Tendencias de Ciberseguridad 2022 - 2023

MSc. Ing. Mateo Martínez

www.kmhcorp.com

Contexto Internacional
COVID 19

INTERPOL

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

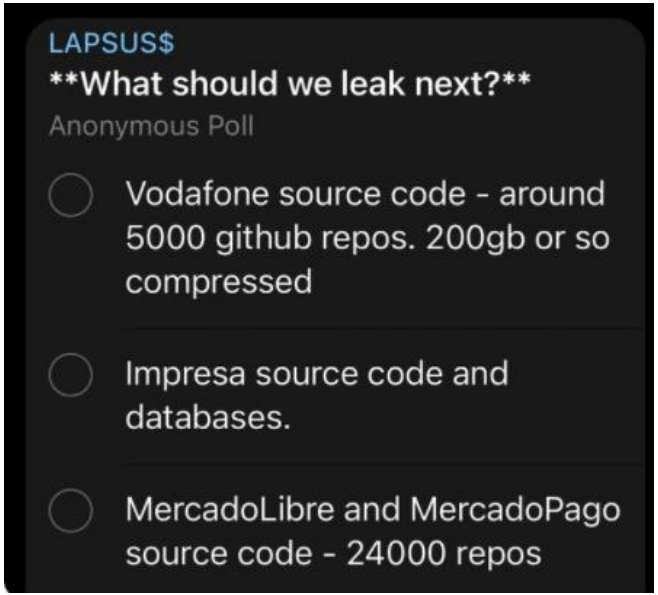
Jürgen Stock, INTERPOL Secretary General

Fuente: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Contexto Internacional
Russia - Ukraine

Immediately after the conflict broke out, suspected Russian-sourced cyber-attacks were observed over a 48-hour period at an increase of over 800%. U.S. [-] AFP VIA GETTY IMAGES

Contexto Internacional
Mercado Libre



Argentinian e-commerce giant Mercado Libre has confirmed "unauthorized access" to a part of its source code this week.

Mercado additionally says data of around 300,000 of its users was accessed by threat actors.

The company's announcement follows a poll by the data extortion group, Lapsus$ in which they threatened to leak data allegedly stolen from Mercado and other prominent companies.

Fuente: https://www.bleepingcomputer.com/news/security/e-commerce-giant-mercado-libre-confirms-source-code-data-breach/

