Orange Romania

Business Internet Security Report

2nd edition, 2019

Contents

”

In a world of seamless connectivity, with the advent of more and more connected devices, data is becoming critical. At Orange, we value and understand the privacy of data throughout all its life cycle, from data collection to its transformation and usage. We also believe that providing secured connectivity and developing cybersecurity solutions for our clients is just the first step in what needs to become a way of thinking. Therefore we apply “security by design” in our infrastructure and product developments.

In this new era of automation, developing skills in cyber security is essential for the protection against the complex threats of the future. That is why we invest in education through partnerships with universities all across the country, we participate in research and development projects, where Orange Romania is part of international consortiums and we support cybersecurity startups with new technologies.

As an infrastructure operator and IT&C service provider, we take very seriously our role in shaping the world into a safer place and we invite you to join us on this journey.

Emmanuel Chautard
Chief Technology Officer, Orange Romania

Cyber risks:
New actors and threats

Shifting motivations

Cyberattacks are the fastest growing criminal activity in both the United States and the European Union as they are increasing in volume, complexity and costs.
One report states that by 2021 cybercrime will have a 6 trillion dollar cost attributed to damages, at a global level. In the past 5 years a great deal of this cost was created by ransomware attacks with a fast-growing cryptomining wave seen in 2017 and 2018. DDoS attacks gain in scale as they rely on the ever-growing size of botnets and they can cause multiple billion dollar worth of damages to companies with large IT and OT infrastructure.

We've seen worrisome increase in politically motivated hacking as tension arises in most part of the North Hemisphere centered around elections in E.U. countries, with large-scale botnets spreading fake news becoming the norm for 2018. This trend poses challenges for social networks and media outlets alike.
Cyber warfare is no longer exclusive to highly industrialized and rich countries. The means and tools used by cyber actors can be efficient at a low cost, with great anonymity. This 'levels' the playing field with countries in Africa, Central and South America and South East Asia coming into focus and gradually entering various stages of cyber warfare.

2018 in a nutshell

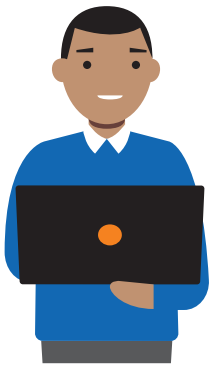
2018 was a very prolific year for cyber criminals and cyber security defenders alike. Evolving technology usually means evolving hackers and this was a confirmed trend for 2018 as well.

The cyber criminals are using e-mails as the principal vector for spreading malware, in opportunistic or targeted campaigns and they rely on Microsoft Office files as a primary method of delivery. One statistic goes as far as to show that one third of all phishing e-mails are actually opened in the U.S..

45%
of all business were a victim of a cyber security breach in 2018.

Ransomware attacks are on a downward trend globally as the attackers are becoming more focused on one industry in particular: healthcare.

2018 was a great year for hackers targeting embedded and IoT devices with a large number of attacks coming from compromised commodity devices such as wireless routers, 'smart-home' devices and alike.



Security awareness:
10 statistics you'll want to read

Browsing data from our Business Internet Security platform, the open web and major publications, we selected 10 interesting statistics that paint the cyber security landscape of 2018.

Small businesses invest less than 500 US Dollars per year in cyber security products and services. While their business makes up for up to 13% of the cyber security market, the individual spending is very little.

SMBs/SMEs fall victims to 43% of all cyberattacks.

76% of all organizations, regardless of size and business vertical, were targets of phishing attacks in 2017. These numbers closely mirror their 2018 counterparts.

The public administration sector is a prime target for attackers and e-mail is the preferred vector as one in 302 targeting public administration users are malicious.

Forget about SSL encryption being good enough to defend against most threats while serving and consuming web content is false. 95% of all HTTPS servers are vulnerable to at least one kind of Man-In-The-Middle (MitM) attack.

You can buy a DDoS attack from the dark web for as low as $30 for nearly 300 gigabits per second.

The average percentage of the IT budged used for cyber security is 2%.

Routers account for 75% of all infected devices in IoT-based attacks. The connected camera categories accounted for 15%.

E-mail is used to spread 92% of all malware, becoming the principal method of delivery for most types of malicious code. This include phishing attacks.

70% of U.S. employees lack a basic understanding of cybersecurity best practices. This number could represent a correct estimate of the lack of awareness on cybersecurity matters at a global level.

Cyber Security from Orange

Orange offers Business Internet Security – a managed security service leveraging industry-leading capabilities in areas such as intrusion detection and prevention, web application firewall, e-mail and web protection, anti-phishing and sandboxing, anti-DDoS, log and data correlation and reporting.

Findings – Orange Romania Business Internet Security Insights

Orange Business Internet Security (BIS) analyzes more than 5 million security threats monthly within our customers' security infrastructures. We gather anonymized relevant data from companies across industries such as government, automotive, retail, transportation and energy.
Data for this report was generated by correlating information from multiple security systems deployed within BIS, such as NG-firewalls, web filters, e-mail filters, DDoS mitigation systems and Intrusion prevention systems with statistics gathered from penetration testing and security audits performed for our customers. We used available data from the second half of 2018 up to August 2019.
We are using a Machine Learning-driven platform that leverages our Big Data Analytics capabilities of observing patterns in huge volume of data to detect new threats and zero-day vulnerabilities.

What's new: improved Threatmap

Threatmap began its journey as a real time analytics platform back in 2017, with real-time data gathered from Orange's Business Internet Security infrastructure – firewalls, endpoints, IPSs, sandboxes etc. Threatmap gathered anonymous data from all these 'sensors' and presented it in a human-readable format with insightful graphics and statistics.

After its launch, Threatmap received an innovative component – a free to use web vulnerability assessment tool powered by Pentest-Tools.com technology. This add-on allowed users to 'scan' their websites, in a non-intrusive and secure way- against the most common vulnerabilities. A detailed report of all vulnerabilities found is made available to the user after the scanning process is completed.
We further upgraded the 'Are you vulnerable' component to perform automated, anonymized and completely non-intrusive weekly scans of the Top 100 Most Visited websites in Romania and output the statistical results in the "Insights" Page of Threatmap. This allows Threatmap users to receive important information on the current threat level of the Romanian web and to better understand the risks of using unsecured websites. Users of Threatmap can now see a real-time map of cyberattacks detected in our BIS Infrastructure, various statistics about the top Threats detected, their impact on different business verticals and a short description of their effect and modus operandi and insights on the most visited 100 websites in Romania and their vulnerabilities.
The update is based on three innovative tools:

DEKENEAS

a waterholing attack detection service

Pentest-Tools

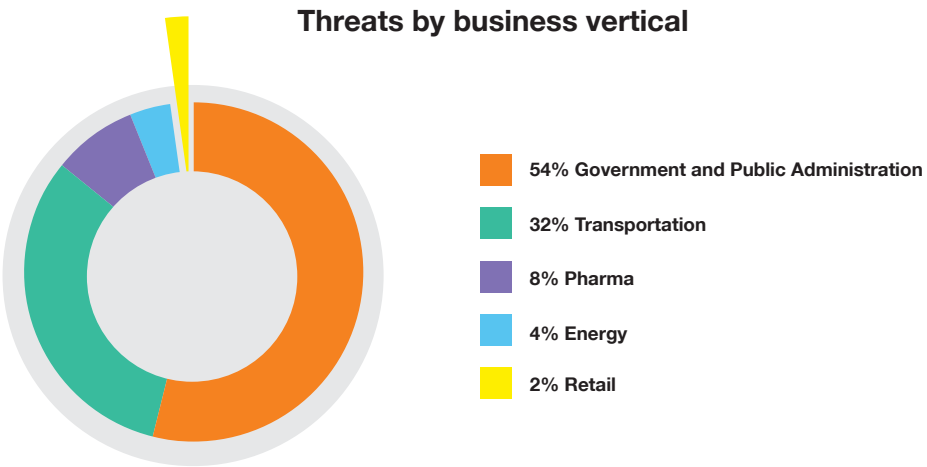
a service that searches for specific vulnerabilities of the most common publishing platforms

RO Hacked

a large IoC database of previously hacked websites

Distribution of threats by business vertical

The cyber threats landscape in Romania generally follows the international trends with vulnerable endpoints being the principal vector of infection and phishing threats the most common vector for distribution. We are noticing a worrisome increase in waterholing websites, used to spread malware to masses of unsuspecting users and a rise in DDoS attacks against essential service providers and critical infrastructure.



Public Administration / Government institutions, are once more at the fore front of both targeted and opportunistic attacks with the principal vulnerabilities being the massive technological debt of outdated computers, servers and applications, aggravated by the lack of security trainings and awareness programs for their users.

The ample variety of threats and attack vectors we're detecting ranges from portable media infection to phishing and spear phishing attacks. In fact, we believe that more than 24% of all the threats detected in the Public Administration and Government Institutions are using phishing as a means of spreading, including e-mails and social media / messaging services. We've noticed some DDoS attacks of low yield targeting some public institution's web services but the main category of threats for this vertical remains phishing.

While there are several technologies that can successfully mitigate phishing threats we strongly believe that cyber security awareness and training of users is paramount for cyber protection.

The transportation industry accounts for a third (32%) of all detected threats in the past 12 months. We have detected some interesting vectors and targets alike, with embedded and IoT-type devices beginning to 'show up' in the dashboards. These targeted devices include Mobility Access Points and Fleet Tracking Devices and while the attackers interest was mostly focused in 'scanning' these category of devices, trying to discover as much information as possible about their architecture and vulnerabilities, their final goal being to disrupt the services.

