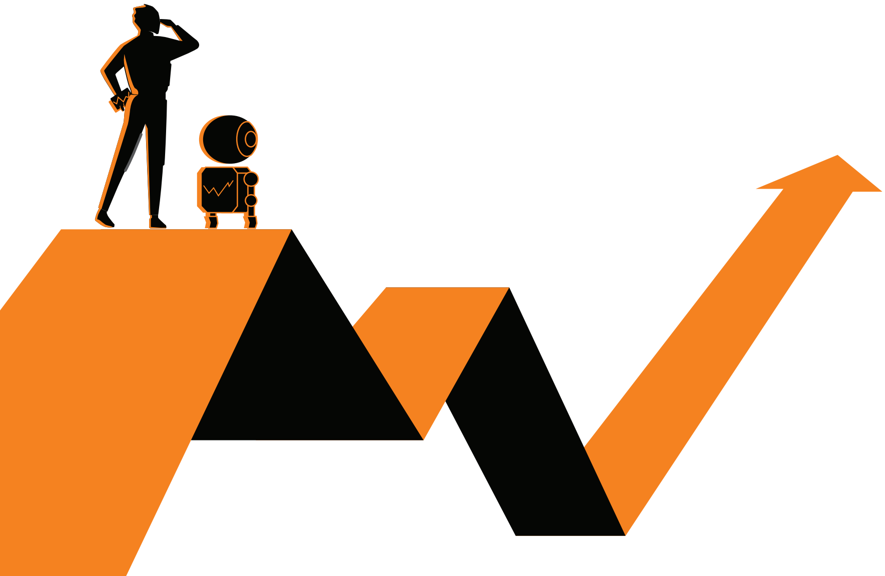
Dekeneas - Web Security solution using artificial intelligence to address some of the most complex and hard to tackle computer attacks: watering holes and crypto jacking.
www.dekeneas.com

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

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

More details on www.orangefab.ro



Research - H2020 Projects

What is Horizon 2020? -Horizon 2020 is the biggest EU Research and Innovation programme ever with nearly €80 billion 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.

RESISTO

RESIlience enhancement and risk control platform
for communication infraSTructure Operators

In November 2021 the RESISTO project reached its final validation stage during a second run of all the macro-scenarios involving all the Telecommunications Operators end-users. These simulations validated the objectives of the RESISTO platform, improving situational awareness for the end-users of the platform and increasing overall resilience of the infrastructures to hybrid cyber-physical attacks.

Our testbed in Bucharest hosted both rounds of validation, in April 2021 and October 2021 with optimal results, in line with the expectation set forth in the Macro-Scenarios. Orange's scenario involves the simulation of large-scale DDoS attacks targeting our customer facing infrastructure, while fibre cuts are affecting availability and integrity of voice and data services.

During the 3 years of research and validation work in RESISTO, the consortium developed new best practices, new methods and new softwares useful for improving the resilience of telecommunication operators in Europe to complex, hybrid attacks. As of November 2021, all public deliverables of the project along with all dissemination and communications materials are available on the www.resistoproject.eu website.

UNICORE

Orange is a member of a consortium of Technology Vendors, Research Institutes and Universities involved in the Horizon 2020 UNICORE Project – A Common Code Base and Toolkit for Deployment of Applications to Secure and Reliable Execution Environments. At this point, the software world appears stuck with inherently insecure and not-so-efficient containers, because virtual machines are deemed too expensive to use in many scenarios.

