Orange Romania
Business Internet Security Report

3rd edition, 2020

IoT-based attacks

Phishing

Spam

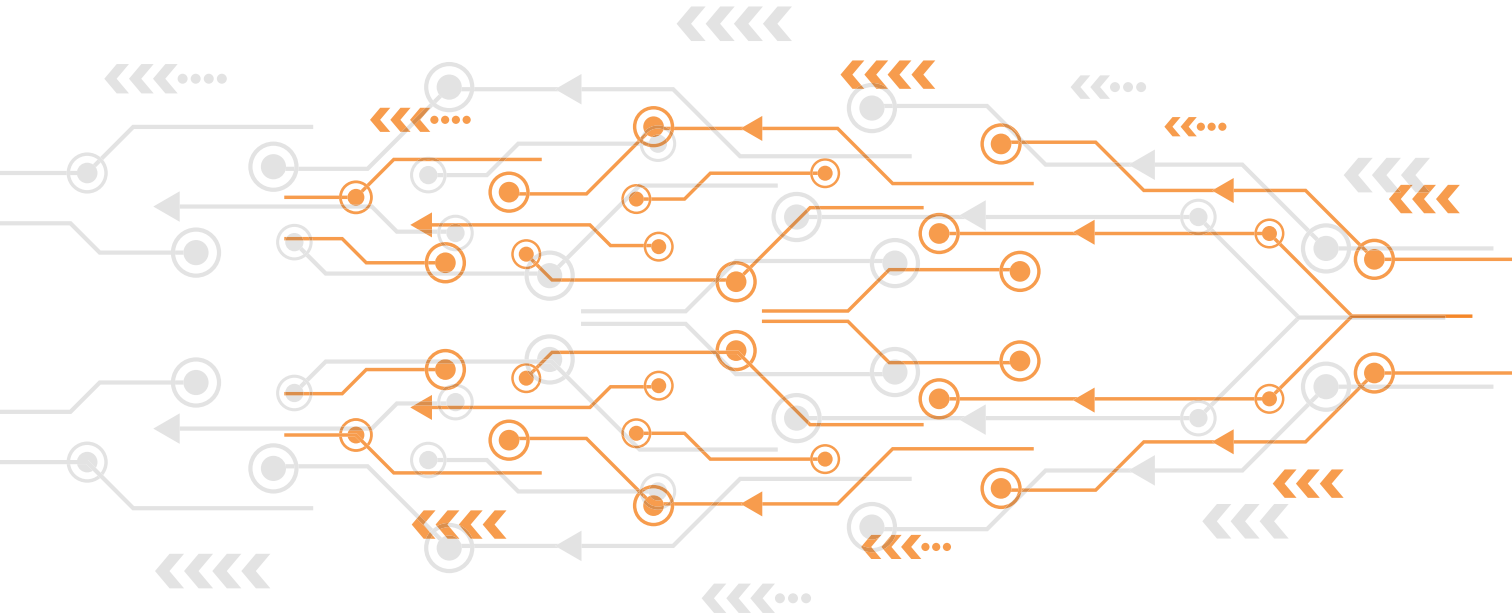
DDOS

Ransomware

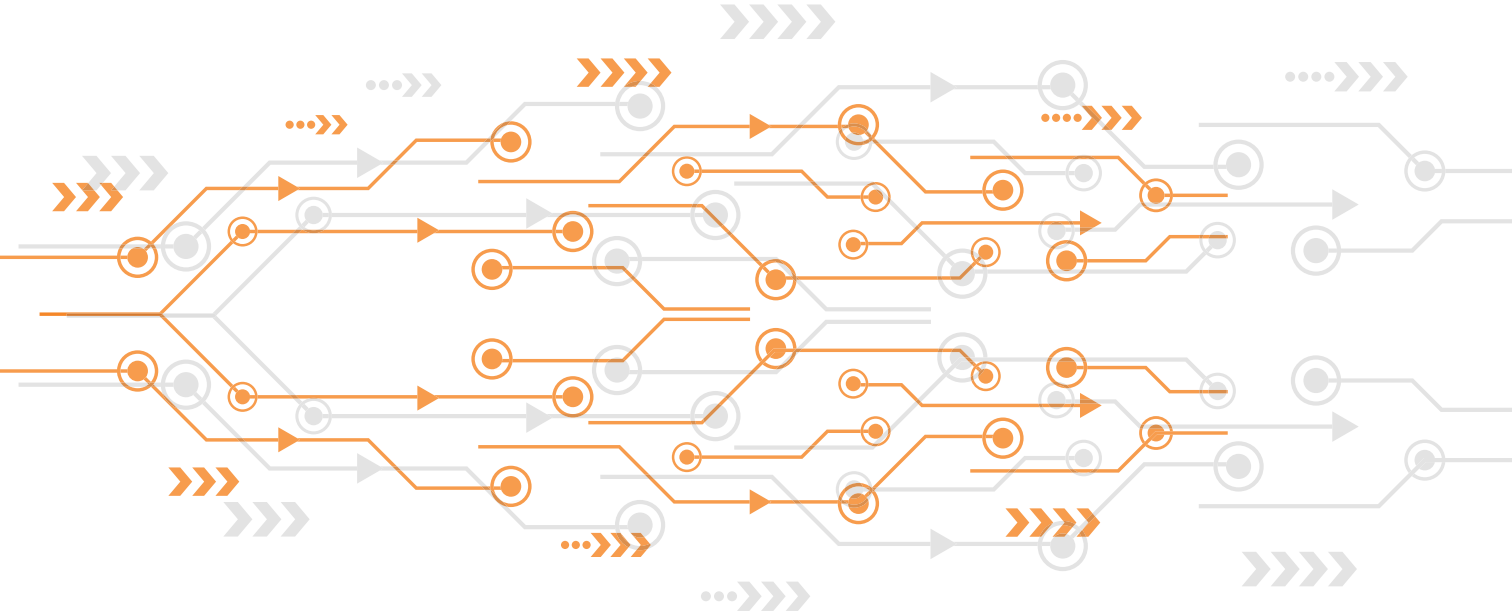
Vulnerabilities

Botnets

Social Engineering



Contents



”

Cyber security became top of mind for every CIO in 2020. Influenced by the pandemic, many companies went through a forced and accelerated digital transformation journey with most of their teams working from home. In a matter of weeks, this new context became the perfect playground for attackers and brought continuous challenges for security experts. At Orange, we focused on developing and delivering cyber security solutions adapted for remote working environments that can protect companies against today's and tomorrow's threats.