24%
of all threats detected for public institutions use phishing

Common vectors detected for the pharmaceutical industry were phishing e-mails and social media and messaging platforms with payloads ranging from ransomware malware to data stealers and banking Trojans. A major concern about data privacy is specific to this business vertical as the distribution and retail networks of large pharmaceutical groups, store and processes confidential patient data. Ransomware attacks in particular are a serious threat to large organizations such as pharma groups as they can compromise availability of resources and lead to massive infrastructure downtime and loss of critical data.

One such incident was the 2017 NotPetya attack that affected Merck, a U.S-based pharma giant – employees were sent home as most of their computers were completely locked down by the malware.

The cyberattack cost Merck about $670 million, including sales losses and manufacturing and remediation-related expenses, according to the company[5].

Key players in the **Energy** business are prime targets for large botnets that 'scan' the internet for exposed industrial/OT devices and **Retail** businesses are targeted by a vast category of threats, from DDoS attacks to phishing.

The Retail business is of particular interest to malicious actors who use infostealers and malware targeting customers of online stores. Attackers are trying to exploit poorly configured and unpatched online shopping platforms looking for customer databases of users, passwords, addresses, credit card info and social logins, with credit card data increasingly becoming a form of currency for hackers and retailers having lots of it.

Attackers try to exploit poorly configured and unpatched online shopping platforms

Point of Sales (POS) systems are a popular vector of attack for actors looking to gather transaction data. Technological advances in wireless payment models, including NFC 'contactless' cards, mobile phones and wearables are expanding the surface of attack for skilled actors. Fortunately, most of these systems adhere to at least a minimum set of cyber security requirements that makes them more secure than the previous generation devices.

”

CERT-RO built and operates a complex network for the detection and monitoring of cyber threats targeting the Romanian cyber space. Using various honeypots with different levels of interaction, this network can identify and observe unauthorized or suspicious activities that affect 'traditional' IT services such as HTTP/S, SMTP, DNS, TELNET, SSH, RDP, VNC, FTP, NTP et. al., Smart Devices, IoT and OT – SCADA equipment. The network also monitors attacks against crypto wallets and various administrative interfaces for network equipment. The data is collected automatically and processed in order to generate Indicators of Compromise (IoCs) which are distributed through a network of intelligent 'agents' to the beneficiaries of CERT-ROs monitoring services. This process provides increase protection of local entities by promptly identifying the threats targeting the Romanian cyber space.

CERT-RO is building a subscription-based platform for threat sharing allowing interested parties to access information, IoCs and samples of the latest threats affecting the national infrastructures.

By implementing these measures, CERT-RO wishes to identify the threats that affect the Romanian cyber-space, in correlation with global events, and deliver predictability for future attacks, thus reducing the impact of these threats on the Romanian users.

Andrei Bozeanu
Cyber Security Researcher, CERT-RO

Innovative cyber security detection tools

”

When it comes to malware and viruses, there are multiple solutions that can help in preventing the infection, and the most common tools are: Endpoint Protection with AntiVirus and AntiMalware, Sandboxing, Endpoint Behavior Analysis

Each cyber security vendor implements unique functions in their products to speed or ease malware detection and activities or malware like programs customized for a certain customer or network.

Despite of the above mentioned products and methods, there are some advanced malware programs that before taking any action on the target device, are testing the environment in which are present. They verify if prevention tools are deployed and are trying first to disable them, or are verifying if they are running in a sandboxing environment or not, and some more advanced malware can wait for specific user activity before activating.

Besides advanced malware, zero-day vulnerabilities can be exploited by malicious actors, which are using advanced techniques in order to penetrate and exploit the targeted network.

In order to protect against these advanced malware programs and advanced penetration techniques it is quite hard to deploy a traditional security solutions that can also bring visibility into this type of activity.

Luckily, the cyber security vendors are investing lots of resources into keeping the pace with bad actors and they are constantly developing new products or tools that are helping in protecting our networks. One tool, result of research and development is FortiDeceptor, developed by Fortinet.

This product is automating the deployment of Deception Virtual Machines and decoys to lure and stop the attackers that have breached the network. The purpose of this tool is to deceive, expose and eliminate advanced attacks by breaking the kill chain and stopping malware from spreading while providing visibility into malicious activity that could have bypassed traditional security controls.

FortiDeceptor deploys Deception VMs and Decoys which inspects the behavior of the attacker and validate the malicious intent. Attackers are redirected to deception hosts and away from customers’ real production servers, thus protecting high value company assets. When an attack has been detected, actionable intelligence (Indicators of Compromise) are subsequently generated and the information is shared across a broad set of in-line security controls through the integration with Fortinet's Security Fabric to proactively block these unknown threats in real-time. Companies can create automated response processes to shut down current attacks and to prevent or detect future attacks. Security operations teams are notified with alerts and counter intelligence so that the kill chain is broken and attacks can be shut down immediately.

One of the main benefits is that it can expose hacker activity with early, accurate detection and actionable alerts. It can also trace and correlate hacker’s lateral movement and notify Security Administrators through Web UI, email, SNMP traps and logs. Another huge benefit is that it can correlate incident and campaign information of attackers’ traffic in order to identify the target system or network asset.

The attack methods and tools have become more sophisticated, that is why there is a need for innovative and advanced protection solutions that are using Machine Learning, Artificial Intelligence, automated correlation and analysis. Such solution is FortiDeceptor, an advanced cyber security tool that is adding an additional internal defense layer complementing the existing traditional cyber security tools.

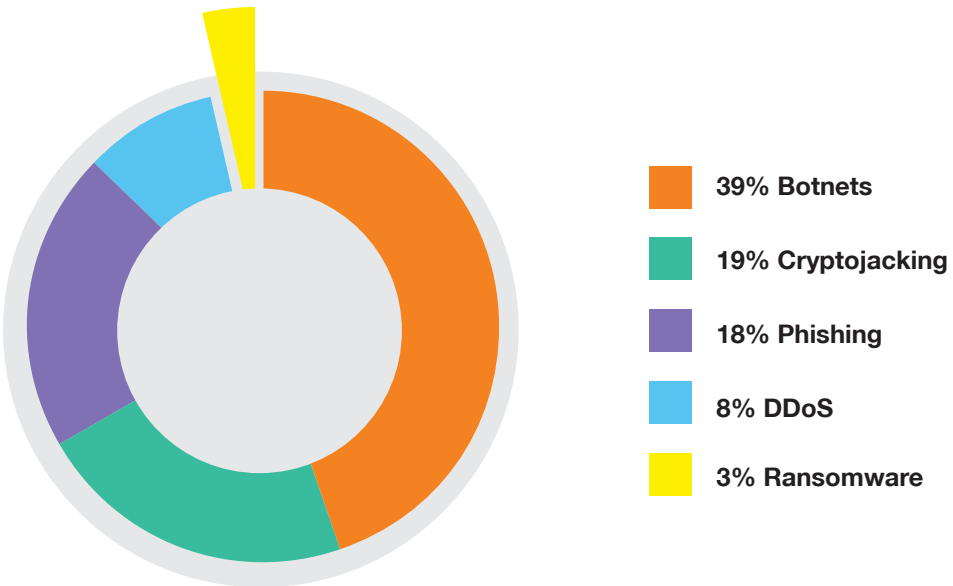
Mădălin Vasile
System Engineering Manager, Fortinet SEE

FORTINET®

Distribution of threats by type

Looking at the distribution of the most wide spread types of threats for the past 12 months you will notice that the national threat landscape hasn't changed too much from the first edition of this report. The type of threats stay the same but their distribution levels vary with Botnets becoming the most common threat for Business Internet Security customers, followed by Cryptojacking and Phishing. DDoS spiked in incidence in the first half of 2019 and Ransomware is in a steady decline by detection rate but still poses a major concern to vulnerable infrastructures.

Threats by type



84% **of the tested companies are exposed.**
If you are wondering if your company's systems are vulnerable, specialists say that most probably they are. For 84% of the companies tested through Orange Romania's platforms, we discovered critical vulnerabilities.

Let's dive into the most common type of threats that we detected in our Business Internet Security platform infrastructure in the past 12 months.

Botnets: The zombie computer armies

Some fifteen years back, zombie armies were invading the TV screens of movie fans – playing back a DVD or a VHS tape rented from the local shop. Nowadays zombies are taking over the internet in the form of massive botnets, some of them relying on today's smart TVs to spread their malicious content.

A botnet is a group of computing devices, all infected with malware (usually the same strain of malware) that gives the malicious actors remote control of these devices in order to surreptitiously commandeer them without their owner's knowledge. The 'herder' can send commands and instructions to the group of devices via the internet from a C2C (Command And Control Server) to act in a malicious way such as steal user's private information like credit card numbers and banking credentials or as using their internet connections to drive massively Distributed Denial of Service attacks against websites or other targets in the internet or to deliver spam and malware to victims.

The first malware cited as botnet was the Morris Worm, unleashed in 1988, infecting thousands of computers on the ARPAnet (the Internet's precursor). While the person that wrote Morris didn't actually controlled its victims' actions, the worm spread uncontrollably to most of the machines networked in this proto-internet.

Decades later, in the early 2000s, botnets such as CoreFlood commandeered nearly 3 million machines and gained it's operators earnings in the low 6-figures. CoreFlood was operational for more than 10 years with authorities shutting down its operations in 2011. Botnets like Bredolab, SpyEye or Zeus have been around for some years now being extremely profitable to their herders as they steal and siphon banking credentials and credit card info and even automate the process of siphoning money into the author's accounts.

