Eleven Paths

Cybersecurity Trends for 2020

This report aims to focus on the potential threats that could arise in the 2020 digital environment by offering a picture of a possible future driven by the evolution of threats and technological progress

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Contents

Executive Summary

This report aims to focus on the potential threats that could arise in the 2020 digital environment by offering a picture of a possible future driven by the evolution of threats and technological progress.

The future might seem complex, overexposed and poorly-configured, but if there is anticipation, it may be defended.

1. Introduction

The year 2020 will witness of the **transition to a new decade**, and so will do **cybersecurity**. Companies have a wide variety of applications, services and platforms that **will require protection against potential attacks**. We will see known attacks, such as **extortion, obfuscation and phishing.** However, **new risks will arise**.

It should be noted that cybercriminals will not be discouraged by the possibility of compromising systems, they will change and align their choice with tactics and attack vectors, making it completely necessary for **users and companies to try to anticipate, and above all, to be well-protected.**

It is quite possible that attackers overcome incomplete patches and, as a result, **system administrators should ensure both punctuality and quality of the patches.**

Karspersky[1] researchers also point out that targeted attacks will undergo changes during 2020. The trend would show that threats will grow in sophistication and will be more selective, diversifying under the influence of external factors, such as the development of technologies, e.g. Machine Learning for the development of Deep fakes.

1.1. Scope

The scope of this document is the collection of information based on different security firms and providers such as Check Point, Trend Micro, CyberArk, Shophos Lab and Kaspersky, among others, as well as on security experts, who will perform an analysis of future case scenarios related to potential attacks on infrastructure, clients and users that may occur in 2020.

[1] https://www.computing.es/seguridad/noticias/1115428002501/2020-amenazas-creceran-sofisticacion-y-seran-mas-selectivas.1.html

1.2. Objectives

This document is aimed at focusing on the potential threats that the world of cybersecurity would face in 2020.

The threats of the digital world are constantly evolving, and consequently it is essential to adapt to the potential attack scenarios, since currently digital transformation is already a reality.

Threats evolve, and consequently the security environment must progress and even try to anticipate such attacks by securing people, companies and information systems they depend on.

2. Prospect of Trends for 2020

2.1. Ransomware Attacks

The threat landscape continues to evolve, and the speed and scope of such evolution is as accelerated as unpredictable.

2019 has been defined by numerous ransomware attacks that have impacted even on the activity of those companies that were attack targets.

According to **SophosLabs**, ransomware attackers will continue performing active and automated attacks that will put the management tools of organizations against them, avoiding security controls and disabling backups in order to cause maximum impact within the shortest possible time.

The ransomware **will point to the cloud**, according to **WatchGuard Threat Lab**[2]. It is forecast that ransomware attacks will point to the cloud, including file stores, S3 buckets (storage services through a web service interface) and digital environments.

Check Point[3] forecasts the increase in **targeted ransomware attacks** focused on businesses, local governments and specific healthcare organizations. The attackers will devote time to preparing the attack, gathering information about their victims to be sure they can inflict as much damage as possible, so the number of hijackings would increase. In addition, Check Point points out that companies may need to evaluate options to protect themselves and, as a consequence, organizations that contract insurance policies against ransomware may increase, which will result in **demands for ransoms by attackers.**

CyberArk3[4] emphasizes the butterfly effect of ransomware, as it will continue to increase next year. The objective of these attacks would be focused on the disruption and destabilization of the systems, so cities should **focus on cyber resistance.**

[2] https://cuadernosdeseguridad.com/2019/12/watchguard-prediciones-2020

[3] https://cuadernosdeseguridad.com/2019/12/tendencias-2020-ciberseguridad-check-point/

[4] https://www.interempresas.net/Ciberseguridad/Articulos/259701-CyberArk-desvela-las-principales-tendencias-en-ciberseguridad-para-2020.html

Kaspersky defines the evolution of **ransomware,** to **selective ransomware**. Cybercriminals would have become more selective and consequently the generalized multipurpose attack has decreased.

Now, they would focus on aggressive attempts at extortion payments for money. A potential twist could be that, instead of making the files unrecoverable, the actors threaten to make the stolen data public.

2.2.Cloud Computing

Cloud computing environments will be an ideal target for cyberattackers.

Code **injection attacks**, either directly to the code or through a third-party library, will be used prominently against **cloud platforms**. These attacks (**from cross-site scripting and SQL injection**) will be carried out to **spy, take control and even modify sensitive files and data stored in the cloud.**

The attackers will alternately inject **malicious code** into third-party libraries that users will download and execute without realizing it.

In addition, vulnerabilities in the components of the containers[5] will be the main security concerns for DevOps teams (DevOps corresponds to a software engineering practice that aims to join software development and software operation).

Serverless platforms offer "to work as a service", allowing **developers to execute codes without the organization having to pay for full servers or containers.** Obsolete libraries, poor configurations and known and unknown vulnerabilities will be entry points of attackers to serverless applications.

Code injection attacks to cloud platforms **will be performed through third-party libraries.** Therefore, it will be a priority to have security in the cloud environments in **Azure, AWS and Google Cloud Platform.**

For that purpose, the security expert Kevin Beaver[6] recommends using technologies such as network firewalls, Active Directory and end-point logging and warning capabilities.

[5] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2020

[6] https://searchdatacenter.techtarget.com/es/cronica/Principales-tendencias-amenazas-y-estrategias-de-seguridad-de-red-para-2020

2.3.Machine Learning

Machine Learning is designed to remove malware under attack. From 2019 it may be highlighted the potential of those attacks against machine learning security systems.