Contexto Internacional

Log4j 2

NIST

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD **NIST:** NVD

Base Score: 10.0 CRITICAL

CVE-2021-44228 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

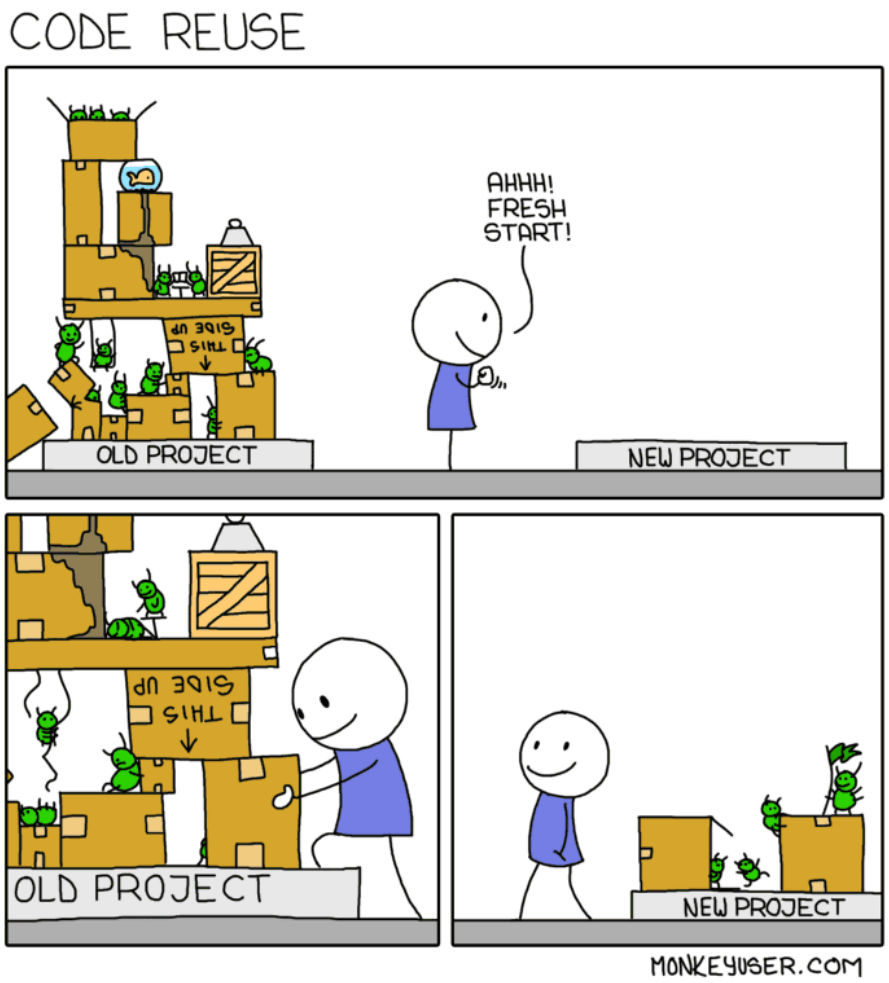
Current Description

Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. In previous releases (>2.10) this behavior can be mitigated by setting system property "log4j2.formatMsgNoLookups" to “true” or it can be mitigated in prior releases (<2.10) by removing the JndiLookup class from the classpath (example: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class).

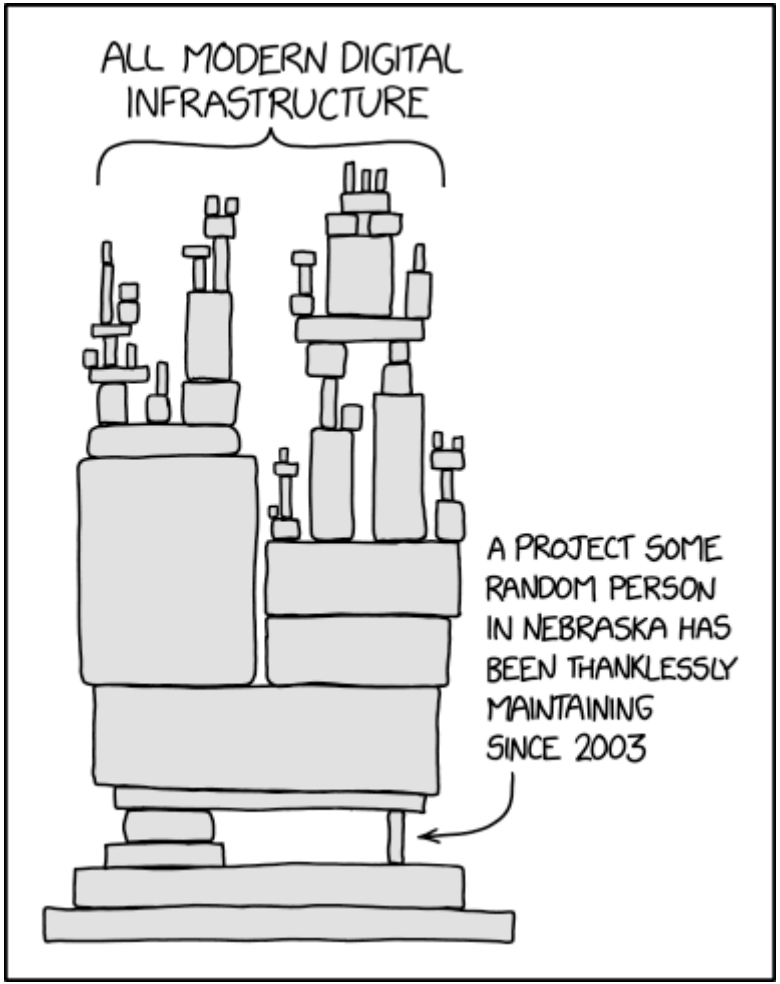
QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228
NVD Published Date:
12/10/2021
NVD Last Modified:
12/13/2021
Source:
Apache Software Foundation

