# “Ciberseguridad Global”

Fuente: INISIEG Ciberseguridad Global 2020.

**A nivel Mundial los piratas informáticos con bandera política parecen estar menos activos en los últimos 3 años a la fecha aunque los 10 años anteriores se sumaron pérdidas catastróficas por Miles de Millones de Dólares debido a estas malas prácticas. Al menos así parece sugerirlo un informe reciente de la sección de Inteligencia de la Agencia de Ciberseguridad de la Unión Europea** (Reporte Anual de Ciberseguridad C. Singleton 2019).

**En resumen algunos de los hallazgos más notables de la corta pero muy destructiva historia del Ciberterrorismo desde el nacimiento de internet** y un poco antes da señales de innovaciones y desarrollo de nueva tecnología aplicada cada día que pasa en este sector **que si bien es algunas veces clandestino hay otras ocasiones que ha sido intencionado por equipos completos de expertos en cibernética, programación e informática que pertenecen a compañías elite de desarrollo de Hardware y Software** cercanas a los países y de zonas más adineradas en el mundo en **países que pueden financiar estas tecnologías de daño masivas como la suscitada en el Hackeo de la NASA y el Sistema de Defensa del Gobierno de USA en 1999. La Compañía Sony en 2014, el sistema Eléctrico de Ucrania en 2015 y la campaña presidencial en USA en 2016 alegando graves fallas de seguridad como es el caso de algunos semiconductores fabricados por compañías como Intel y AMD. Apodados Meltdown y Spectre.** Otro de tantos ejemplos en el recuento de los daños es el Malware Destructivo “**WannaCry” en 2017** que dio a conocer el ***ransomware*** y

el "*malware" de daño masivo.* ***"El ransomware, se trata de una variante de malware, el cual tiene como objetivo entrar a un sistema, a través de una vulnerabilidad y realizar actividades que pueden ser de espionaje, robo de información, uso de recursos del equipo host, o simplemente el monitoreo de la actividad del usuario, existen variantes que inclusive afectan archivos de procesos industriales (SCADA).*** *Lo critico en este caso es que está enfocado a realizar un secuestro de la información y/o equipos de cómputo en los cuales se instala, pudiendo diseminarse de manera automática a otros equipos de la misma institución"…* **En este caso en general tuvo la capacidad de inutilizar 200,000 Equipos de cómputo por día atribuido al gobierno de Corea del Norte mismo que no fue comprobado,** o el ataque del Ransomware conocido como "**ExPetr** o **NotPetya" que ha sido por mucho el más costoso de la historia moderna (10,000 MDD por afectaciones en más de 15 países) y "Stuxnet"** que inutilizó las centrifugadoras de enriquecimiento de uranio en Irán relacionado también al ciberataque de la empresa **Equifax (Visor Mundial de Riesgo), La Aseguradora Británica Aviva Así como la fábrica de Tesla (Automóviles Eléctricos) por mencionar algunos ejemplos representativos.**

En países de diversos continentes se han sufrido a causa de esta mala práctica tanto robos como destrucción masivos de información sensible de usuarios y afectación hasta la inutilización de Hardware, Equipos de Cómputo, Electrónicos y de Seguridad en los sectores bancario y de salud principalmente**, Facebook y la Ciudad de Atlanta en Estadios Unidos de Norteamérica , con la cadena de Hoteles Marriott con el Spyware "Dark Hotel" que descubrió en sus sistemas hasta cuatro años después y ejemplos como los BOTNETS que dieron forma a un *malware* conocido como "Mirai" ("futuro", en japonés), que crecía y crecía a la espera de instrucciones y un día genero un ataque masivo llamado DDoS** que colapso los servidores de tiendas en línea y servicios de Streaming **o "Video en Línea" alrededor del Mundo son de los ataques más publicitados de 2018 igual que las Seis de las principales plataformas de Criptomonedas con Malware Destructivo como "Coinhive y Crypto Miner" hasta el** Malware Destructivo "**ZeroCleare"** desarrollado y neutralizado en su mayor parte en **2019** a varias compañías proveedores del gobierno Alemán y en el **ataque al Parlamento (Bundestag Alemán) Ciberataques que han cambiado la visión del mundo respecto** a las plataformas sociales, los gobiernos y las criptomonedas y el peligro latente de que la información privada de sus usuarios sea vendida y utilizada para fines de Ciberterrorismo como robo de identidad (Pishing), falsificación de documentos, transferencias ilícitas de fondos entre otros.