Digital is here to stay and the need for security skills can only grow. Therefore, Orange keeps its long term commitment for educational programs which can prepare new experts in this field. We welcome fresh minds from universities or startups to join us in our EU research and innovation programs where we set the ground for new security standards. We also support the growth of cyber security businesses through programs like Orange Fab to accelerate innovation in collaboration with startups.

From investment in education to mature solutions, Orange has created an ecosystem for cyber security built upon years of experience, knowledge and data. Our 2020 Business Internet Security report is providing insights on this ecosystem and I trust that you will find useful intelligence here that can help you grow and secure your business.

Emmanuel Chautard
Chief Technology Officer, Orange Romania

2020 highlights

2020 has been a challenging year so far, to put things lightly. Widespread digitalization by means of accelerated transformation and transition towards remote-friendly and remote-only work while facing the economic and social impact of COVID-19 led to a widened security perimeter, for most businesses. Shifting security policies to quickly enable virtual private network access and secure devices, means security-by-design is no longer a given.

Complementary detection and response methods need to be in place. While businesses and remote workers adapted quickly to the quirks of virtual meetings and conferences, attackers had a prolific year in meddling in technologies that usually exist behind corporate firewalls and security operation centres. Most corporate tech that was usually out-of-scope for any hacker became of interest and easily accessible:

As corporate workers become accustomed to using video-conferencing software, attackers responded quickly by exploiting vulnerabilities and configuration flaws

While most users connected to corporate Intranets using VPN, the attackers put that category of software under microscope and began exploiting the flaws they found

Another highly sought-after area of interest for attackers was phishing, this time with a twist – Pandemic-related news

A cat-and-mouse game quickly became the norm for most cyber security people on either side of the ethical barricades. In late-March 2020, FBI has gone as far as warning the public against using teleconferencing software for business or online classroom because of the increasing number of vulnerabilities found in this category of software. Also, they detected malicious practices involving session hijacking (also known as ”bombing”) where one malicious actor would join an online meeting, without being specifically invited but by simply following a ”join link” – a crafted URL embedding the meeting ID and security key phrase.

Exploiting the massive increase in searchable information on the pandemic, malicious domains containing the ”coronavirus” term and variations were piling up across top level domains. A report by Bit Sentinel observed close to 170.000 new subdomains and around 15.000 subdomains redirects containing keywords such as ”corona” or ”covid”. Most of these websites are still being used to spread malware, spyware and trojans through interactive maps of COVID-19 spread.

Adding further pressure to the overwhelmed hospitals, medical centres and public institutions, ransomware quickly began to show up on the radar with attackers believing that these institutions will not afford to be locked out of their systems and will be more likely to pay the ransom.

The principal vectors for spreading ransomware were e-mails but in some cases the attackers went as far as compromising legitimate websites of hospitals and staging watering hole attacks and drive-by downloads or credential stealers in authentication pages used by the staff to access applications.

”170.000 new subdomains with malicious content around 15.000 pages used to spread malware, spyware and trojans in 2020”

An inquiry into hospitals, medical centres and public institutions exposure

Late April we teamed up with our long-time collaborators, CERT-RO – The National Cyber Security and Incident Response Team, in order to monitor the exposure level of 400-some websites of hospitals, medical centres and public institutions in Romania.

We wanted to look into the current state of exposure for most of the websites and gather information on what can be done to further improve the resilience of these web-based resources that people are accessing in search of reliable information on the ongoing Pandemic.

In order to obtain the data, we used Threatmap – a platform included in our Business Internet Security solution, which gathers anonymous data and presents it in a human-readable format, with insightful graphics and statistics.

Threatmap uses 7 advanced ”engines” to scan for vulnerabilities, misconfigurations, data breaches and leaks, SSL errors and IP reputations and returns a complete, in-depth report on the status of security for each asset. It taps into the web services used to host the web assets (OWASP Top 10), the server-side SSL configuration, the blacklist status of the SMTP email servers used by the assets and the reputation of the IPs used by the hosting service or or ISP. It searches most available IP security feeds for references to any on-line attacks, on-line service abuse, malwares, botnets, command and control servers and other cybercrime activities.

The scanning is completely non-intrusive and will not interfere in any predictable way with the intended functionality of the website.

The scans run in batches of 100 websites, with weekly recurrence, totalling 19 iterations. We then normalize the results in a secure single-pane-of-glass dashboard accessible to CERT-RO. We use CVSS 3.0 for scoring of vulnerabilities.