One notable entry in the formidably-long list of botnets is the Conficker Worm Botnet that infected over 10 million machines back in 2009 and is still 'in the wild' today. It used a sophisticated method of communications (at that time) – in the form of Dynamic DNS to prevent its C2C Servers from being shut down. The worm proved to be fairly anticlimactic as no one has ever been able to determine its purpose, only to fear the activation deadline of 1st of April 2009, as it was indicated in the malware's code. April 2009 long came and went to no avail as no immediate event happened on that date.

botnets cost more than 110 billion US dollars in losses, globally, over time

It was later discovered that in the early 2010 some criminal groups from eastern Europe, Ukraine and Russia used Conficker as a banking infostealer botnet with a very pricey 72$ million tag.

One of the latest large-scale army is the Mirai Botnet that spreads to 'Smart' devices, embedded devices, IoT and edge-connected devices such as home routers, Internet connected surveillance cameras, smart-home category products, smart-TVs etc. All. This botnet was prevalent for the most part of 2017 and 2018 with some 500 million infected 'zombies'. It's only recent that researchers found several other large-scale botnets that aren't simple Mirai clones, such as Chalubo bot, the Tori Botnet and the Hadoop cluster hijacking DemonBot.

Romania is a prime target for both victim armies and C2C servers as we still have to deal with a compliance and regulatory gap which means there's a large install base of pirated copies of various commercial operating systems and applications. This represents a vector for malware distribution as a large group of users do not activate protection mechanisms such as Endpoint Anti-Malware solutions. The widespread availability of high-bandwidth high-capacity connectivity, for both residential and business consumers means that malicious actors can orchestrate efficient DDoS attacks stemming from zombies in Romania.

Orange Business Internet Security solution offers protection against large DDoS attacks and against infection and spreading of botnet malware, successfully blocking the detected threats. In the past 12 months we've detected and blocked nearly 1 million attempts of infestation with malware specific to Botnets and up to 10.000 DDoS attacks targeting our customer's infrastructure.

1/2 billion computing devices become victims of botnets each year, with an infection rate of almost 20 devices per second

What is cryptojacking?

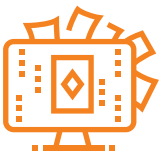
This type of malware leverages computing power of as many devices as they can to generate ('mine') cryptocurrency for the attackers. This translates to increased usage of infected systems, availability issues, increased power consumption and can trigger other web and network-based attacks. Cryptojacking attacks are carried out without the user's knowledge, usually via a script that loads when the unsuspected user visits a website infected with the malware.

Cryptojacking

detections in 2018 = 10x detections in 2017

These websites are sometimes legitimate sites that were compromised and changed to run the cryptojacking script(s).

How it's done?



Attacker uses Coinhive code (or equivalent) on hacked websites to trigger the JavaScript miner on the victim's computer

Victim's computer browser will then mine in the background, without the victim's consent

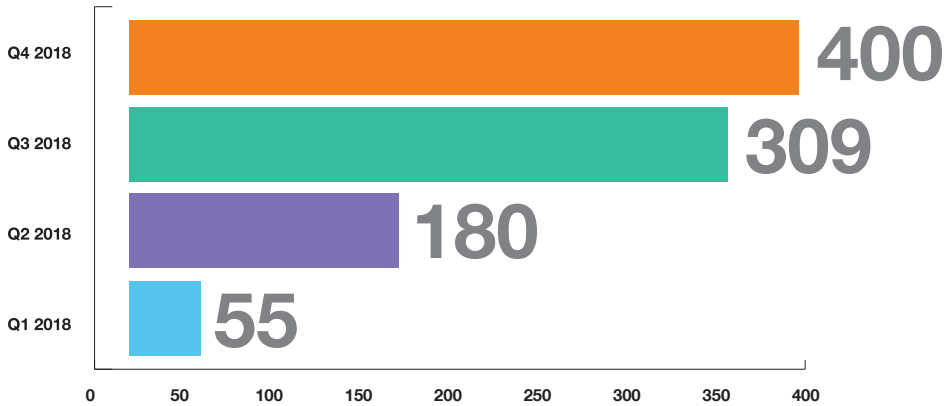
In most cases, these are however, spamming sites that offer illegal free downloads of games, applications or video content or adult websites.

The most common types of cryptomining malware are browser-based, relying on services such as Coinhive to force visitors into crypto-mining while visiting infected websites, in most cases without any indication to the visitor.

One notable vector is CMS – Content Management Systems, specifically vulnerable CMS plugins such as Wordpress plugins that account for almost 4000 critically vulnerable such add-ons.

This noticeable shift in cryptomining malware and cryptojacking drove the global detection rate in 2018 to up to 400 milion detections by Q4 2018.

More than 400 million cryptomining malware detections happened in 2018:



Total cryptojacking detections in 2018 (million)

DDoS – Distributed Denial of Service – the prevalent use-case for large botnets

In its simplest form, a DDoS is an attack attempting to make an online service unavailable by overwhelming it with traffic from multiple sources.
We'll work with the information above to better understand the how and whys of DDoS attacks. First – a DDoS is an attempt to doing something. This implies that there are sufficient methods and technologies that can mitigate to some extent the success of such an attack.

Business Internet Security uses detection and filtering of botnet traffic to protect its customers from DDoSes

Moving on, a DDoS will target an online service – websites, online banking portals, news outlets, social media platforms etc. This is essential for understanding the motivations of the attackers and it usually revolves around their determination in making sure that people can not publish or access information.

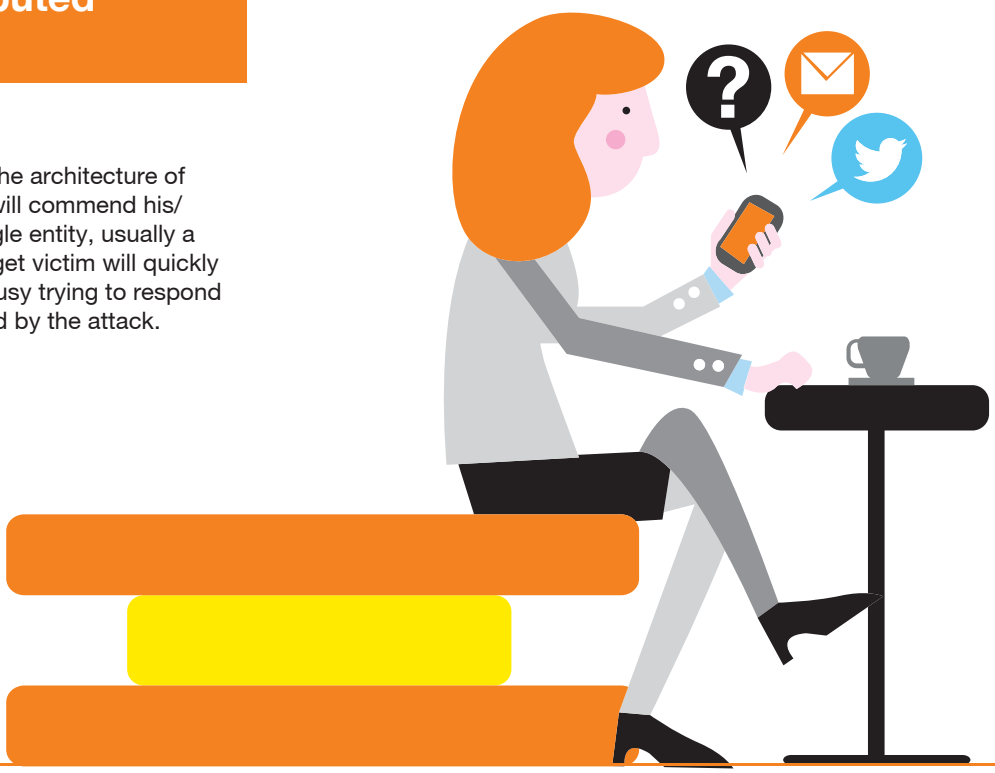
Bottlenecks – a DDoS leverages the power of large-scale botnets to overwhelm its victims with traffic. Think of thousands of festival-goers trying to access the festival site at once, using a single gate that can usually accommodate tens of customers.

2000 DDoS attacks each day with 1/3 of all downtime incidents being attributed to DDoS

This analogy is useful to understand the architecture of a DDoS attack – the malicious actor will commend his/hers botnet to send requests to a single entity, usually a webserver hosting a website. The target victim will quickly become unavailable to users as it's busy trying to respond to the avalanche of requests stemmed by the attack.

Multiple sources – a DDoS success is a function of capacity and capacity is – in its turn – a function of numbers and bandwidth: more victims in the botnet means more bandwidth, more bandwidth means more capacity for the attacker to bring down even the 'largest' websites or online services.

In recent history most of the Internet's largest services have been victims of DDoS at one point. This includes Facebook, Google, Microsoft, Apple, Amazon, Netflix and many, many more. In fact, Arbor Networks' ATLAS observes more than 2000 DDoS attacks each day with 1/3 of all downtime incidents being attributed to DDoS.



Ransomware is still a (big) thing: while attack incidents are down compared to Q4 2018, new variants such as Mark of Zorro and Anatova prove to be more effective in usage compared with their 'traditional' counterparts such as WannaCry, Petya/NotPetya and BadRabbit. These next-gen ransomware strains employ advanced forms of detection evasion technologies and modular design that allows the attackers to deploy customized 'builds' of the malware by adding modules specifically crafted for different endpoints. This form of decentralized distribution, in an AppStore-type mode is becoming the standard model of distributing such attacks.

A ransomware attack is a form of crypto malware that infects the victim's computer with the intent to threaten to publish the victim's data or temporary block access to it until a ransom is paid. Most ransomware attacks use a technique called crypto-extortion in which it encrypts the victim's files, making them inaccessible and demands a ransom payment – usually of the untraceable crypto-currency type- to decrypt them.