Introducción



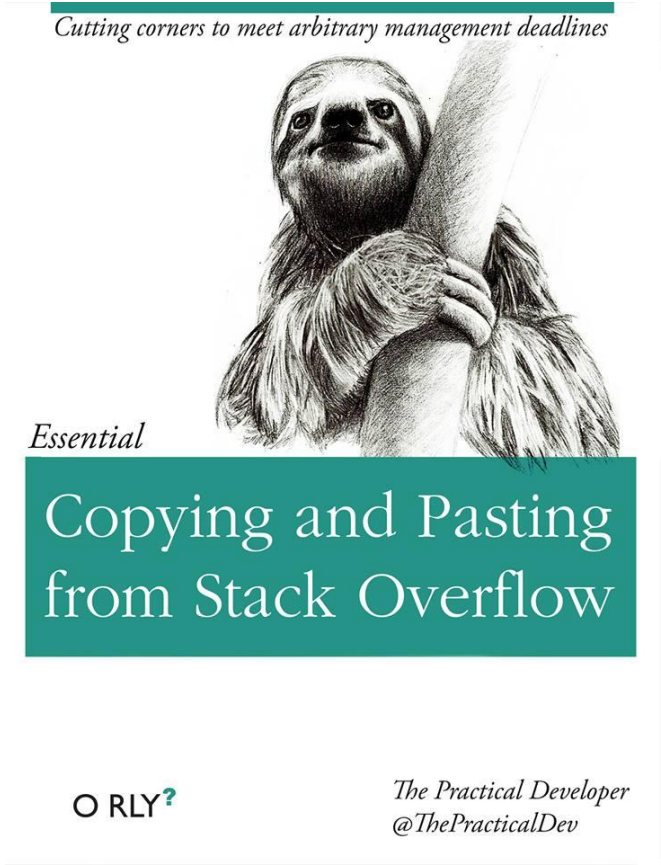
Introducción

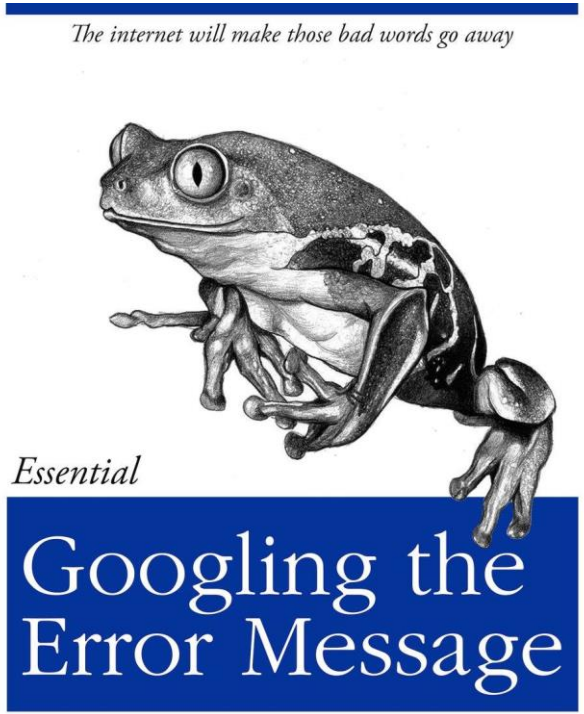


Introducción

Al crear una nueva aplicación, pocos programadores **(si es que existe alguno en el mundo)** escriben cada línea de código desde cero.

Introducción





Introducción

De hecho, muchas de las métricas centrales por las que se evalúa a un desarrollador de aplicaciones se benefician de la **reutilización del código** existente y las **bibliotecas externas**.

Introducción

Está presente en alrededor del **96%** de las aplicaciones y en promedio, el **79%** de todo el código en uso proviene de **bibliotecas de código abierto**