Threatmap uses

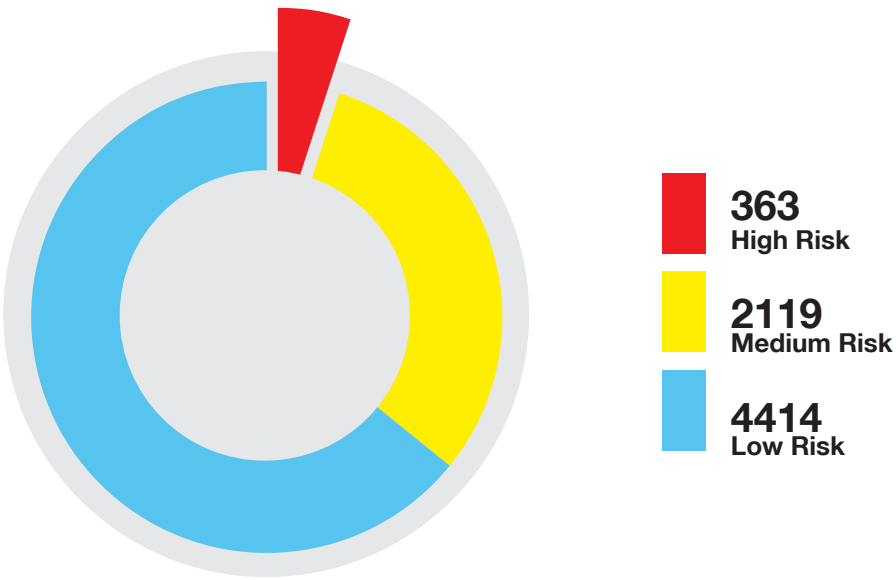
7 advanced ”engines” to scan for: vulnerabilities, misconfigurations, data breaches and leaks, SSL errors and IP reputations

Our findings for the websites we scanned paint a vulnerable picture with **more than 6000 vulnerabilities and misconfigurations for each scan, for all 436 websites**. Out of the the vulnerabilities discovered for the websites, 363 have a CVSS 3.0 score of 7.5 or above (High-Risk), 2119 have a Medium-Risk scoring and 4414 – Low Risk.

Out of the 436 websites we monitored, 311 use an insecure form of authentication and transport (SSL/TLS) with 206 of the 311 websites scanned using none or obsolete implementations of SSL. Furthermore, 36 websites are presenting critical (CVSS 3.0 – Score 10) vulnerabilities in the SSL implementation, making those subjectable to various exploits that could enable various certificate attacks and Man In The Middle Attacks.

Furthermore, 8 out of the 436 websites were previously hacked, as monitored and reported by the included RoHacked Module and 58 out of the 436 websites had data leaks reported in various collections, mostly e-mail users and passwords.

311 scanned websites have SSL/TLS vulnerabilities



Securing remote businesses

As of the beginning of 2020, due to the pandemic, the traditional way we work has changed dramatically. With the workforce moving online, security became top-of-mind for many CIOs, causing a strain for many security teams. As in some cases the entire workforce has started to work remotely, the pressure to protect business data and applications that are accessed outside the corporate offices has increased substantially.

Many CISOs are now forced to secure an increasingly mobile workforce of users, vendors and contractors, often working from personal devices, accessing cloud applications that are not part of the company's network, or otherwise risk creating new surfaces of cybersecurity attacks.

Modern threats try to take advantage of this shift and focus on gaining remote access to users' apps and data — whether it's with stolen passwords or exploited known vulnerabilities targeting users, out-of-date devices, cloud applications and remote access software.

At the same time, the current increase in traffic and connections to the IT environment led to a pre-requisite to secure apps, servers and other workloads that are communicating with each other across cloud infrastructure and data centres.

The main challenge for companies was to protect the data of distant workers. According to a press release published on May 5th by CERT Romania, the number of security attacks targeting this type of connection has increased during the pandemic period. These types of attacks are usually what we call brute-force attacks, during which hackers use multiple passwords in their attempts to break into systems. Once inside the network, they use man-in-the middle techniques to extract data, which is further used for malicious purposes.

One of the main challenges for companies: the use of personal devices for business purposes

The use of personal devices such as smartphones and laptops for business purposes while working remotely is another big challenge for companies in their attempt to protect their business applications running on these devices in the context of BYOD.

Modern threats: out-of-date devices, cloud applications and remote access software

To increase the security of remote connections, organizations must put at the disposal of their employee's additional layers of authentication such as SMS codes, security tokens etc.

When it comes to the use of personal devices, these should be enrolled in Enterprise Mobile Management applications that will allow partition of personal data vs corporate data, the possibility to apply security functions such as the application of white/black listing, content control and URL filtering.

Orange Business Services, Orange Romania's business division, offers a complex suite of Enterprise Mobile Management and security solutions aimed at addressing the increasing needs of enterprises in the context of remote work.

Our network-based security solution, Business Internet Solution (BIS), delivered as service either on-cloud or on premise has a large suite of options designed especially for securing remote connections, such as VPN-RA (VPN Remote Access), WAF (Web Application Firewall) or DDoS features.

Moreover, to strengthen the security posture of our corporate clients, we have added to our security portfolio a comprehensive endpoint protection solution, Bitdefender GravityZone Cloud MSP Security that is delivered remotely via cloud.

On the top of these solutions, we also support our customers in their journey to remote work through:

- Risk assessment to identify key assets and resources so that our customers can prioritize effort smarter and more efficiently
- Network segmentation, allow only required personnel to have access on sensitive areas from your network
- Update of applications, operating systems, and services to the latest version available
- Vulnerability scanning against internal and external environment quarterly
- Penetration testing at any major change of the system or at least once a year
- Intrusion Detection System (IDS) or Intrusion Protection System (IPS) that can help companies identify attacks inside or against their network, with logging capabilities to trace back an incident
- Security awareness trainings, so that the teams become more resilient to ransomware and malware attacks

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

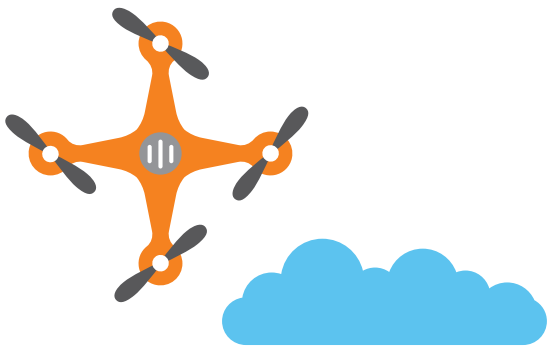
Business Services

orange™

Timeline of events

September 2019

- Malaysia's Malindo Air confirms breach affecting the personal data of nearly 30 million customers. Passenger data was posted in online forums and was initially reported by Kaspersky Lab
- Utah-based Premier Family Medical notifies patients of ransomware attack affecting some 320.000 patients
- A huge database of nearly 420 million records, including phone numbers, is exposed and believe to be linked to Facebook as the records contained a Facebook ID for each phone number listed in the database