Además "EL **Ciberespionaje se ha convertido en una excusa para un negocio muy rentable de los vendedores de tecnología a nivel Mundial y eventualmente también para quienes se dedican a comprarla y usarla en contra de sus enemigos o enemigos de alquien más quien pueda pagarles sus servicios** atestiguando uno de los eventos más evidentes respecto a los escándalos en la

Casa Blanca en U.S.A., en el cual estuvo involucrado el presidente Trump y las suposiciones de sus opositores que redactaron mediante la prensa escrita y por varios medios de información como pudo el gobierno Ruso Intervenir la campaña que sucedió en contra de Hillary Clinton en su momento directamente y después haciendo uso indebido de información de millones de usuarios de la compañía “**Cambridge Analytica”** quien argumento ser víctima de un Ciberataque masivo **en 2018 durante y al final de la campaña que asesoró al ahora Presidente Trump.**

**ESPAÑA (apro).- Los mejores 'Hackers' de España pasan de alistarse en el ciberejército de Rajoy**

**El Gobierno del Partido Popular de España ultima el borrador de una proposición de ley para crear un organismo que nunca se había puesto en marcha en nuestro país: una ciberreserva con miles de ‘hackers’ y expertos en seguridad informática listos para hacer frente a nuevos ciberataques globales.** El documento fue confirmado por el propio gobierno Español, pero **El problema: los mejores ‘hackers’ de España, que deberían ser parte clave de este nuevo cuerpo de seguridad, aseguran no tener el más mínimo interés de unirse al ‘ciberejército’ de Rajoy.** Califican la iniciativa de **“equivocada” y de “pura propaganda”.** El proyecto corre el serio riesgo de nacer muerto desde el inicio debido a que es bien sabido que existen gobiernos que han reclutado Desarrolladores y Expertos en esta área de Cibernética y Ciberseguridad y han sido presos y algunos desaparecidos y denunciados ante las instancias Internacionales la referencia más rápida es **el Australiano Julianne Assange Co-Creador y Co-fundador de WikiLeaks movimiento que sucumbió ante la persecusión y reciente arresto al finalizar su “Asilo Político” en la embajada de Ecuador de Londres Reino Unido y que durante este periodo vio nacer a “Anonymous”.**

**“Las últimas campañas de Anonymous han sido primar la propaganda en redes sociales para luego lanzar ciberataques con mínimo impacto.**

**En Latinoamérica se vive la misma "inactividad" y "declive general"**, dice el informe. Anonymous Venezuela y Anonymous Brasil

**CIUDAD DE MÉXICO (apro).- México activó en siete ocasiones el protocolo de seguridad por ciberataques entre septiembre del 2016 y julio de este 2017, reportó el gobierno del Ex Presidente de México Enrique Peña Nieto en su Quinto Informe de Gobierno.**

**“El Centro Nacional de Respuesta a Incidentes Cibernéticos (Cert-Mx) de la Policía Federal activó el protocolo de coordinación siete veces**, con el objetivo de dar seguimiento a las operaciones relacionadas con la ciberseguridad durante diversos eventos importantes”, señala el documento entregado por la Presidencia de la República a la Cámara de Diputados y Senadores de México.

Sin precisar las ocasiones en que se activó el protocolo, el Informe muestra en el capítulo de Seguridad Nacional que los ciberataques están cada vez más presentes en la agenda de las agencias de seguridad, tanto civiles como militares según lo reportado también en los siguientes informes **del Nuevo Presidente de México Andrés Manuel López Obrador 2017-2018 en donde el mensaje de la Procuraduría General de la República, Centro de Investigación y Seguridad Nacional (Cisen), Ejército y Marina tienen un intercambio internacional para enfrentar esta nueva amenaza a la seguridad nacional** y que en el país han dado ejemplos claros del daño político y Económico de estas malas prácticas contra empresas Gubernamentales como **el Ciberataque a BANCOMEXT en Enero de 2018 Evitando el Gobierno un Robo de 110 Millones de Pesos evitando una transferencia internacional por SWIFT al banco Standard Chartered en USA sumados a 5 Hackeos al Sistema Financiero de México menos graves y el Reciente Ciberataque a PEMEX en Septiembre de 2019 que coincidió con las fechas de investigación y la posterior aprehensión el 12 de Febrero 2020** en España de Emilio Lozoya Austin Egresado de Harvard por un caso de Corrupción y Vínculos con Actividades ilícitas.

El documento también asegura que el gobierno mexicano realizó adecuaciones normativas para **“Ejecutar en territorio nacional”** las resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas (ONU) para el mantenimiento de la paz y la seguridad internacionales en el tema de Ciberseguridad y Ciberataques.