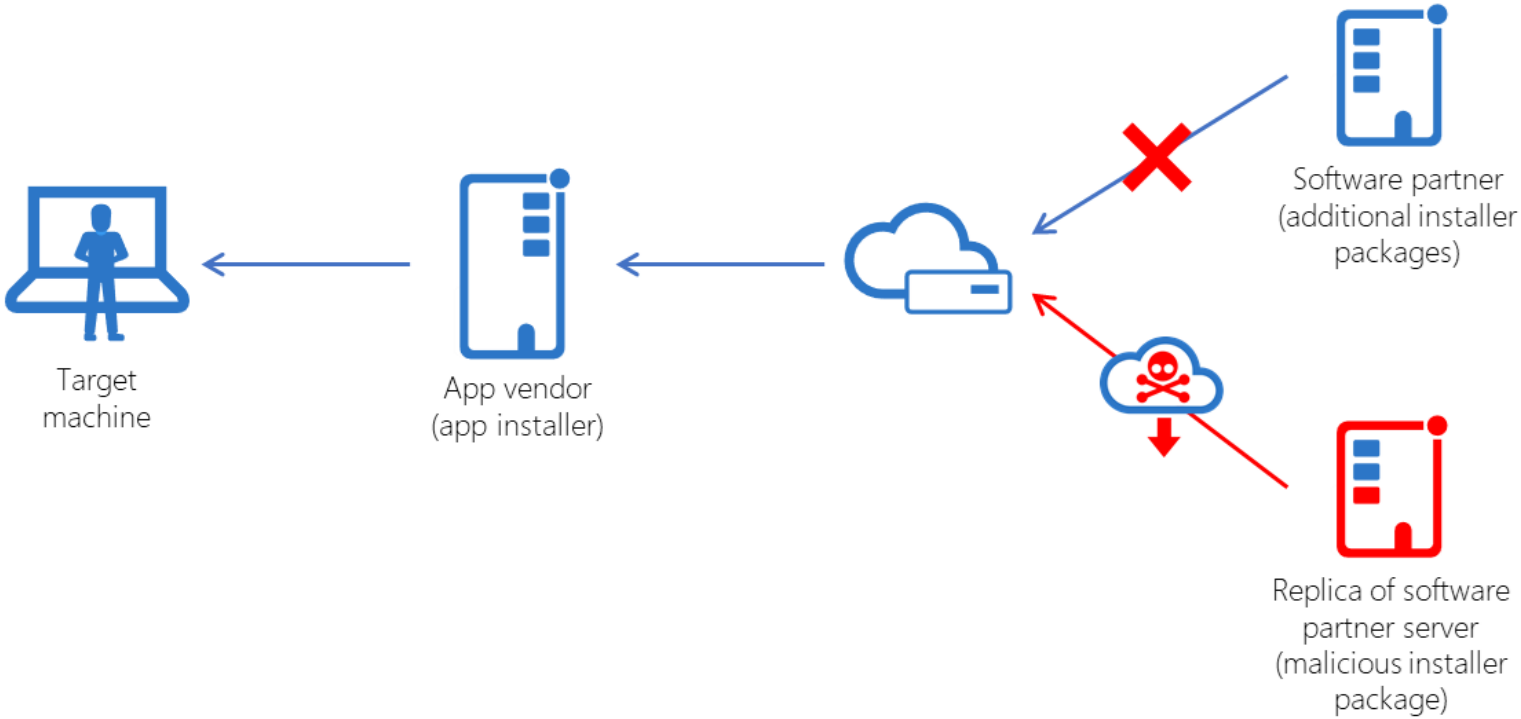
Introducción

85% con componentes out-of-date de más de 4 años!

Caso de Estudio: Solarwinds

El ataque **SolarWinds** se ha cubierto ampliamente durante los últimos meses, dirigido a SolarWinds y **comprometiendo el código en las actualizaciones** de software entregadas a sus clientes.