October 2019

- Zynga confirms breach and database dump containing records of 218 million users of their successful Words with Friends application
- North-Florida OB-GYN discloses ransomware incident affecting more than half a million patients records
- Two popular cashback services operating in the UK and India leaked more than 2 terabytes worth of personally identifiable information through and unprotected elastic database

November 2019

- T-Mobile's US Customers affected by cyberattack, exposing personally identifiable information of more than 1.1 million customers
- An unsecured elastic server was discovered containing information on an unprecedented 4 billion user accounts spanning more than 4TB of data. This is to the day the largest data leak from a single source in history with a unique user count of 1.2 billion people. The source of the data seems to be two companies offering data enrichment services.

December 2019

- Canadian healthcare provider LifeLabs reported an unauthorized access to its systems affecting information of approximately 15 million customers
- Maastricht University (UM) announced that almost all of its Windows systems have been encrypted by ransomware, following a cyber-attack that took place on December 23rd. It is believed that Clop Ransomware has been used in this attack.
- A critical vulnerability has been found in Citrix Application Delivery Controller (ADC) and Citrix Gateway. If exploited, it could allow unauthenticated attackers to gain remote access to a company's local network and carry out arbitrary code execution. The affected products are used to secure remote access and are installed in at last 80000 companies in 158 countries.

January 2020

- Microsoft confirms massive data breach affecting anonymized data held on its customer support database, affecting up to 250 million people
- Travelex, a major international foreign currency exchange confirms suspension of services due to ransomware attack
- Cable Hunt Modem vulnerability leaves 200 million devices in Europe at risk

February 2020

- A major ransomware cyberattack has hit a gas compression facility, forcing it to shut it down for two days as it struggled to recover, according to an alert from the U.S. government
- NRC Health, one of the largest healthcare companies in the US hit by ransomware attack
- MGM Resorts hacked and personal data of more than 10 million customers leaked in hacking forums.

March 2020

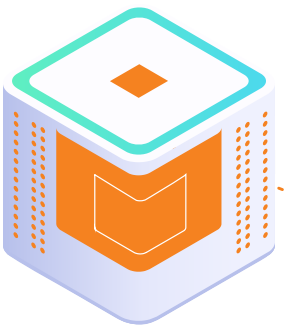
- Czech hospital forced to shut down entire IT network due to an unspecified cyber-attack amidst COVID-19 crisis
- Chinese-based Weibo confirms 538 million user records were leaked and listed for sale on the Dark Web. The records included user IDs, number of Weibo posts, number of followers, gender, and geographic location
- Phishing attack on the World Health Organization (WHO) targeting employees' passwords. Cybersecurity experts believe 'Elite Hackers' group Dark Hotel might be behind this attack

April 2020

- Energy Giant Energias de Portugal (EDP), one of the largest energy suppliers in Europe, was hit by a major ransomware attack that affected 10 terabytes of information, with Ragnar Locker ransomware operators threatening to leak the exfiltrated documents
- COVID-19 research facility 10x Genomics (US) hit by ransomware
- Personal data of 115 Million Pakistani Mobile users go on sale on the dark web

May 2020

- Personal data of 9 million easyJet customers leaked in an highly sophisticated attack. Credit card details of 2208 were also compromised.
- Coronavirus drug maker Gilead Sciences were targeted by Iran-linked hackers through spear-phishing and whaling attempts
- Several healthcare institutions targeted by Maze Ransomware, including Bellevue and Maxwell Aesthetics, two US-based plastic surgery clinics



June 2020

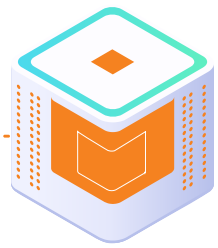
- Australian government attacked by 'state actors, with significant capabilities. The attack is said to have affected a range of political and private-sector organizations.
- Honda, one of the world's leading automobile manufacturers, fell victim to another cyberattack in June 2020 that halted standard operations in multiple plants.
- North Korean state hackers reportedly sent COVID-19-themed phishing e-mails to more than 5 million businesses and individuals in Singapore, Japan, the United States, South Korea, India, and the UK in an attempt to steal personal and financial data

July 2020

- Security officials in the US, UK and Canada announced that hackers were trying to steal COVID-19 vaccine research. The announcement came in the form of a joint statement form the officials.
- Celebrity Twitter accounts hacked in a coordinated spear phishing attack. The attackers sent tweets from the compromised accounts asking for bitcoin donations, promising a doubling of investments.

August 2020

- Seven semiconductor vendors in Taiwan were the victim of a two-year espionage campaign, hackers targeting firms' source code, software development kits, and chip designs
- New Zealand's stock exchange faced several days of disruptions after a severe distributed denial of service attack was launched by unknown actors



Business Internet Security

Insights and Findings

Business Internet Solution (BIS) offered by Orange Business Services, available for medium and large companies, analyzes more than 5 million security threats monthly within our customers' security infrastructures. We gather anonymized relevant data from companies across industries such as public services, retail, transportation and energy.