UNICORE will solve this problem by enabling software developers to easily build and quickly deploy lightweight virtual machines starting from existing applications. UNICORE will develop tools that will enable lightweight VM development to be as easy as compiling an app for an existing OS, enabling EU players to lead the next generation of cloud computing services and technology. Despite their advantages, developing applications with unikernels is a manual process today requiring significant expert resources, which prevents them from being widely used by the software industry. UNICORE will enable standard developers and dev-ops engineers to create, maintain and deploy unikernels with ease. UNICORE will achieve this goal by developing an open-source toolchain that will enable secure and portable unikernel development. Developing unikernel based applications will be reduced to slight changes in the app Makefile, choosing from a menu of available implementations for the required system functionality, and compiling the app.

www.unicore-project.eu

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, in order to foster rapid development and testing of new and innovative NetApps 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 NetApp 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 NetApps, through our Facility in Bucharest and to create a community of developers of 5G-enabled applications.

www.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 (NetApps). 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

Predictions for 2022

Supply chain woes - 2021 was by far a challenger for global supply chains and large-scale logistics. Beginning with the disarray brought forth by the economic and social challenges of the Pandemic, moving forward to disruption in shipping of goods and ending with a global chip shortage, 2021 is a turning point for supply chain security. The cost of manufacturing and moving goods has increased significantly over the past 12 months so did the cost of ensuring proper cyber and physical infrastructure controls against complex threats. 2022 might be at the tipping point of large supply chain disruptions by cyber criminals. Such operations might further affect the resilience of large infrastructures, including health, communications or government.

Data portability and interoperability - 2022 could be the year where data interoperability will become the norm for business and people wanting to access and share their data across multiple platforms or to correlate all their datasets to single apps. Multiple cloud SaaS and IaaS should have the capability to allow easy data portability for its users while they consume all their data across platforms through multiple endpoints and applications. This will, predictably, increase the overall value of given datasets and transform cloud-enabled data, services and apps into prime targets for malicious actors.

Ransomware-as-a-service likely the norm for large-impact attacks - 2021 saw ransomware effectively cut-off a large part of the United States' East Coast from a gas and fuel pipeline. The Colonial Pipeline attack will, for sure, pave the way for cybercriminals groups to leverage Ransomware-as-a-Service ecosystems for their nefarious purposes. 2022's Ransomware attacks will probably impact essential infrastructure and purpose-built ICS Ransomware might become the "gold standard" for threat actors.

Data leaks in the Exobytes - The past few years saw a plethora of incidents where misconfigured or unsecured big-data instances were targeted by cybercriminals. This resulted in spectacular data leaks, with billions of records up for grabs on various forums on both dark and "bright" web. 2022 will continue this trend and we will most likely witness countless incidents of unsecured instances being dumped of content. Furthermore, APIs will be of real interest to hijackers as standardized interfaces through which anything-data-consuming communicates.

5G and IoT Threats - Actors will become increasingly interested in poking around exposed infrastructures and interfaces hosting 5G Applications (NetApps) that facilitate IoT operations. Such applications include eHealth and Tele-Health services, V2X communications, smart-territories deployments and even smart-home services. 5G will become prevalent in 2022 with the market for Applications and Use-Cases opening up to new players and new technologies. This will increase the value-chain for malicious actors.

Glossary of terms

Term	Description
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 is able to 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 cryptovirology 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

Is a number of 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 Center, 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 in an attempt 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 is able to 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. The vast majority of websites use it, and all major web browsers have a dedicated JavaScript engine to execute it.

(Malware)
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

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 behavior to occur on computer software, hardware in order to gain control of a computer system, allow privilege escalation, or execute a denial-of-service (DoS or related DDoS) attack.