How it's done?

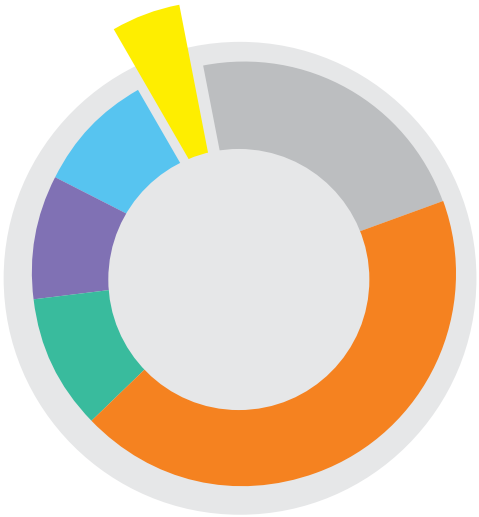
- In a Fileless attack, the attacker usually deploys toolkits that exploit specific vulnerabilities found in commonly used operating systems and applications.
- Most often, an exploit kit is executed when a victim visits a compromised website. Malicious code hidden on the site will redirect the victim to the exploit kit landing page, unnoticed. If vulnerable, a download of the malicious payload will be executed and the system becomes infected and – most of the times – encrypted with a public/private key pair.
- The malware then displays a notification to the user, asking for an untraceable cryptocurrency transfer to the attacker in exchange for the decryption key.
- In a file-based attack, the victim usually downloads and executes a malicious file (be it a portable executable -.exe file, a Word document with macros or a .JS file. Upon execution, the malware downloads and runs the malicious payload and the system becomes infected.

Mobile malware

We gather anonymized data and statistics from our Orange Antivirus solution to better understand the current status and trends in mobile malware in our large user base.

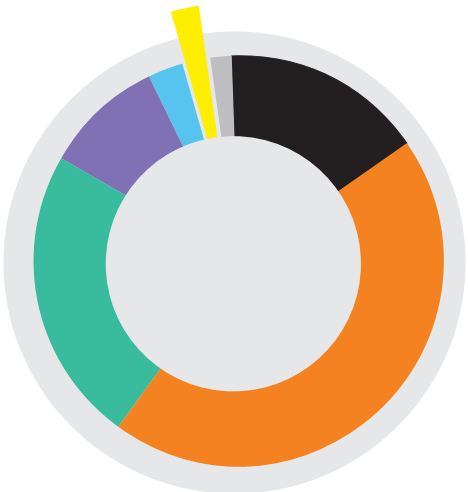
The usual suspects are the run-of-the-mill Trojans hiding adware, SMS and web subscribers, rootkits, app installers, downloaders, credentials stealers, bankingware etc.

We're reporting a decline in the number of detections, year-over-year, as users are updating their apps and Operating Systems to the latest available versions on a regular basis.



Distribution of Trojan Infections

- **43.36% Trojan.Downloader**
- **10.37% Trojan.Cunk**
- **9.34% Trojan.HiddenApp**
- **9.34% Trojan.HiddenAds**
- **5.19% Trojan.SmsSpy**
- **22.40% Others**



Distribution of Potentially Unwanted Applications

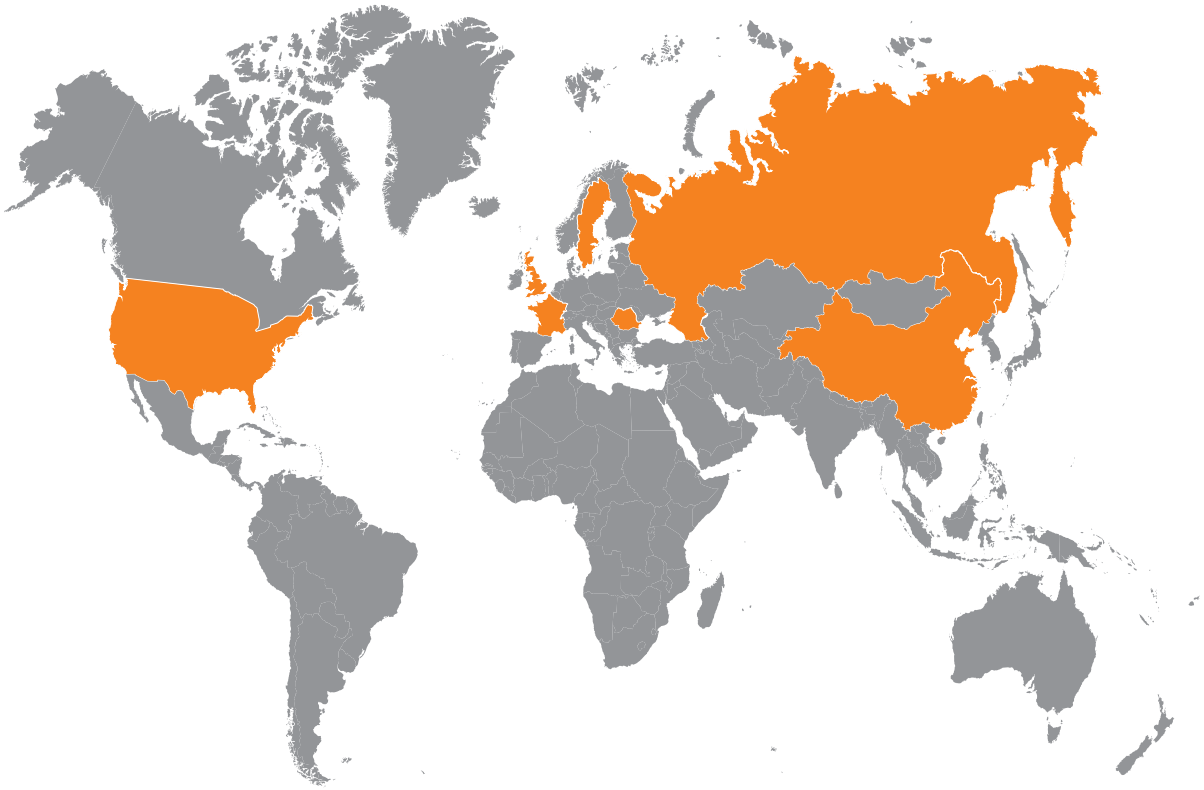
- **44.80% Riskware.TaJawaBar**
- **23.29% Adware.Agent**
- **9.60% Adware.Dowgin**
- **2.59% Adware.Yekrand**
- **2.24% Adware.Mulad**
- **1.67% Riskware.SMSSend**
- **15.81% Others**

Global mapping of cyberattacks

As most of these attack sources actually use spoofed source IP addresses it's difficult to precisely identify the 'true' source of attack, i.e., the command and control center of the botnets or the geographical location of the attacker(s).

We use threat intelligence feeds to automatically update our firewalls with the latest IPs found to be C2 servers for various Botnets or found to host websites with embedded malware used in phishing attacks. 2018 sees a spike in C2C activity controlling large-scale cryptomining zombies as malicious actors are branching out of the malware-spreading for destructive purposes business and reaching into the distributed mining business.

Sources of attack



49080	37090	13000	11000	8000	4300	3890	1800
USA	China	Romania	Russia	France	Singapore	Sweden	U.K.

Emotet: A (brief) case study

Whilst sounding like an ancient Egyptian king, Emotet is in fact a nasty piece of banking Trojan that evolved into a veritable malware platform with various use-cases detected around the world in the past 3-4 years.

Emotet was first identified by security researchers more than 5 years back, being originally designed as a banking malware that spread through spam and phishing e-mails, hidden in malicious document macros, embedded scripts or links.

Emotet uses various forms of obfuscation to prevent being detected by anti-malware products and has worm-like capabilities that allows it to move laterally trough computer networks being, practically, a self-contained distribution and delivery agent.

The United States Department of Homeland Security concluded that Emotet is extremely costly and destructive with costs upwards of $1M per incident.

Emotet is polymorphic – this means that it can change itself every time it is downloaded, successfully evading traditional signature-based detection techniques like the ones used in most corporate networks. Moreover, it can detect if it is running inside a Virtual Machine and if so – it chooses to lay dormant and evade detection in a sandbox-like environment.

In its latest versions it gained C2C capabilities allowing commanders to control its zombies and push updates and malware modules – think of payloads with specific functionality, i.e. for a certain version of a business application. These updates are fully transparent to the victim user as it happens in the background using a mechanism very similar to Microsoft's Windows Update.

In final, Emotet can perform various malicious actions like spreading itself through the corporate computer network, stealing banking credentials, capturing keystrokes, deploying any other type of malware, stealing usernames and passwords and even modifying system files and configuration.

Emotet is quickly becoming the 'go-to' platform for malicious actors mainly because its versatility and availability of modules for most types of attacks.

Emotet spreads opportunistically and targets everybody – from individuals clicking on malicious links in e-mails to large corporate users opening Word documents. There were reports of Emotet 'hitting' all around the globe and our Business Internet Security anti-malware component 'caught' samples of the malware trying to infect customers from Romania, across multiple business verticals.