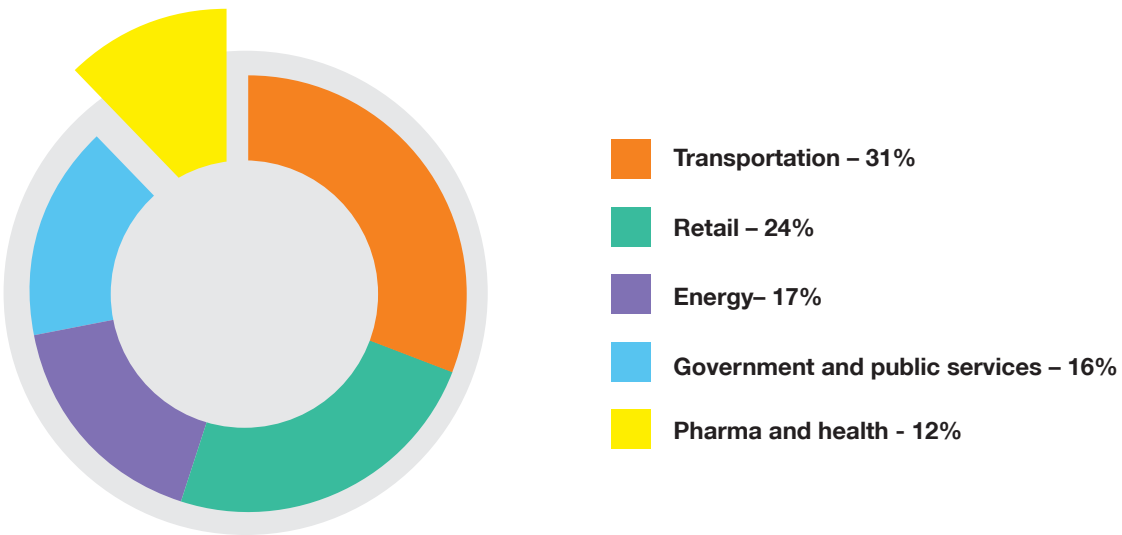
Data obtained was then processed through CyberAI -our new in-house developed platform, in order to correlate and enrich the business intelligence we provide our customers for insights and actionable intel.

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 presented herein represents all findings from Q4 2019 up to Q3 2020.

Distribution of threats by business vertical

The national threat landscape is well aligned with the international trends with endpoints being the principal vector of infection and phishing the most common vector for distribution. This closely mimics the number we have reported in our previous edition.



The transportation industry is quickly becoming prime real-estate for bad actors looking for low-effort high-reward attacks due to the increase in their exposures and attack surfaces.

As more and more companies from this business vertical implements IoT-class sensors and actuators to their vehicles, these headless counterparts of modern-day computers are creating opportunities for attackers looking to exploit firmware bugs and misconfigurations.

IoT-based botnets are common in this realm so is your run-of-the-mill malware installed on outdated, unpatched systems used in Point-Of-Sale scenarios or ticketing and info kiosks machines.

An increased in interest from the attackers was given to the **Retail industry** as more and more customers rely on e-commerce for their daily shopping, given the massive migration to home offices and lock-down measures implemented.

We have detected and blocked large-scale DDoS attacks against some of our Retail customers' websites and web applications and we have blocked numerous reconnaissance scans and intrusion attempts on internet-facing infrastructures.
The boom in interest from hackers for the retail business mostly manifests in the on-line shopping platforms as we are noticing a drop in location attacks such as Wi-Fi MITMs, evil twins, and such.

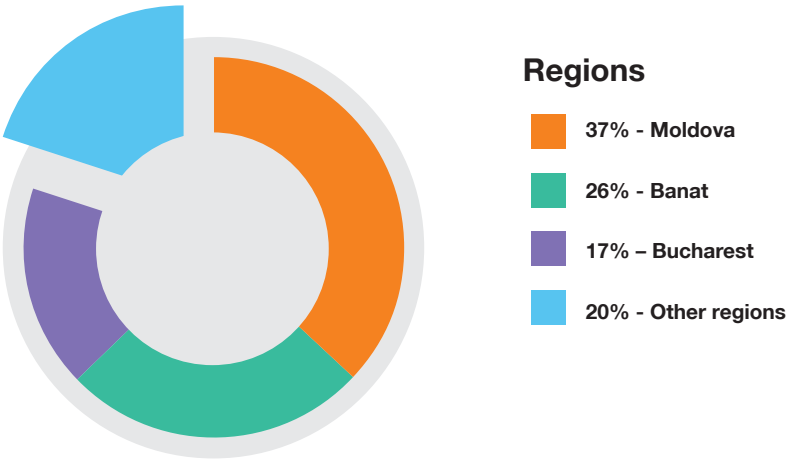
Vulnerabilities: unpatched systems used in point-of-sale scenarios or ticketing and info kiosks machines

Distribution of threats by region

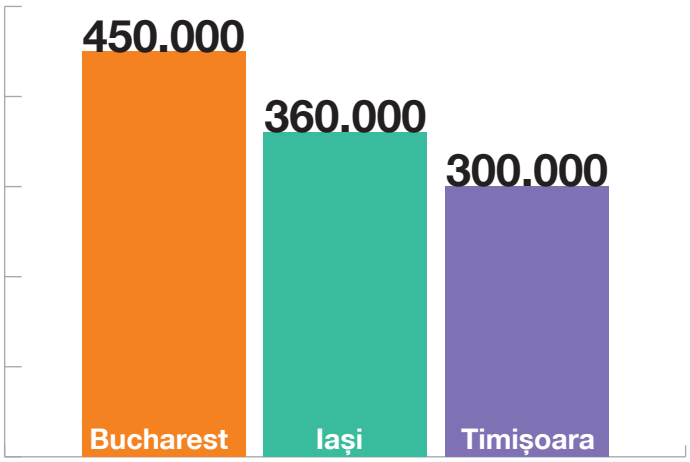
Within a nation-wide customer base, we gathered information related to attacks across-industries and the Moldova region seems most targeted, with 37% of all detected threats.

Coming in second is the Banat region with 26% of all threats distributed across-industries and in third is Bucharest with 17% of all threats.

As for **the most affected** cities in the past 12 months, Bucharest is in first place with an average of 450.000 attacks prevented each month, across all our customer base located there, with Iaşi coming in second with on average 360.000 attacks blocked each month and Timişoara counting for third place with almost 300.000 threats detected and blocked, each month.