Caso de Estudio: Solarwinds

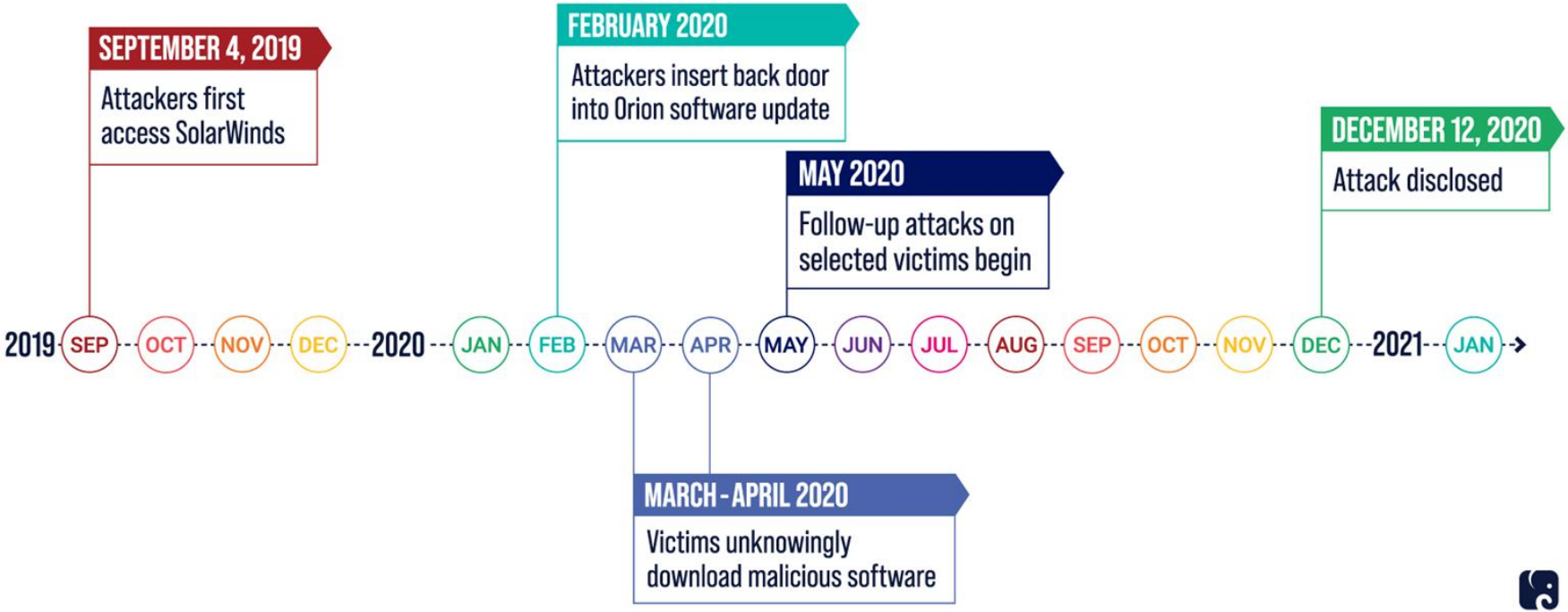


Caso de Estudio: Solarwinds

Los atacantes obtuvieron acceso por primera vez al entorno de desarrollo de servidores para la plataforma de administración de infraestructura SolarWinds Orion en septiembre de 2019, **14 meses antes de que se descubriera el ataque**.

Caso de Estudio: Solarwinds

Los atacantes fueron muy meticulosos en **cubrir sus huellas** y tomaron medidas extremas para permanecer **sin ser descubiertos.**



Caso de Estudio: Solarwinds

"At Microsoft, we have an **inner source approach** – the use of open source software development best practices and an open source-like culture – to making source code viewable within Microsoft. This means we do not rely on the secrecy of source code for the security of products, and **our threat models assume that attackers have knowledge of source code**. So viewing source code isn't tied to elevation of risk.

As with many companies, we plan our security with an **"assume breach" philosophy** and layer in **defense-in-depth protections** and controls to stop attackers sooner when they do gain access"

Protegiendo toda la cadena de suministro

Este evento también es un recordatorio de que las organizaciones **deben proteger todos los elementos de la cadena de suministro de software**, incluido:

- **Lo que escribe:** código personalizado desarrollado internamente
- **Con qué construye:** cientos de herramientas de desarrollo de software en uso en muchas organizaciones
- **Lo que compra:** aplicaciones de software como servicio (SaaS) listas para usar
- **Qué usa:** las numerosas bibliotecas de terceros de las que dependen la mayoría de las aplicaciones

Caso de Estudio: Event-stream

URGENT: SECURITY: New maintainer is probably malicious

Caso de Estudio: Event-stream

Un actor malintencionado se hizo cargo de un proyecto de código abierto publicado y **mantenido por un solo individuo**, **Event-stream**, que logró insertar código de ataque en la biblioteca de códigos distribuida a través de **NPM**, un popular administrador de paquetes para desarrolladores de Javascript.

Caso de Estudio: Event-stream

La propiedad de un paquete npm popular, event-stream, fue transferida por el autor original a un usuario malintencionado, **right9ctrl**. Este paquete **recibe más de 1,5 mm de descargas semanales y casi 1.600 paquetes más dependen de él**.