Protection and Prevention:

Knowing how Emotet works and spreads is key knowledge in order to protect your computers and users against this malware. There are some additional steps you can take:

1. Update: keep your computers up-to-date with the latest Operating Systems patches and Application Updates.

2. Do not download suspicious attachments from e-mails. Do not follow links you are unsure of. Read all e-mails carefully and delete those that look suspicious

3. Strong passwords and two-factor authentication is the way to go. You can actively prevent someone logging in your accounts –even if they have your passwords – if you use two factor authentication

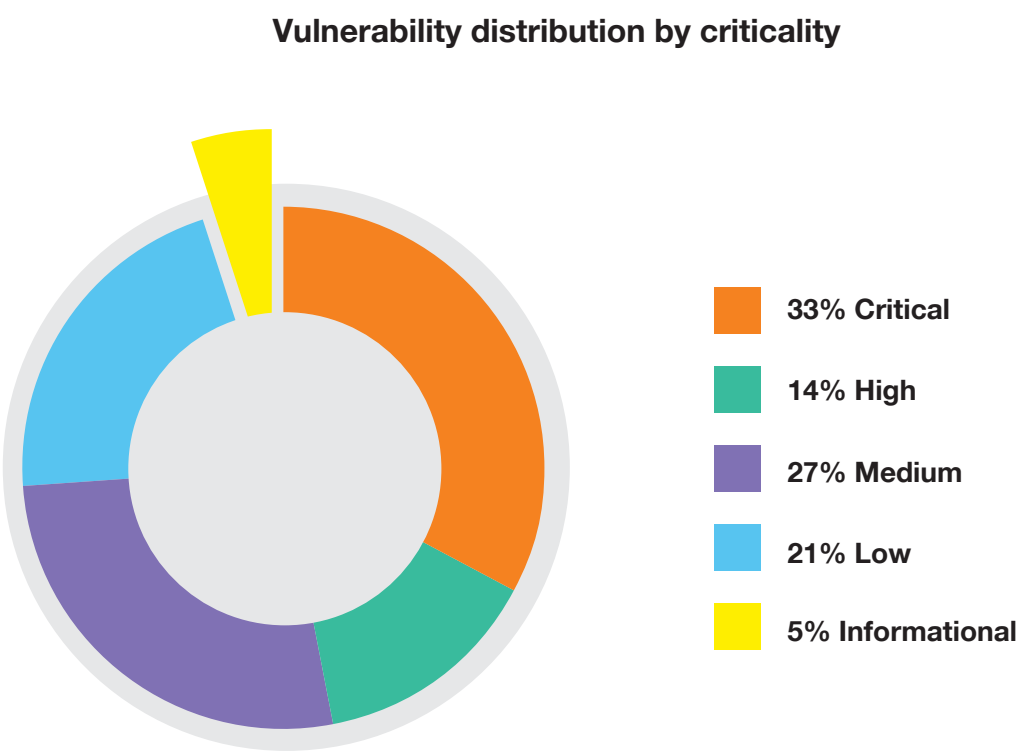
4. Use a robust and complete cyber-security protection technology such as Business Internet Security from Orange

Emotet is extremely costly and destructive with costs upwards of $1M per incident

Vulnerability distribution by criticality

The distribution of threats by criticality follows a risk-based assessment model where vulnerabilities and weaknesses that can be exploited are ranked as per Mitre's CVE – Common Vulnerabilities and Exposures System.

The severity ranking used herein is closely linked with the CVSS 3.0 base score for each weakness, with values in the range 9.0 to 10.0 matching the "Critical" level, followed by "High" 7.0 to 8.9 as per CVSS, "Medium" for 4.0 – 6.9, "Low" for 0.1 to 3.9 and finally – Informational which represents a qualitative severity ranking of precisely zero.



”

Malware authors are permanently innovating to find new infection vectors in order to spread their creations. Cybercriminals are always doing everything in their power to become more effective and accurate. While in the past years we've seen a lot of ransomware attacks and crypto mining malware, these days we see more targeted attacks so cybercrime is getting more personal.

For instance, in June several Romanian hospitals were hit by ransomware attacks almost at the same time. Many cybercriminal groups are still looking for fame and they create a lot of buzz around them, but there are others who take their time to conduct surveillance activities in order to ensure they hit the right target. In the end, the motivation remains the same: MONEY. We also expect an increase into using state-of-the-art technologies to communicate with C&C in order to bypass security monitoring measures.

In July, Network Security Research Lab of Qihoo 360 reported that the new Godlua malware evades traffic monitoring by using DoH (DNS over HTTPS), a proposed standard as of October 2018 that is already supported by quite a long list of publicly available DNS servers, as well as web browsers like Google Chrome and Mozilla Firefox.

On the other side, we have the organizations. More and more companies are becoming aware that they can easily transform into a target. That is why they started to use antivirus solutions, perform backups, encrypt PCs or focus on educating their employees on what social engineering tactics might an attacker use.

Moreover, we must take into account that technology is evolving and AI is very attractive for companies who want to develop fast and efficient but also attackers are seeing this so probably we will see more complex attacks in the near future based on the latest cutting edge technologies.

Andrei Avădănei
CEO Bit Sentinel

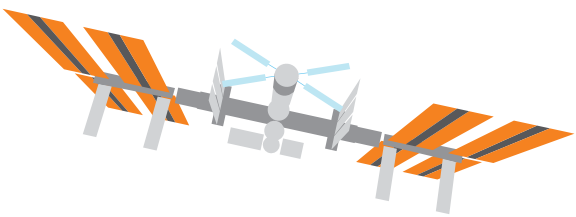
Timeline of events

Sept 2018

- On September 6th, British Airways announced it had suffered a breach resulting in the theft of around 380.000 customer's data, including personal and payment information. The attackers were a familiar adversary – the Magecart APT Group.

- The United States State Department confirmed it was affected by a data breach that lead to employee data being exposed. The breach affected the Officials' unclassified e-mail systems and the incident came to light only after Politico got hold of a notice about the breach, on September 7.

- California State passes legislation that bans default password, hardcoded or elsewhere, from all connected devices to be sold and used in California starting from 2020. The legislation states that passwords must be unique to each device.



Oct 2018

- Cathay Pacific breach exposes personal data for 9.4 million people including travel histories as their systems were breached at least seven months back.

- Apollo, a sales engagement solutions company had its database hacked with a possible 200 million records being stolen. The data included names, job titles, employers, phone numbers, and email addresses.

- Up to 30.000 military and civilian personnel have had their personal information and payment card data exposed following a security breach at the third party vendor that provides travel management services for the United State Department of Defense.

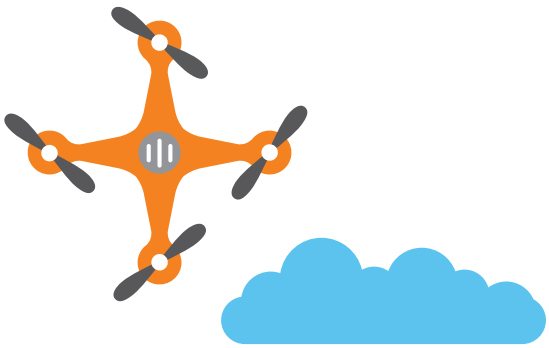
Nov 2018

- In what has to be one of the largest data breach in terms of affected users, Marriott Hotel Group announced that the guest reservation database used for Starwood reservations has been compromised exposing private details of up to 500 million guests.
- United States Postal Service (USPS) site exposed data on 60+ million users. The issue was addressed by USPS no sooner than one year after it was first reported by an anonymous researcher.

Dec 2018

- Google admits it's Plus service was subject to a critical privacy flaw that could have exposed personal data such as usernames, e-mail addresses, photographs to a third-party, via a flawed API. This security issue could have affected more than 52 million ursers.
- 100 million users's data was stolen by hackers that breached Quora.com. Data included full names, e-mail addresses, passwords, direct meesages, answer requests and any public content and actions.

Jan 2019



- Close to 25 million financial and banking documents representing tens of thousands of loans and mortgages from U.S. banks have been found online after a severe security breach. The culprit was an elasticsearch server containing a decade's worth of data.

- More than 140 airlines affected by major security flaw in the Amadeus online booking system, widely used by most of airlines. Amadeus is used for nearly 45% of all bookings and reservations. The flaw was discovered on Israel's El-Al National Airline's website that pointed the user to an URL which could be easily modified to view a PNR page containing personal information.

- Someone uploaded a file containing more than 773 million plaintext passwords and associated user accounts. The file first appeared on the file sharing service Mega but has been deleted since. It was distributed in the form of 12.000 separated files totaling 87 GB of data.

Feb 2018

- A Pakistani hacker claims to have hacked dozens of popular websites and selling their databases online for nearly 127 million records. The same hacker claimed to have access to another 620 million records originating from 16 hacked websites such as 500px, MyFitnessPal, Artsy, Dubsmash Those are up for sale as well.

- Romanian Police, in collaboration with BitDefender and Europol have released a free data recovery kit for victims of the Grandcrab Ransomware that affected tens of thousands of users in the previous months. The tool was made available through the nomoreransom.org portal.

Mar 2019

- Orange County located in the Los Angeles Metropolitan Area of California has been the target of a focused ransomware attack that caused downtime to digital services offered by the local authorities. Most such services such as marriage registration licenses or real estate dealings have been shut down temporarily.
- Nearly 810 million records containing e-mail addresses were disclosed via an unprotected, publicly accessible MongoDB Instance. The records stemmed from an e-mail marketing company.
- An unsecured server exposed more than 2.3 million user's private data and shopping lists from online shopping giant Gearbest. The researcher that disclosed this vulnerability claimed to have found an unprotected elastic search server that anyone could access.
- According to the Department of Homeland Security, FEMA mistakenly exposed personal information of 2.3 million disaster victims including survivors of hurricanes Harvey, Irma and Maria. The exposed info included addresses and bank accounts.