Cities by monthly average of blocked attacks



Distribution of threats by type

The global health crisis and the rapid digitalization actions it brought onto most businesses determined a shift in the types of prevalent threats we have detected in the past year in our business customer base. Some of the 'usual suspects' such as DDoSes and botnets lost the spotlight to their mostly-abandoned counterparts from last year – ransomware, phishing.

Phishing attacks were the most detected type of cyber threat in the past 12 months and this validates that e-mail represents, still, the principal vector for infection with attackers preying on the comfort and false sense of security most users get from working from home.

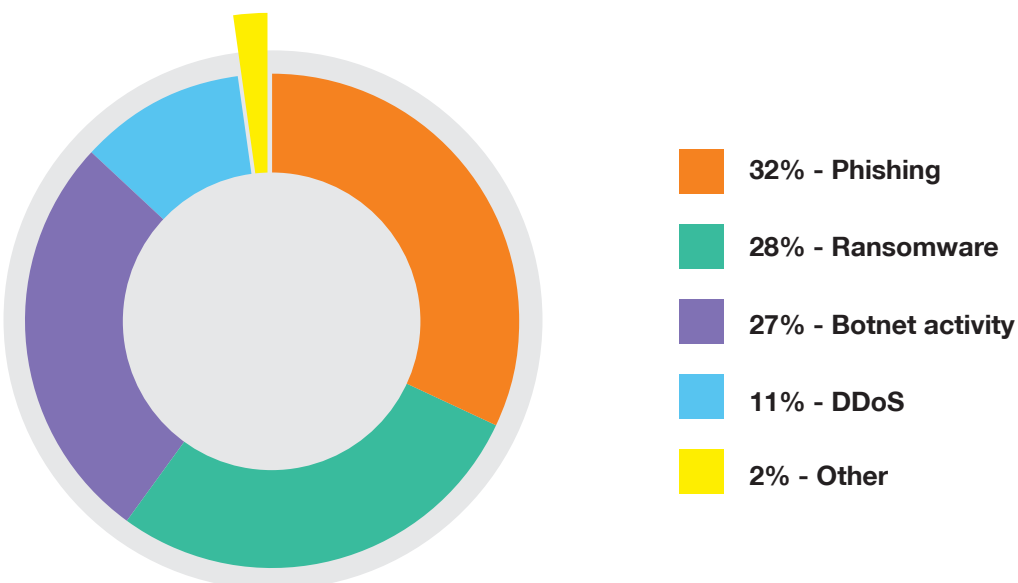
This, coupled to widespread false news campaigns shared through scam-websites with topics of high interest related to the ongoing pandemic, wreaked havoc on a large number of users and companies with the end-goal of the bad actors being, in most cases, information stealing and the installation of malware – be it banking trojans or in some cases ransomware

Ransomware's big comeback to the global threats stage is 2020. This time is targeted against healthcare, hospitals, and public institutions in general. We have noticed an uptick in the detection of some well-known ransomware species to our Pharma and Healthcare customers and blocked those according to the security policies in place.

In the third place we have botnets and we have noticed large-scale activity across business verticals.

This is a mixed-bunch of Windows-based zombies and on-device infections with Wireless Gateways and security cameras prevalent.