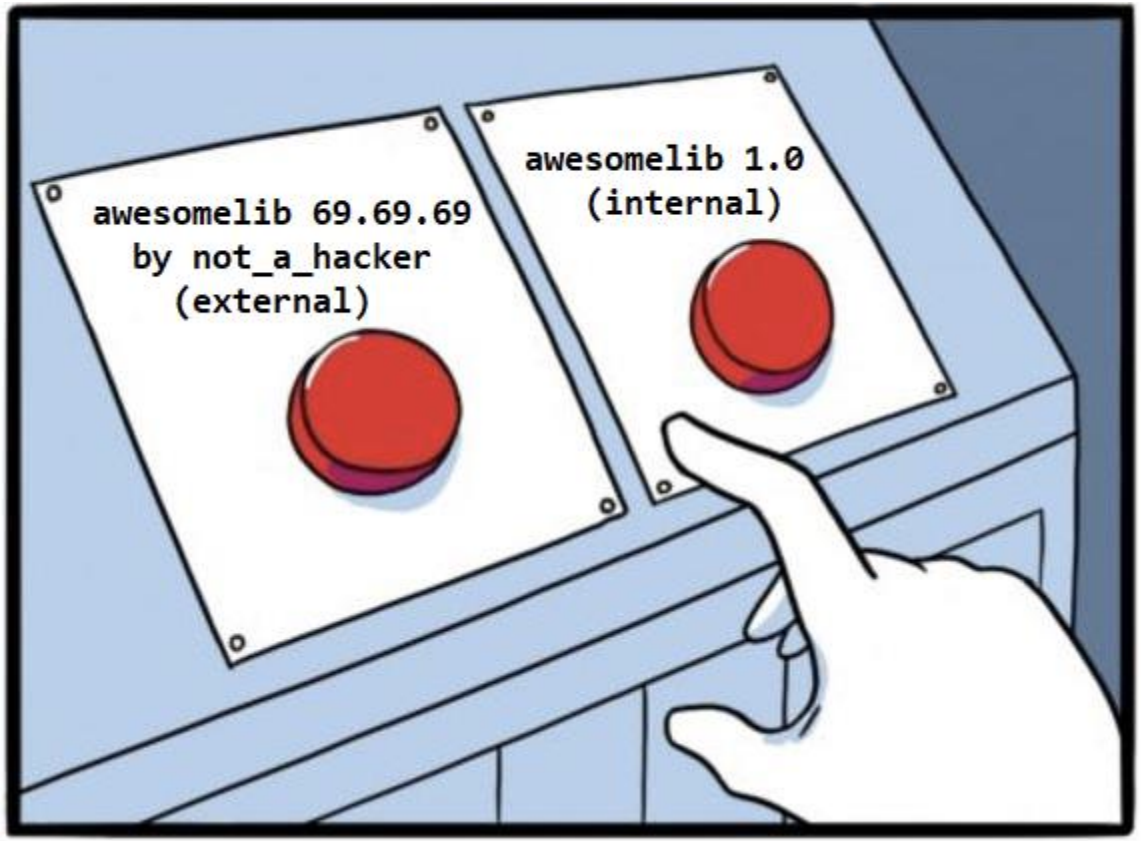
El usuario malintencionado pudo **ganarse la confianza del autor original** haciendo una serie de contribuciones significativas al paquete. La primera publicación de este paquete por parte del usuario malintencionado se produjo el 4 de septiembre de 2018.

Caso de Estudio: Event-stream

El usuario **modificó el flujo de eventos** para depender de un paquete malintencionado, **flatmap-stream**.

Este paquete fue diseñado específicamente para los propósitos de este ataque. Ese paquete contiene un archivo index.js bastante simple, así como un archivo index.min.js reducido. Los dos archivos en GitHub parecen lo suficientemente inocentes. Sin embargo, en el paquete npm publicado, la versión reducida del archivo tiene un código adicional inyectado. No hay ningún requisito de que el código que se carga en un módulo npm sea equivalente al código almacenado públicamente en un repositorio de git.