Apr 2019

- India in the news as several apparently unrelated breaches leave a least 100 million peoples data exposed. The Government Healtcare left an unprotected database with more than 12.5 million pactient records, exposed on the web then more than 78 million people sensitive data was found on an hard disk In an unrelated event, India's JustDial service is breaching user;s personal data in real time.

- Georgia Tech says data breach exposed info on 1.3 million people as someone gained access to a unsecure web application. The victims include former and current faculty members and the data stolen may include name, addresses, birth dates and Social Security Numbers.

- Scranos, an info-stealer malware operating with an apparently valid digital certificate began to spread through Romania after infecting mainly Chinese targets. The malware can be 'customized' by adding various modules that can either extract cookies and credentials from most common web browser or can steal user's payment data from sites like Facebook or Amazon.

May 2019

- Ladders, one of the most popular job recruitment sites in the U.S. specializing in high-end jobs, has exposed more than 13.7 million user records following a security lapse that left a Elasticsearch Database exposed to the internet without a password.

- WhatsApp, the Facebook-owned instant messaging app confirmed an important vulnerability in their system on Monday, 13 May that left users open to spyware installation on their devices. This vulnerability targets both iOS and Android users and enables an attacker to install malware by leveraging a serious bug in the way voice calls are handled by the system. WhatsApp prompted it's users to update the Application to its latest, safe version.

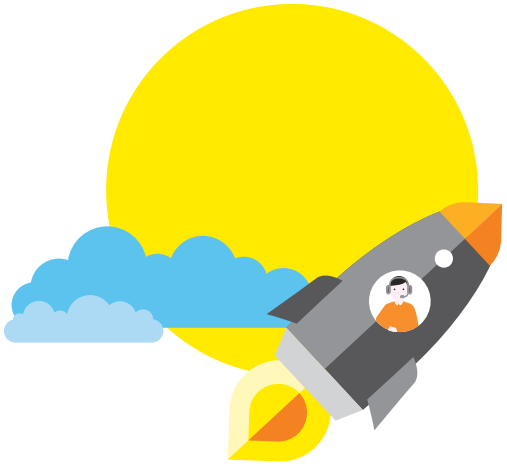
- An ongoing attack targeting the users of more than 105 e-commerce websites is used to steal credit card information, as a cyber security research firm revealed. Researched monitored known malicious domains for several months and found that the JS scripts used on these domains are spread to more than 105 other e-commerce sites. The scripts in question are used for credit skimming.

June 2019

- Five hospitals in Romania were infected with a variant of BadRabbit, a 2 years-old strain of ransomware. The malware spread through phishing campaigns and exploited the unpatched, unprotected and outdated systems in use. The attack managed to compromise some data although the extent of the damage is unknown as of this writing. Some of these incidents were reported to CERT-RO's 1911 hotline for Cyber Security Incidents Monitoring and were investigated by specialized teams from SRI.

- Researchers from security company Cybereason stated that hackers broke into the systems of more than a dozen global telecom firms, in a seven-year campaign and stole large amounts of data. The hack is believed to be linked to Chinese espionage groups.

- Filesharing service WeTransfer had a bit of a mix-up sending data to the wrong people for a two-days period. The company announced the security incident stating that users began receiving e-mails confirming transfers on the 16th and 17th of June 2019.



May 2019

- A Japan-based cryptocurrency exchange called Bitpoint has become the latest victim to lose large amounts of money in an on-going cat-and-mouse game of poor security and electronic wallet hackers. A total of 3.5 billion yen (USD 32M) had been stolen, a large portion of this amount – up to USD 23M of which were customer-owned funds.

- A publicly accessible ElasticSearch cluster owned by Orvibo, a Chinese smart home solutions provider, leaked more than two billion user logs containing sensitive data of customers from countries all over the world. We are losing count of incidents involving unsecured Elastic clusters.

Aug 2019

- A security bug discovered in British Airways' e-ticketing system has the potential to expose passengers' data, including their flight booking details and personal information. The British airline operator has since patched their system but this is not the first time BA's online reservation systems are found to be vulnerable.

- The fingerprints of over 1 million people, as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees, was discovered on a publicly accessible database for a company used by the likes of the UK Metropolitan police, defense contractors and banks.

Education, innovation, 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.

In 2019 we extended our program with a 'Spring School' session in Iaşi, at the Faculty of Computer Science from Alexandru Ioan Cuza University. Our tutors prepared courses, workshops and hackathons on Computer Forensics and

Threat Hunting successfully engaging students into cyber-security topics and paving the way for a complete curriculum in 2020.

We've seen great engagement from the students participating in a 24-hours hackathon, challenging them to build a home-cyber security gateway using only open source software on a cheap, widely available x86 computer. They worked in teams and delivered some ingenious designs, leveraging some of the theoretical and practical – hands-on-knowledge in virtualization, cloud computing and distributed computing.

The European Cyber Security Challenge

We support Romania's team for ENISA's European Cyber Security Challenge, a yearly event in which some of the most talented young people in Europe team up against their contenders in a 2-day hacking marathon with challenges in areas such as encryption, steganography, web security, computer forensics, malware analysis.

Orange offers not only financial support, but also mentoring and training, delivered through softskills presentations and security challenges.

This year's ECSC main competition takes place between 9-11 October, in Bucharest, Romania with Orange being one of the main sponsors of #TeamRomania.

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

The project is already well into the development phase with contributors working on building the software components of this Risk and Resilience Enhancement Platform.

Here at Orange we are preparing for testing these software components in a complex, multi-tier connected scenario in which our test-bed will be the target for several cyber and physical attacks.

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 will be interconnected to other RESISTO members testbeds.

www.resistoproject.eu

UNICORE

Here at Orange we are constantly researching new ideas, new technologies and new tools that better serve our goal of providing the best cyber-security services. From applying Machine Learning and A.I. to huge datasets in order to find anomalies in usage and stealth attacks and threats, to sharing threat intelligence with other industry-leading players, researchers and practitioners, Orange is continuously investing in research.

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/

Orange Fab - corporate accelerator

Orange Fab Romania is part of the Orange Fab international network of accelerators, currently operating in 17 countries all across the globe. The program was initiated in 2017 and, from the very beginning, had a dedicated Security track.

Orange Fab offers innovative startups:

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

More datails on www.orangefab.ro

"

At Orange Fab, we work with startups in various fields, from IoT to Machine Learning or Big Data, with applications in various industries. Having technology more and more intertwined in the way we live and work daily, comes with a big challenge to make sure our data is safe and is being used in genuine and well-intended manners.

We are actively searching for startups solving various security issues, as well as educating and supporting all entrepreneurs we work with to ensure the highest level of security in their products and in all their interactions with the clients.

Monica Obogeanu
Startup Programs Manager, Orange Romania

In 2019, **Siscale** joined the Orange Fab Romania's security track, and from the previous years we still collaborate with three other powerful security startups:

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/home

Dekeneas

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

www.dekeneas.com/

Appsulate (recently acquired by Zscaler)

isolated environment that acts as a shield between the user and web applications, preventing data exfiltration and providing control, monitoring and compliance with security standards.

www.zscaler.com/products/browser-isolation

Siscale

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

www.siscale.com

Orange Fab was a great opportunity and venue for Siscale to showcase how Machine Learning and AI addressing the ever more complex world of real time security and threat analysis/mitigation with a new state of the art platform called Intelscale.

Intelscale is a scalable, open threat intelligence platform with strong analytics and machine learning capabilities. The solution combines custom deployment with the rich experience of our engineers, coming from a security and IT infrastructure background.

Intelscale provides all the features that a Security Operation Center requires in today's world. Using a comprehensive threat intelligence processing framework it can aggregate and filter indicators from a variety of sources and intelligence feeds and identify/detect hosts and other anomalies contained within incoming security log data. Intelscale innovations in Machine Learning not only reduce false positives but can also apply counteraction/mitigation and extended automation, reducing the manual load Security Operations.

Siscale is an international systems integrator leading AIOps adoption in more than 15 enterprise Fortune 500 customers across the US and Europe. Siscale has successfully integrated Big Data projects for customers in the Information Technology, Retail, Healthcare, Financial Services, Insurance, Telco, Life Sciences and other industries. Part of the growing Data Revolution, Siscale was born as an integration pioneer in this area and has been evolving at the pace of the industry right from the beginning.

Siscale is a team of professionals with long and varied experience in the IT & Telecom market for the past 20 years, planning, designing and implementing data ingestion and processing pipelines from various industries use cases, using cutting-edge technology to shorten solution time-to-market. We help our customers to monetize available data to enrich the relationship with their clients, create additional revenue streams or optimize their operations.

During our experience at Orange Fab we had the opportunity to validate our Intelscale solution in the company of experienced professionals both technically and from a business perspective. The Orange team was extremely helpful in guiding us in our Fab journey.

Peter Ruţă
CEO and Founder, Siscale

Highlights: Relenting control: A new era of automation

The automotive industry has been – for decades – one of the last large industries not heavily reliant on software code in their final products – the vehicles. There was a visible line between the electrical and mechanical control systems used to operate a vehicle and their software counterparts, used to perform computer tasks.

The security implications for crossing this line were deemed to be too big and up until recently, most vehicles used by the general public were operated under the complete, utter control of their user. A steering column –be it electronically enhanced – will connect key components of the car's mechanic to the hands of the driver, on the steering wheel and allow her or him to literally turn the wheels of the car. On the other hand, the car entertainment system is generally computer controlled in fact – it is usually a full-fledged computer with a simpler U.I. paradigm than your average Windows or Mac laptop.

62% of responders from the automotive industry think it is very likely that their software will be the target of malicious attacks

People have been reluctant in relenting their physical control over the mechanics of a moving vehicle but – in recent times - they were more than happy to have a computer in charge of various other secondary tasks such as navigation and entertainment or climate control.