According to Shophos lab, Machine Learning could have a negative connotation, since ML detection models could be deceived and, consequently, machine learning may be applied to offensive activity to generate false content, which would be convincing for social engineering.

According to **Ponemon Institute**, experts in Artificial Intelligence anticipate that Artificial Intelligence and Machine Learning will lead to continuous improvements in the management of company assets and IT security. In particular, thanks to the development of **endpoint** resilience, among other things.

In addition, tools will keep improving thanks to different data sets, which will result in a broader picture of global threats.

In addition, it should be noted that it could be an increase in the **exploitation of personal information** with **Artificial Intelligence**. This technology is already being used today, so it would be only a matter of time before **some attackers may take advantage of it**.

Therefore, Machine Learning (ML) and Artificial Intelligence (AI) may be exploited to listen on connected devices such as televisions and smart speakers to get into personal and business conversations, **and this in turn could provide material for extortion or corporate espionage.**

2.4.Phishing Attacks

Check Point places phishing as a threat that will leave its mark on the 2020 threat landscape, alongside ransomware.

Phishing attacks will go beyond email. While email remains the most used attack vector, cybercriminals increasingly employ a greater variety of formulas to deceive potential victims with the aim of obtaining personal information, credentials, or money transfers. Thus, it is expected that phishing attacks will be used **against mobile phones through SMS messages, as well as through social networks and gaming platforms.**

2.5.Open Banking and Mobile Malware

This type of attack is intended to steal **payment data, credentials and money from victims' accounts**, so that anyone willing to pay malware developers could extensively distribute malware. Moreover, phishing attacks are expected to be more sophisticated and effective, attracting mobile users to click on malicious web links.

In relation to malware, it should be noted the existence of targeted attacks against Open Banking. **Banking systems will be more vulnerable as online mobile payments thrive.**

Mobile malware targeting online banking and payment systems will be more active, since online mobile payments in Europe thrive thanks to the revised Payment Services Directive (PSD2) of the European Union (EU).

From this directive, faults may result from the Application Programming Interfaces (APIs), and even new phishing schemes.

Therefore, banking systems will be targeted by Open Banking and ATM malware. It is expected that the unauthorized sale of malicious programs for ATMs will continue to gain ground.

Following this, **espionage and extortion** will increase, and Machine Learning and Artificial Intelligence will be used **in order to spy on personal and business conversations.**

2.6.5G

The 2020 technological revolution will be accompanied by the **implementation of the fifth generation of wireless communication technologies and standards.**

According to the European Commission, this innovation will offer a faster Internet connection speed from all mobile devices. For this reason, it may become an attack target and **be used by hacktivists, criminal groups with financial interests or even by countries with the aim of attacking other nations.** Among the main targets there could be essential service systems such as electricity supply, but also the financial system itself.

These alleged attacks that could be derived from hacktivists are related to the concept of potential '**cold cyberwar**'[7] forecast by Check Point.

As society depends on continuous and uninterrupted connectivity, criminals and creators of threats to states and nations are more likely to influence the results of political events, cause disruptions, and even massive damage that may threaten thousands of lives.

It is worth mentioning, for example, the confrontation between the United States and China, where the former has created a blacklist of Chinese products considered to be dangerous for the country. This has happened with Huawei, that cannot use US technology products for their products.

From Check Point, they point out that there will be an upward trend of cyberattacks against **critical infrastructure and public services.**

3. Conclusions

The world of threats is continuously evolving. Therefore, the world of cybersecurity should try to anticipate and set a continuous improvement plan of its solutions.

How? By performing an active search for threats, adopting a comprehensive and holistic approach to proactively monitor and identify suspicious or potentially-malicious activities and, thus, take measures, minimize or avoid (when possible) the impact of the damage.

[7] https://www.europapress.es/portaltic/ciberseguridad/noticia-check-point-alerta-llegada-ciberguerra-fria-2020-20191028143414.html

Critical infrastructures will be affected by more attacks and production disruptions, as well as companies; ransomware being the favorite weapon.

In general, the forward-looking perspective of attacks suggests that they will focus on increasing ransomware activity and rising stealth in malicious applications by taking advantage of improper cloud settings, and even fooling Machine Learning.

Therefore, it is essential to prioritize **anticipation**, as it will always be the best defense against potential attacks. In 2020, threats will grow in **sophistication and be more selective**. Consequently, threat **prevention** must be a priority so we must focus on monitoring, detection and response and, of course, end-to-end security of all security layers.

It is no longer enough to defend ourselves just with traditional security models based solely on detection. When the threat is detected, often damage is already done, so there is a need to automatically block advanced attacks with the aim of preventing them from affecting the systems. We should combine **threat prevention in real time, shared intelligence and advanced protections in all networks, clouds and implementations.**

About ElevenPaths

At ElevenPaths, Telefónica Cybersecurity Unit, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

We combine the freshness and energy of a start-up with the power, experience and robustness of Telefónica to provide solutions that enable prevention, detection and response against everyday threats in our digital world.

We build strategic alliances to provide a strengthened security to our clients. Moreover, we work jointly with organizations and entities such as the European Commission, Cyber Threat Alliance, ECSO, EuroPol, Incibe, and the Organization of American States (OAS).

More information

elevenpaths.com

@ElevenPaths

blog.elevenpaths.com