Librerías Privadas



Caso de Estudio: Apple & Microsoft

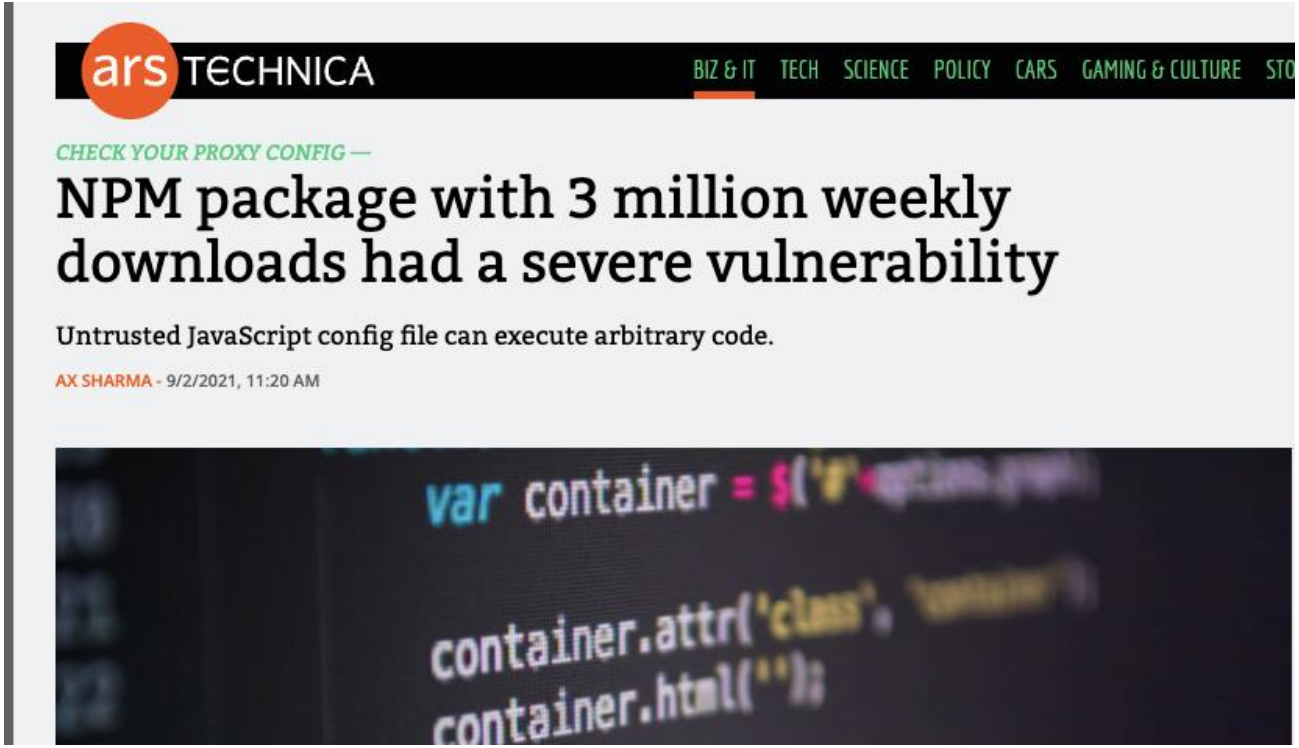
¿Qué es la confusión de dependencia? (Dependency Confusion)

El problema de confusión de dependencias es una falla de diseño inherente en las herramientas de instalación nativas y los flujos de trabajo de DevOps que atraen las dependencias a su cadena de suministro de software.

En este contexto, la confusión de dependencias se refiere a la incapacidad de su entorno de desarrollo para **distinguir entre un paquete actual privado creado internamente** en su compilación de software y un **paquete con el mismo nombre disponible en un repositorio de software público**.

https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

Caso: NPM



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

CHECK YOUR PROXY CONFIG —

NPM package with 3 million weekly downloads had a severe vulnerability

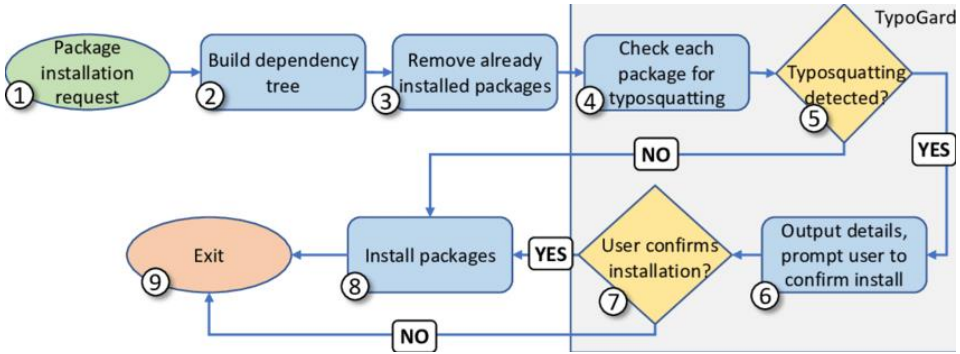
Untrusted JavaScript config file can execute arbitrary code.