Today we are witnessing a shift in this paradigm with assisted driving becoming the norm for most modern vehicles, in various forms from intelligent 'self' parking to autonomous driving with speed and directionality control. This is possible with the advent of low-latency high-reliability wireless data networks (think 5G, LoRa, LTE-M etc.) and low-power embedded computers capable of processing large amounts of data within neural networks and specialized silicon for tasks such as Machine Learning. Of course, the technology that ties it together is software in various forms and –as per everything we've learned as of today- software can be and at most times will be vulnerable to cyber threats.

Thinking of some of the high-profile cyber security conferences, CTF competitions and practical demonstrations in the past decade, there were several competitions in the broader 'hack the car' category where talented cyber security people managed to gain access to in-vehicle systems that allowed them to actually control the dynamics of the target car – brakes, acceleration, directionality.

Fortunately most of these demos happened in a controlled environment, as they targeted test vehicles, not in current production and their findings gave the manufacturer sufficient time to investigate and fix the vulnerabilities.

Betting on the transformation of the transportation and automotive industry, stakeholders are pushing these security issues under the radar of their researchers and are trying to develop functional frameworks for resilience and cyber security in the key areas of assisted driving and autonomous vehicles.

The road is, however, long and difficult as some surveys found that up to 62 percent of responders from the automotive industry think it is very likely that malicious attacks on their software or components will occur in the next 12 months.

This study also shows that software security is not keeping pace with technology in their industries, as a result, connected vehicles have a range of unique security issues.

What can be done to improve the security of these systems of critical importance? While there's no definitive answer there are some key factors that can drive the security and resilience of such technologies to levels acceptable by society.

One can start by identifying threats such as the possibility of malicious actors to either gain access to personally identifiable information (PII) and / or inject malware in the critical software components of a vehicle or even in the components of the road infrastructure (think: traffic lights, toll booths, license plate recognizance software, road-side cameras etc.). Compromising either one of these components, road-side or vehicle-side can cause a tremendous chain of events, affecting large number of the population.

Scaling this to 'smart cities', where the foreseeable trend is towards moving the control components of the infrastructure from human operators to automated, sensor input-based, machine learning modeled operational mode, the surface of attack becomes wide and diverse.

Industry leaders and regulatory bodies are pushing towards unified frameworks and best-practices guides for automotive and transportation cybersecurity, such as SAE International's, NIST's 800-series publications or Auto-ISAC's forum for cybersecurity professionals.

As a key take away, cybersecurity in the automotive and transportation business is a fairly new interest with most companies being active in this space for merely 3 or 4 years. Until reaching a level of maturity that allows the validation of the autonomous, connected vehicle use-case from a security stand point, most of these industry players will have to catch up with this ever-growing and complex domain.

Highlights: Feeding the fake news machine – bots, automation and A.I.

Social Media is probably the most important phenomenon to drastically change the ways in which we communicate, disseminate information and read news. The past decade saw a 3 fold increase in total number of social media platforms users with up to 2.77 billion registered in 2019.

Social media has become a great medium for sharing user generated content moving past its publishing capabilities. This largely impacted journalism and traditional media as content in the form of user-reported news began to inundate walls and stories. This happened across-platforms, with media enrichment becoming the norm, in the form of videos, photos, live streaming of events, audio recordings or document sharing. Most platforms were not designed with source validation in mind and this paved the way for the global phenomenon we're now referring to as Fake News.

While traditional media has checks in place in order to validate and factually check the reported information, social media allows any of its users to post, share, comment and disclose their content as a relatable information which has the potential to reach millions in minutes or hours. This could be considered a vulnerability from both a technical and a societal point of view. We're used to rely on code validation and input validation in cyber security as a countermeasure to bugs and cyberattacks. Unfortunately, social media platforms cannot provide the same countermeasures to false information spreading. With every vulnerability there's usually a plethora of exploits a malicious actor could use and this is true for social platforms as well. In this case, it's fake news. But given the sheer number of users on these platform, a complexity issue arises for even the most skilled of attackers: how to you target a specific group of people with your false information? How do you share it across language barriers? What about political preferences and personal believes? Can you factor those in the creation process of your news?

Given these challenges are impacted by a factor of scale, malicious actors have become more and more interested in using automated tools that could actually learn and predict user behavior and consequentially write and disseminate news in such ways as to maximize the reach and impact. A practical solution to these challenges are programmable bot nets and Machine Learning algorithms. Let's look into each of these two technologies and describe their impact on spreading false news:

A bot, in it's simple form is a piece of software that can be explicitly programmed to perform an action. Bots are used for automation of repetitive tasks and when controlled en-masse they become a Network of Bots or –in short – a Bot Net. There are several ways one could program a bot to perform a specific action but in terms of malware, the most common route is to infect internet connected devices and computers with malware that allows the attacker to command these devices to act as multiple attackers, performing their malicious role or –in the case of false news spreading – to act as 'ghost' users of social networks and publish, share and comment on fake news posts. The automation part is useful for quickly creating fake user accounts on various platform, emulate some form of reputation by adapting the 'ghosts' behavior to mimic that of a human user – i.e: join various

discussion groups, select interests and preferences, interact with generic content, create and upload media – photos, videos etc.

A bot net is, thus, useful when it comes to creating armies of fake user accounts that act as closely as real users as possible. Machine Learning and various other forms or methods of A.I. are useful for adapting the behavior of these fake users, learning behavior models and language intricacies generating content that appears as 'human' as possible. Technologies such as Natural Language Processing, Text Mining and Sentiment Analysis play a huge role in this.

As complex as this reads it is actually a pretty straight forward process that leverages some of the technologies developed for automation of various tasks such as headless web browsers that can be implicitly programmed to perform various user actions in web sites and monitor the output or automation tools such as Puppeteer, allowing centralized deployment and control of multiple such instances or – in our case, bots.

These technologies are within reach of most malicious actors, the majority of these are open source and can be used free of charge. All that's needed to complete the job of spreading fake news is a warm and cozy place that lies within the borders of a nation with a relaxed legislation regarding the spreading of misinformation. Having secured all the requirements on this checklist – devices with bots running atop of them, automation platforms and a place to do it without looking over one's shoulder – an attacker could drive such fake news campaigns for as long as they wish so.

Studies of impact performed on such networks show that they are efficient to the point of actually altering the expected results of electoral votes or in such ways as to severely alter the public perception on a given fact or person. These networks are in fact one of the most important challenges for the security of the cyber space and major technology players are lining up their efforts in preventing the rapid spread of disinformation over social media. Such actions include the active 'hunting' of ghost accounts by using A.I., or improvement in national, Federal and European legislation in this aspect.

Using Artificial Intelligence in Cyber-Attacks

Artificial intelligence may be used by cybercriminals to analyze large amounts of data from various sources across the Internet, to identify vulnerabilities of systems and users, and to improve and intensify cyber-attacks.

Traditional cyber-attacks involve an attacker's presence and interaction with specific computer systems to make certain decisions, which often limit his anonymity. Artificial intelligence will further obfuscate the connection and increase the distance between victim and attacker. The emergence of autonomous cyber-attacks, capable of taking the best decisions alone based on the existing ecosystem, will make it difficult to investigate and assign them.

Social engineering

Social engineering remains one of the main vectors of attack. Frequently, malware is introduced into the computer system by its users, by downloading infected files or by clicking on malicious links in emails. But making these emails interesting for users requires a lot of effort and documentation on the part of cybercriminals. Using artificial intelligence in this area will greatly simplify their work. Analyzing vast amounts of data on the Internet and Darknet, artificial intelligence will be able to accurately build a social profile of potential victims, based on their behavior in cyberspace. Once the victims have been selected, attractive emails and websites are created for all targeted users. Moreover, artificial intelligence can gain users' confidence through sustained dialogue across various social platforms, without the involvement of human attackers. There are already different forms of chatbots - programs that automatically initiate dialogue and generate responses on the Internet and who manage to have good conversations with the users by simulating the writing style of real people. In the future, these discussions will not be limited to text, but will also have a voice component, given the rapid development of voice synthesis applications. Artificial intelligence can simulate the voice of a person with a high degree of accuracy, based on recordings posted by that person on social media.

Malware applications

Malware variants are continually evolving, being equipped with various modules for multiplying, infecting, blocking and retrieving data from compromised systems. Once these types of malware are made by artificial intelligence, they will be able to propagate on a much wider scale and exploit any encountered vulnerabilities. Thus, command and control servers used by cybercriminals will no longer be needed, with artificial intelligence being able to make decisions based on encountered vulnerabilities and the desired purpose.

Once inside computer networks, the smart forms of malware will go into stand-by mode, intercept communications between systems and the running trusted applications, and then attempt to mimic the behavior of network users in order to mislead cybersecurity solutions. Artificial intelligence will be perfectly tailored for the target environment, knowing where critical data is, what vulnerabilities exist in the system, the right time to attack, and how to accomplish the cyber-attack.

It is likely that in the future, intelligent ransomware applications used for encrypting data on compromised systems will be able to study the victim's profile with the aim of determining the amount of money the victim is willing to pay cybercriminals for unblocking access to their data, maximizing the chances and profit of any attacker.

Conf.dr.ing. Ioan-Cosmin MIHAI
Department director
”Al. I. Cuza” Police Academy

What's next? Predictions for 2020

Attacks on shadow resources: As we're moving into an era where we deeply embrace the Bring Your Own Devices philosophy and with the advent of connected 'smart' devices – wearables, sensors, monitors, anything with an 'IoT' ring to it, we can expect that a significant volume of cyber attacks will target these 'shadow resources' – computing devices and resources that are virtually unknown to the network and security administrators.