**En una nota titulada “El declive del hacktivismo:** Los ciberataques de esta naturaleza Política-Económica cayeron 95% desde 2015 a la fecha a nivel global”, pero hay una salvedad en aquellos países en donde continúan al día de hoy lo que parece ser una herramienta sistemática de **“Hacktivismo”** con fines políticos todavía en 2020 y nos hace la pregunta de lo que esta pasando en este momento respecto a la **pandemia de COVID-2019 y que hay detrás de la guerra de acusaciones de Manufactura del Virus y Bioterrorismo** entre los países más desarrollados que actualmente puso en duda la actuación de la **Organización Mundial de la Salud (OMS) "El hecho de que los casos de más repercusión mediática pongan el foco en EEUU no debe llevarnos a pensar que solo desde allí se proyectan y ejecutan operaciones de espionaje masivo o monitorización selectiva de políticos o diplomáticos, amigos o enemigos" si no también en países como Rusia China y Emiratos Árabes Unidos además de muchos otros países en América Central y América Latina”.**

Gustavo Ernesto Rodríguez De Lira
Fundador IT Capital

Referencias Periodísticas y de Investigación (Research References & Journal)-
https://www.elconfidencial.com/tecnologia/2017-05-03/ciberguerra-espana-ciberataques-espionaje-hackers_1374693/

# “Global Cibersecurity”

Fuente: INISIEG Ciberseguridad Global 2020.

**Globally, political flagged hackers appear to be less active in the past 3 years to date, although catastrophic losses of Billions of Dollars have been added in the past 10 years due to these bad practices. At least, this seems to be suggested by a recent report by the Intelligence section of the European Union Cybersecurity Agency** (Annual Report on Cybersecurity C. Singleton 2019).

**In summary, some of the most notable findings of the short but very destructive history of Cyberterrorism since the birth of the Internet** and a little earlier gives signs of the new development and new technology applied every day on this sector that, **sometimes clandestine but there other occasions by entire professional teams of cyber, programming and computer experts belonging to elite Hardware and Software development companies** close to countries and wealthier areas in the world that can finance these massive damage technologies like that raised in the **Hacking of NASA and the Defense System of the US Government in 1999. The Sony Company in 2014, the Electricity system of Ukraine in 2015 and the presidential campaign in the USA in 2016 alleging serious security flaws as is the case of some semiconductors made by companies like Intel and AMD. Nicknamed Meltdown and Specter**. Another one of many examples in the damage count is the Destructive Malware “**WannaCry**” **in 2017** that unveiled ransomware and massive damage “malware”. ***"Ransomware, is a variant of malware, which aims to enter a system, through a vulnerability and perform activities that may be espionage, information theft, use of resources***

***on the host computer, or simply the monitoring user activity, there are variants that even affect industrial process files (SCADA). What I criticize in this case is that it is focused on seizing the information and / or computer equipment in which it is installed, and can automatically spread to other teams from the same institution "***… In this case, in general, it had the capacity of disabling 200,000 computer equipment per day attributed to the North Korean government itself that was not verified, or the attack of the Ransomware known as "**ExPetr or NotPetya" that has been by far the most expensive in modern history (10,000 MDD for damages in more from 15 countries) and "Stuxnet**" that disabled the uranium enrichment centrifuges in Iran also related to the cyberattack by the company **Equifax (World Risk Viewer), The British Insurer Aviva As well as the Tesla factory (Electric Cars) to mention some representative examples .**

In countries of different continents, thefts and massive destruction of sensitive user information have been suffered as a result of this bad practice, and even the use of Hardware, Computer Equipment, Electronics and Security in the banking and health sectors, **Facebook has been used. and the City of Atlanta in United States of America, with the Marriott Hotel chain with the "Dark Hotel" Spyware that it discovered in their systems up to four years later and examples such as BOTNETS that shaped a malware known as "Mirai" ("future ", In Japanese), which grew and grew while waiting for instructions and one day generated a massive attack called DDoS** that collapsed the servers of online stores and Streaming or **"Online Video" services around the world are the most common attacks Advertised in 2018 as well as the Six of the main Cryptocurrency platforms with Destructive Malware like "Coinhive and Crypto Miner" up to Destructive Malware "ZeroCleare**" Developed and largely neutralized in 2019 to several German government provider companies and in the attack **on the Parliament (German Bundestag) Cyber attacks that have changed the world view** regarding social platforms, governments and cryptocurrencies and the latent danger of that the private information of its users is sold and used for cyber-terrorism purposes such as identity theft (Pishing), falsification of documents, illegal funds transfers, among others.