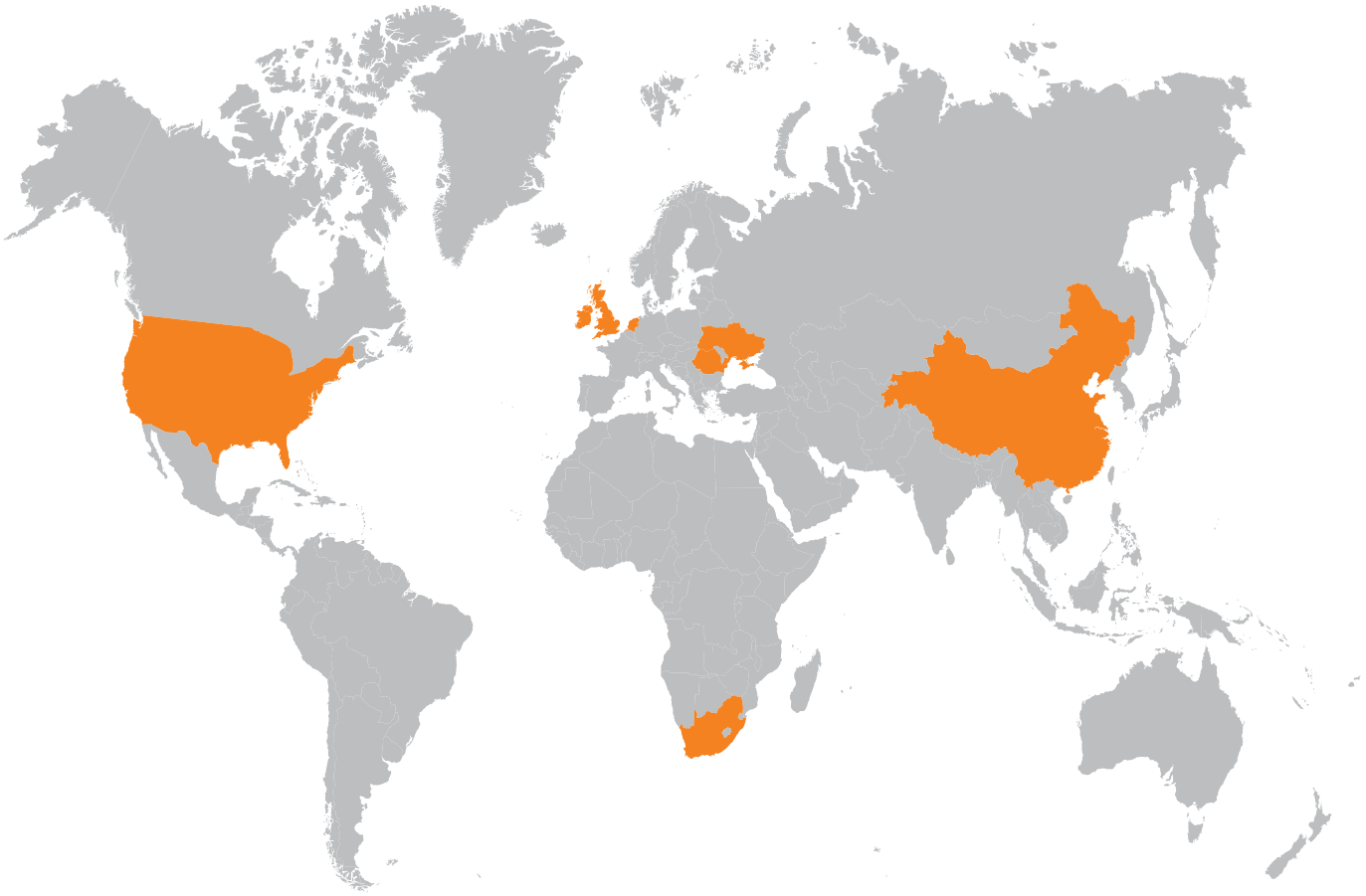
Distribution of threats by type



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.

Source of attack by country and unique offenders

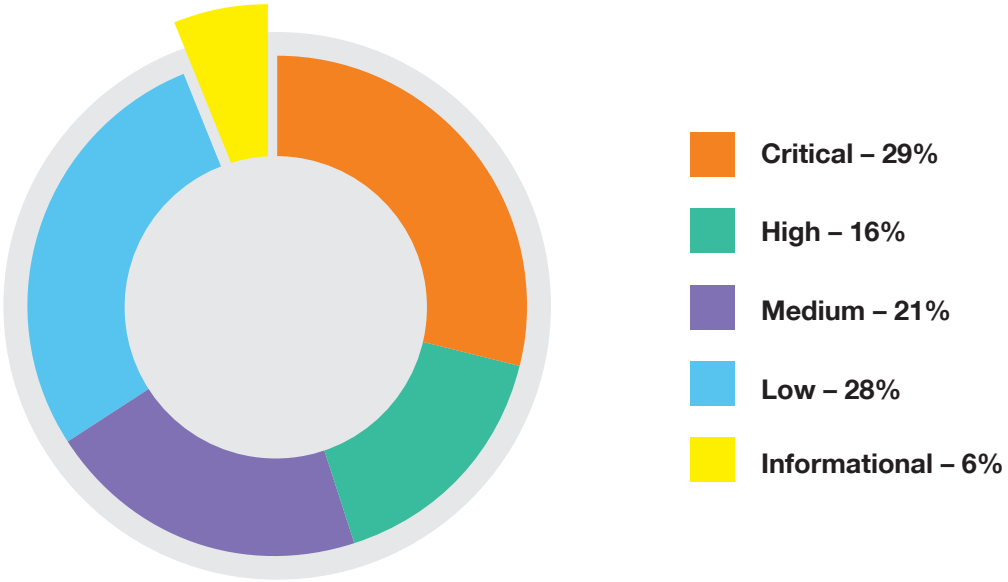


50109	339a08	27090v	13221	11562	9032	7112
USA	Romania	China	Netherlands	Ukraine	United Kingdom	South Africa

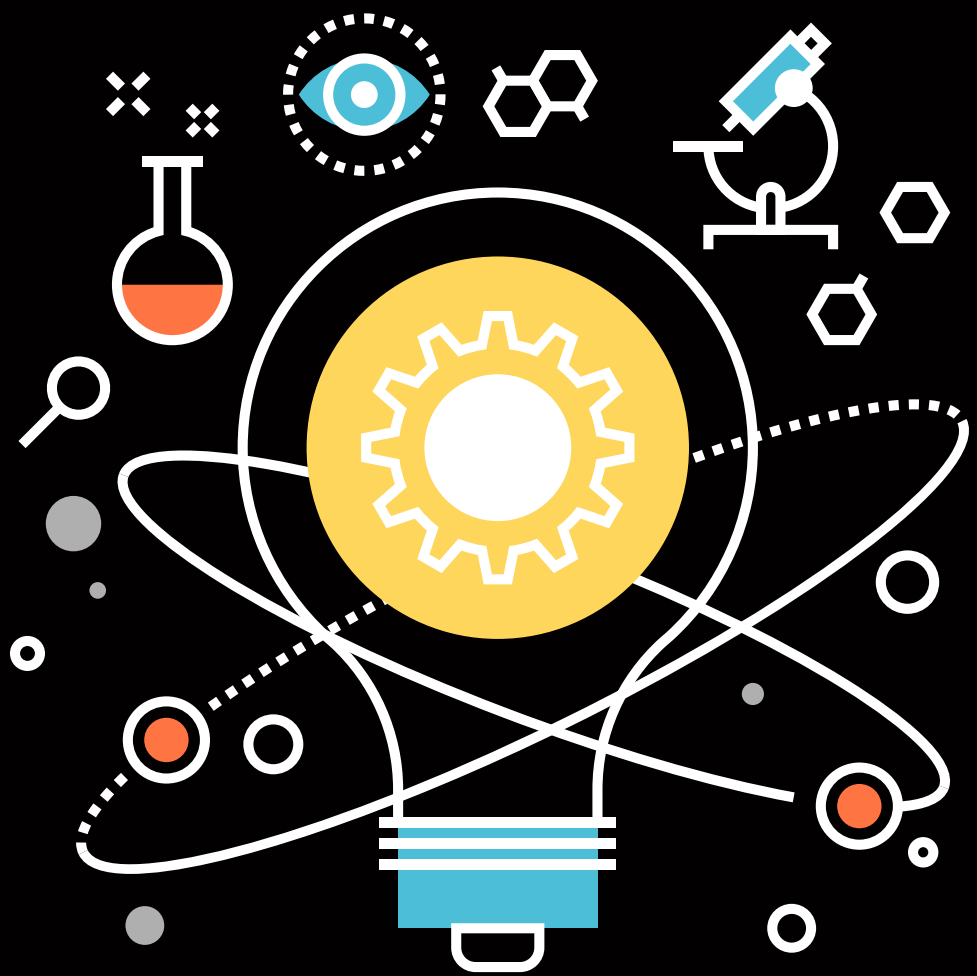
Distribution of threats by criticality

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.