Cyber Security practices are closely linked to assets and having a persistent inventory of devices, technologies, software and hardware allows CISOs and ISMs optimum visibility on their network's footprint and security perimeters.

Moving away from this principle, BYOD-enabled business are expanding the attack surface of their networks on a daily basis with threats spreading across logical and physical boundaries.

We're expecting this threat to grow in the foreseeable future with more businesses being victims of attacks vectoring-in their employees personal devices.

5G deployment will expand attack surface
With 2019 being the year for initial deployment of some 5G networks world-wide, it is believed that 2020 will accelerate 5G activity.

It will take some time for 5G networks and 5G devices to become broadly available but the growth will be rapid as it will accelerate towards the end of 2020.

2022

by 2022 the 5G network infrastructure will have a 'price tag' of nearly 25$BN worldwide

Give the 5G advantages and generational deltas from 4G such as data rates of up to 10Gbps and extremely low latency it is expected that 5G will be the catalyst for new operational models, new architectures and – of course – new vulnerabilities and related threats.

As more 5G IoT devices will connect to the Internet, with multiple vendors and technological suppliers entering the market, the attack surface available to malicious actors will increase exponentially – possible – beyond reasonable control.

One particular offense that we predict it will happen in the upcoming years is the use of 5G IoT devices to orchestrate large-bandwidth attacks like DDoSes.

Statistics:

The BYOD Market will value almost 400$ BN by 2022

61%

of all workers believe the tech they own is more effective and more productive than the technologies offered by their employers

Companies favoring BYOD make a per annum saving of 350$ per employee

What's next? Predictions for 2020

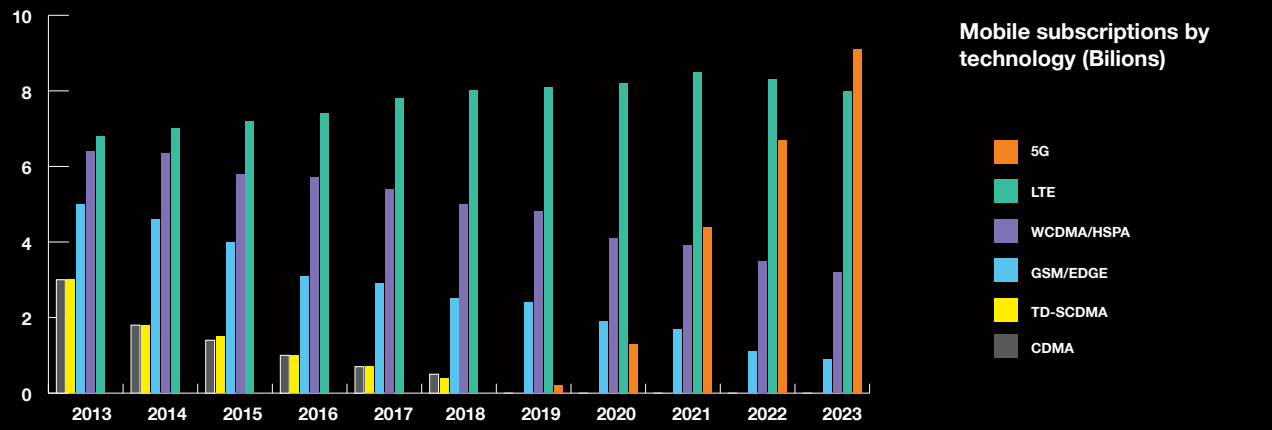
A.I. will be at the forefront of cyber threats, on both sides: We've seen forms of A.I. being used to orchestrate attacks back in 2017 with the advent of the first Swarm Botnets – large zombies that had the ability to orchestrate attacks by communicating to each other, like in a hive, over encrypted channels. No C2C server was needed and most detection mechanisms proved to be inefficient in detecting such unknown threat. 2020 will likely see this form of A.I. being used to drive attacks, to generate new strains of malware or even to obfuscate existing strains from detection technologies by masquerading the malware into a form that resembles legitimate code or communications.

One particular interest of attackers investing in A.I. capabilities is the possibility of driving an exponential growth of opportunistic attacks volumes and success rates. By leveraging the massive processing power of current generation hardware and by using various implementations of A.I., an malicious actor cu increase thousand-fold the number of exploited victim devices. This –in theory- could lead to very large scale botnets that have the ability to provoke great damage to services and infrastructure alike.

A swarm-bot or a network of compromised machines that can talk to each-other using encrypted, secure channels and have the ability to move laterally without explicit programming can spread to hundreds of millions of vulnerable devices and end-points. Such a massive army could be used for spreading misinformation, altering existing information, creation of ghost accounts used for anything from spamming e-mail to voting in online pools.

It will become increasingly difficult to prevent and stop these kind of threats but we'll likely see A.I. used by 'the good guys and girls' as well, with advanced learning models and machines used to detect and even predict vulnerabilities appearing in software and hardware or by simulating attacks in order to test existing infrastructure.

IoT-Based Attacks will diversify: Massive IoT-based botnets are used in principal for large-scale DDoS attacks. This will continue to be the major threat for 2019 and 2020 but attackers will increasingly move to using poorly secured IoT devices as a means to a physical effect. Some IoT devices are kinetic in a way that they either use actuators for completing some form of physical activity or they command moving parts (think connected vehicles) in order to improve human physical response. The next few years will probably have us witness this next generation of large-scale attacks with malicious actors trying to compromise physical devices controlled by IoT logic. The advent of 5G will be a key factor in the widespread adaptation of these technologies.



Best practices guide for a cyber-secured business environment

Powered by BITSENTINEL

Cybersecurity is an area of increasing priority for decision-makers in all business sectors. Why? Because all businesses rely on a network infrastructure and they are connected to the internet and a breach can escalate to a disaster from which a company cannot recover easily.

The good news is that cyber security grows exponentially with the measures a company introduces, meaning that with a relatively small effort you can reduce the attack surface even by 90%. We compiled a list of certain steps that greatly reduces the risk while keeping your effort to a minimum:

Perform a risk assessment in order to identify key assets and resources so you can prioritize your effort smarter and more efficient

Perform network segmentation, allow only required personnel to have access on sensitive areas from your network

Always update your applications, operating systems and services to the latest version available

Perform vulnerability scanning against internal & external environment quarterly; you can always use free open source tools such as OpenVAS, Vulners or ask help from certified independent contractor

Undertake penetration testing at any major change of the system or at least once a year

Introduce an Intrusion Detection System (IDS) or Intrusion Protection System (IPS) that can help you identify attacks inside or against your network when they happen, this also will enable you some logging capabilities in order to trace back an incident

Perform security awareness training for your team to help them become more resilient to ransomware, malware attacks but also to differentiate a malicious/fake email from one which is benign

Develop a Responsible Disclosure Program to encourage security research community to report vulnerabilities they've discovered

Perform an Incident Response plan, have Disaster Recovery & Data breach response plans in place

Glossary of terms

Term	Description
Cyber Security	Cybersecurity, computer security or IT security is the protection of computer systems from the theft and damage to 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 (Oxford Dictionary)
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.
Fileless (attack)	Zero-Footprint Attacks or fileless attacks are types of attack that don’t install new software on a user’s computer so anti-virus solutions are more likely to miss them
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.

Mirai (Botnet)	Mirai is a malware that turns networked devices running Linux into remotely controlled "bots" that can be used as part of a botnet in large-scale network attacks. Most of the affected devices are routers, IP cameras and connected 'smart' devices.
Coinhive	Coinhive is a cryptocurrency mining service that relies on a small chunk of computer code designed to be installed on Web sites. The code uses some or all of the computing power of any browser that visits the site in question, enlisting the machine in a bid to mine bits of the Monero cryptocurrency
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.
Monero	Monero (XMR) is an open-source cryptocurrency created in April 2014 that focuses on privacy and decentralization
(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.
Code Injection (attack)	Code injection is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution
Process Hollowing	Process hollowing occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to Process Injection, execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis.
Living of the Land (attack)	In the cyber security world, living off the land attacks describe those attacks that make use of tools already installed on targeted computers or attacks that run simple scripts and shellcode directly in memory, without the need to download additional software.
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
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
Andreea Grigorescu, Brand Specialist
Alexandra Pascali, PR Specialist
Monica Obogeanu, Startup Programs Manager
Cristian Paţachia, Development & Innovation Manager

Acknowledgements

We extend a big thank you to our partners who have supported our efforts:
Andrei Avădănei, President of Computer Security Research Center in Romania
Corporate and public partners: Bit Sentinel, Fortinet Romania, CERT-RO


Projects supported by the European Commission
Horizon 2020
SliceNet
GA no.: 761913
SLICENET
slicenet.eu
@SliceNet_5G
Matilda
GA no.: 761898
MATILDA
matilda-5g.eu
@matilda5g
5G EVE
GA no.: 815074
5G EVE
5g-eve.eu
@5G_EVE
5G Victori
GA no.: 857201
5G-VICTORI
5g-ppp.eu/5g-victori
#5G-VICTORI
Unicore
GA no.: 825377
UNICORE
unicore-project.eu
@unicore_project
Resisto
GA no.: 786409
RESISTO
resistoproject.eu
@RESISTO_project
NEXES
GA no.: 653337
nexes.eu
/NG112.EU/
Orange Romania is involved in all these Horizon 2020 projects along with its parteners from more than 15 European countries.
If you want more details on these projects or you want to create a partnership for other research projects, please write an e-mail to cristian.patachia@orange.com

orange™

Fab Romania

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