Furthermore, **"Cyber espionage has become an excuse for a very profitable business for technology vendors worldwide and eventually also for those who are dedicated to buying and using it against their enemies or enemies of someone else who can pay for their services"** Witnessing one of the most evident events regarding the scandals at the White House in the USA, in which President Trump was involved and the assumptions of his opponents that were drafted through the written press and by various media such as the Russian government. that happened against Hillary Clinton directly at the time through the bad use of information from millions of users of the company **"Cambridge Analytica" who claimed to be the victim of a massive Cyber attack in 2018 during and at the end of the campaign that advised the now President Trump.**

**SPAIN (apro) .- The best 'Hackers' in Spain go from enlisting in the Rajoy cyber army.**

**The Government of the Popular Party of Spain finalizes the draft of a law proposal to create an organism that had never been launched in our country: a cyber-reserve with thousands of 'hackers' and experts in computer security ready to face new cyber attacks global.** The document was confirmed by the Spanish government itself, **but the problem: Are the best hackers ’in Spain, who should be a key part of this new security body, claim not to have the slightest interest in joining Rajoy's‘ cyber army ’**. They call the initiative "Wrong" and "Cheap Publicity". The project runs the serious risk of being born dead from the start because it is well known that there are governments that have recruited Developers and Experts in this area of Cybernetics and Cybersecurity and sometimes have been prisoners and some disappeared under investigations even been reported to International authorities **the most representative Example is the Australian Julianne Assange Co-Creator and Co-founder of WikiLeaks movement that succumbed to persecution and recent arrest at the end of his "Political Asylum" at the Ecuatorian embassy in London, United Kingdom and who during this period saw the birth of "Anonymous "**

**“Anonymous's latest campaigns have been to prioritize propaganda on social networks and then launch cyber attacks with minimal impact**” (C. Miller 2019 Annual Cibersecurity Report).

**The same "Inactivity" and "General Decline" are experienced** in Latin America, says the report. Anonymous Venezuela and Anonymous Brazil.

**MEXICO CITY (apro) .- Mexico activated the security protocol for cyber attacks seven times between September 2016 and July 2017,** the government of former President of Mexico Enrique Peña Nieto reported in its Fifth Government Report.

**"The National Cyber Incident Response Center (Cert-Mx) of the Federal Police activated the coordination protocol seven times,** with the aim of following up on cybersecurity-related operations during various important events," states the document delivered by the Presidency of the Republic to the Chamber of Deputies and Senators of Mexico.

Without specifying the occasions on which the protocol was activated, the Report shows in the chapter on National Security that cyber attacks are increasingly present on the agenda of security agencies, both civil and military, as also reported in the following reports from the **New President of Mexico Andrés Manuel López Obrador 2017-2018 where the message from the Office of the Attorney General of the Republic, Research and National Security Center (CISEN), Army and Navy have an international exchange to confront this new threat to national security** and that in the country they have given clear examples of the political and economic damage of these bad practices against Government companies such as

**the Cyber-attack on BANCOMEXT in January 2018, the Government Avoiding the Theft of 110 Million Pesos, avoiding an international transfer by SWIFT to the Standard Chartered bank in USA** added to 5 less serious Hacks to the Financial System of Mexico and the Recent Cyber Attack **to PEMEX in September 2019 that coincided with the dates of investigation and the subsequent arrest on February 12, 2020 in Spain of Emilio Lozoya Austin Graduated from Harvard for a case of Corruption and Links with Ilicity Activities.**

The document also ensures that the Mexican government made regulatory adjustments to **“Execute in Domestic territory”** the resolutions of the Security Council of the United Nations (UN) for the maintenance of international peace and security on the subject of Cybersecurity and Cyberattacks.

**In a pressnote entitled "The decline of hacktivism: Cyber-attacks of this Political-Economic nature fell 95% from 2015 to date globally"**, but there is a caveat in those countries where what appears to be a systematic tool **of "Hacktivism"** for political purposes still in 2020 and asks the question of what is happening at the moment **regarding the COVID-2019 pandemic and what is behind the war of accusations of Virus Manufacturing and Bioterrorism** among the more developed countries that currently questioned the **performance of the World Health Organization (WHO) "The fact that the cases with the most media impact put the spotlight on the US should not lead us to think that only from there do operations are planned and executed of massive espionage or selective monitoring of politicians or diplomats, friends or enemies "if not also in countries like Russia, China and the United Arab Emirates, as well as many other countries in America Central and Latin America”.**

Gustavo Ernesto Rodríguez De Lira
Founder IT Capital

Referencias Periodísticas y de Investigación (Research References & Journal)-
https://www.elconfidencial.com/tecnologia/2017-05-03/ciberguerra-espana-ciberataques-espionaje-hackers_1374693/

Documents for Download:
Full Article SPA/ENG
https://drive.google.com/file/d/16-U9JGXPH6o9J3k9kTTLcmcrnLdmL6SS/view?usp=sharing