Vulnerability distribution by criticality



Education, Innovation and Research



Orange Educational Program

We believe that investment in education and innovation should be de-facto for all major technology-driven companies and here at Orange we take pride in supporting talented people in mastering their skills and knowledge and driving innovation as a core-business component.

Orange Educational Program (OEP) is an ongoing project, in its sixteenth year, jointly developed with ETTI (The Faculty of Electronics, Telecommunications and Information Technology in Bucharest) aiming to provide advanced classes, internships and scholarships for gifted students. Orange provides technical resources such as laboratories, software, and hardware, offering the students enrolled in OEP the possibility to access and learn about the state-of-the-art technology currently deployed in the Orange network.

Cyber Security has a strong presence in OEP's curriculum with students benefiting from classes and workshops taught by Orange Cyber Security Experts and other key people in the field.

This year we adapted the delivery of classes and workshops to an online-only environment, given the global health crisis and restrictions and we further expanded our presence in other cities, such as Constanta and Iasi. Students learned about the anatomy of a cyberattack or notions about cloud or mobile security.

We aim for a more engaging 2021 as we're preparing to host virtual cyber security laboratories in an online platform jointly developed with our partner Bit Sentinel, through which we can host Capture-The-Flag type competitions and exercises dedicated to students.

www.orange.ro/educational-program

Research at Orange – Horizon 2020 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 2020) – 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 – With the project moving to its final stages of validation of the platform and testing of the macro-scenarios, we are preparing our testbed for the simulated cyber-attacks and physical attacks described in our Use-Case.

This scenario will give us the correct framework for evaluating the response of the RESISTO platform to threats such as massive DDoS attacks against our edge networks combined with physical events like power outages and cable cuts.

Our test bed closely mimics to scale the end to end architecture of our current-gen networks as it is interconnected to other RESISTO members testbeds.
www.resistoproject.eu

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

Projects supported by **the European Commission** Horizon 2020

Orange Romania is involved in all these Horizon 2020 projects along with its parteners from more than 15 European countries.

Orange Fab – accelerator for innovative 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:

- Early access to the newest technologies
- Mentoring and on-demand learning opportunities
- Working space in start-up community hubs
- Access to Orange's distribution network
- Client pilot projects supported by Orange
- International exposure

Security startups from Orange Fab

Pentest Tools

online framework for 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

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

More details on www.orangefab.ro

Predictions for 2021

Rampant phishing campaigns: With more and more people reverting to the internet as a prime source of information about COVID-19, malicious actors will continue to spread malware and info stealers through e-mail campaigns, social media and personal messaging apps targeting specific information on COVID-19 vaccines and cures.

Attacks on VPN: Given the remote-friendly or remote-only nature of tomorrow's work paradigm, more users are relying on secure connectivity to the corporate networks. Attackers will increasingly target VPN clients, VPN gateways and MFA methods used for authentication.

We will witness an increase in SSL certificate replacement and certificate forging techniques used for MITM attacks as some VPNs use SSL.

First large 5G-enabled botnets: with the expanding of 5G infrastructure, performance and availability, coupled to accessible onboarding and a richer device catalogue, vulnerabilities in mobile applications and mobile operating systems components can be used to compromise 5G-enabled devices and enrol those to a botnet which each 'zombie' capable of up to hundred-fold bandwidth saturation compared to previous-gen devices.

Add to this the prevalence of 5G IoT devices and -without proper access control- we could face a first-of-its-kind 5G mobile botnet.

Videoconferencing apps at the forefront of exploitable software: we estimate that the trend set in motion in 2020, of scrutinizing videoconferencing applications and platforms and exploiting any found vulnerabilities will continue in 2021 with malicious actors being more attentive to the monetization potential of these apps.

As for most users, the clients for multiple apps runs in the background, malicious actors could leverage this to inject crypto mining scripts in various components of the software clients.

A.I.-driven swarm-bots: moving from cumbersome C2C servers and avoiding IPs being blacklisted are highly sought after treats for most botnet controllers.

By leveraging technologies such as lambda functions (serverless computing), machine learning and headless devices (IoT-class devices) we could face a first generation of A.I.-commended bots, targeting large-scale DDoS attacks against vulnerable defences.

Glossary of terms

Term	Description
Cyber Security	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	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	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 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 attack (DDoS attack), steal data, send spam, and allows 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	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	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	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 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	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 smart phones) 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
WannaCry (malware)	WannaCry is a ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency
Petya (malware)	Petya is a family of encrypting ransomware that targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.
NotPetya (malware)	NotPetya is a variant of the Petya Malware that propagates trough a specific Windows vulnerability (EternalBlue). In addition, although it purports to be ransomware, this variant was modified so that it is unable to actually revert its own changes.
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 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	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.
BYOD – Bring Your Own Device Policy	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 smart phones) 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

Thank you

The Team

Ioan Constantin, Cyber Security Expert
Laurenţiu Popescu, Security Product Manager
Andreea Grigorescu, Brand Specialist
Mădălina Cojocaru, Senior PR Specialist
Cristian Paţachia, Development & Innovation Manager
Ştefan Buzea, Graphic Design and DTP

orange™

Do you believe in unicorns?
Follow your dream @Orange Fab

www.orangefab.ro

We are offering innovative startups:
Access to new technologies
Access to Orange distribution network
International exposure
Client pilot projects supported by Orange