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

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

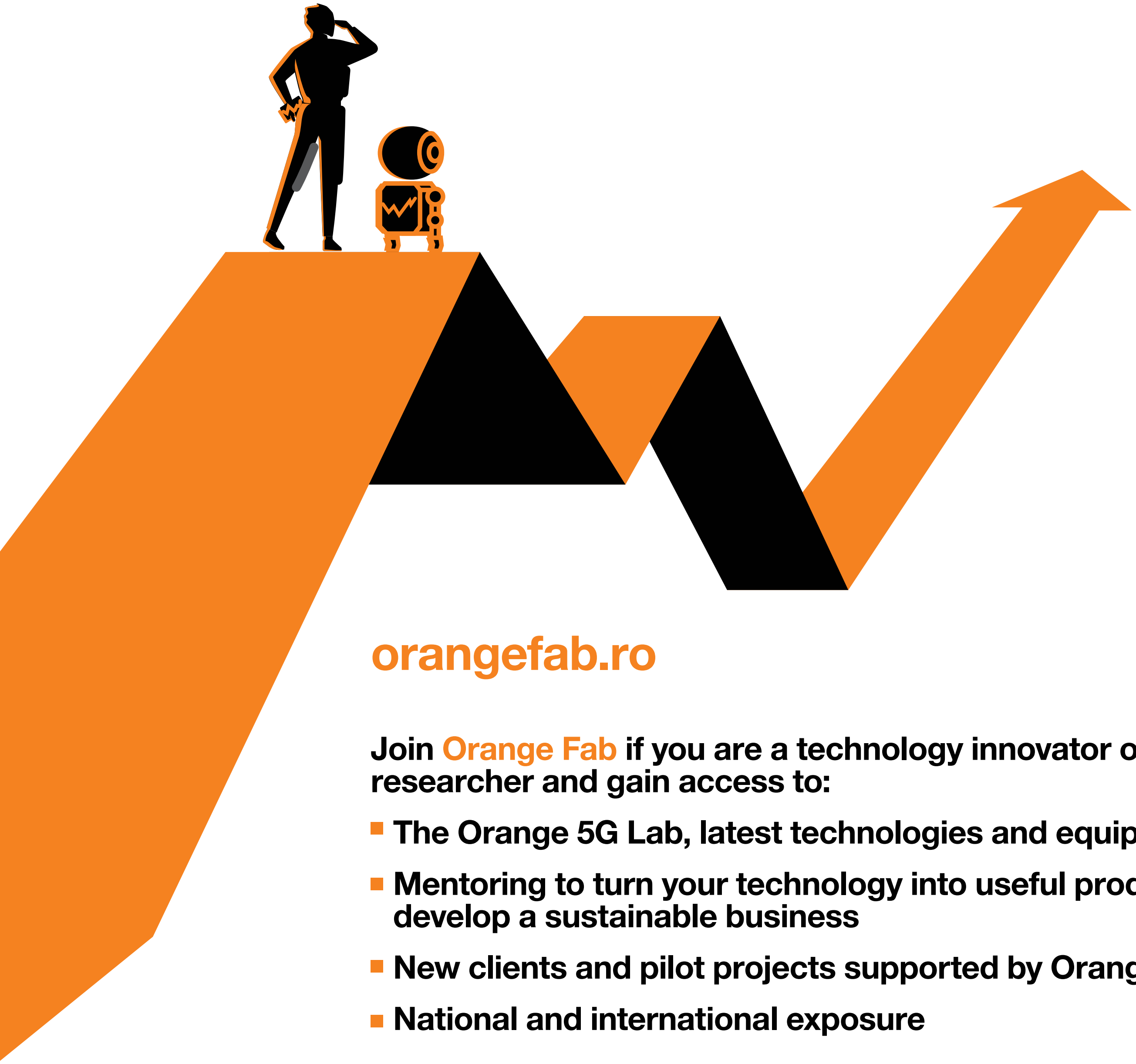
Thank you

The Team

Ioan Constantin, Cyber Security Expert
Laurenţiu Popescu, Security Product Manager
Cristian Turcin, Cloud Services Product Manger
Victoria Cîrstescu, Brand Specialist
Valentin Dinu, Senior PR Specialist
Cristian Paţachia, Development & Innovation Manager
Ştefan Buzea, Graphic Design and DTP

Orange Fab

Startup accelerator program



orangefab.ro

Join Orange Fab if you are a technology innovator or a researcher and gain access to:

- The Orange 5G Lab, latest technologies and equipment
- Mentoring to turn your technology into useful products and develop a sustainable business
- New clients and pilot projects supported by Orange
- National and international exposure