AX SHARMA - 9/2/2021, 11:20 AM

https://arstechnica.com/information-technology/2021/09/npm-package-with-3-million-weekly-downloads-had-a-severe-vulnerability/

Typosquatting

Los atacantes crean paquetes maliciosos que se parecen mucho a los de los paquetes legítimos y luego los cargan, por ejemplo, en el repositorio de descargas de NPM. Por ejemplo, si hay un componente de código abierto llamado **"set-var"** que se utiliza para configurar el entorno operativo de una aplicación creada para un marco específico, un equipo malintencionado podría crear un clon de ese proyecto llamado **"setvar"** que incluye su código malicioso.



https://www.researchgate.net/figure/Modified-package-installation-process-with-typosquatting-protection_fig3_347749212

NVD

En promedio, una vulnerabilidad en un proyecto de código abierto tarda **54 días** en agregarse a la Base de datos nacional de vulnerabilidades (NVD) **después de ser divulgada públicamente**.

Diferencia de tiempo

Un atacante puede desarrollar un exploit para la vulnerabilidad **un par de semanas después de la divulgación pública**. Esto significa que los desarrolladores pueden continuar usando código vulnerable durante un mes después de que los ciberdelincuentes **comiencen a explotarlo antes de que una entrada en el NVD indique que es necesaria una actualización.**

SCA

SCA implica escanear una aplicación en busca de componentes de código abierto que contengan vulnerabilidades conocidas. Sin embargo, el **40%** de los desarrolladores **nunca realizan SCA** o **insisten en que nunca usan código de fuentes abiertas**.

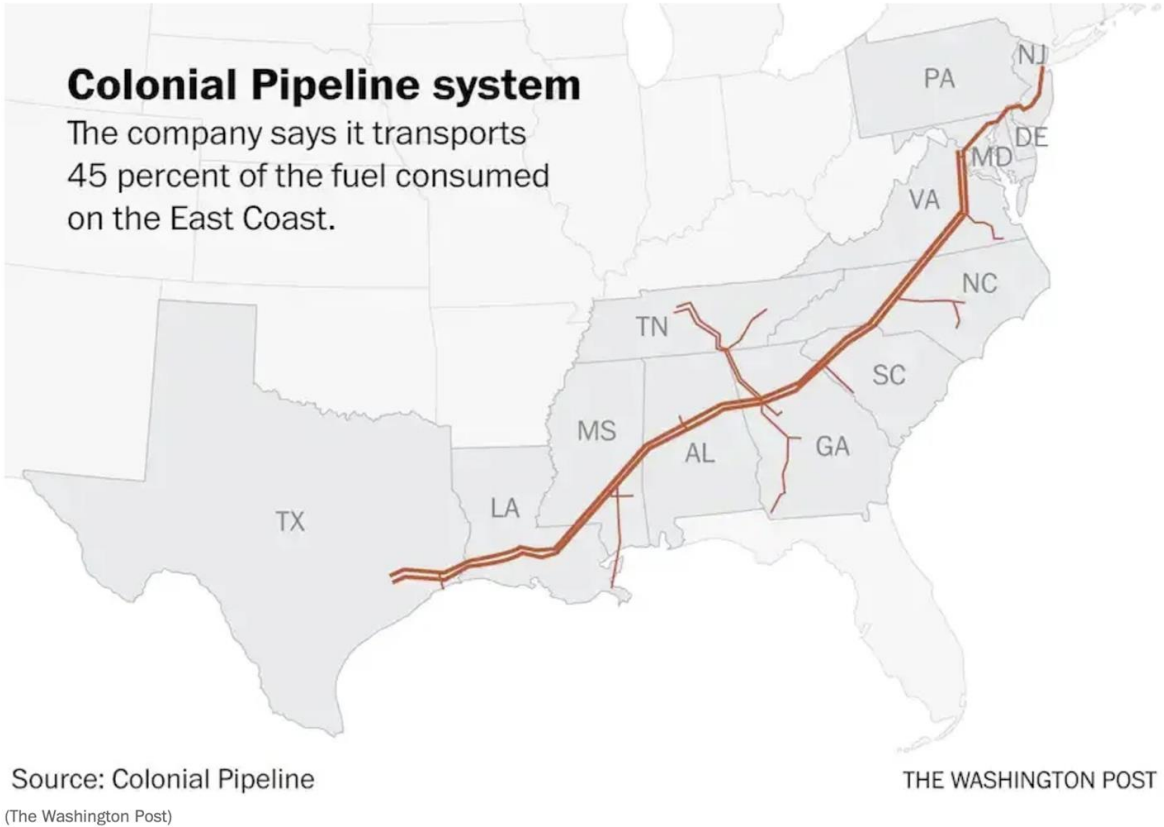
Contexto Internacional

Ransomware attack leads to shutdown of major U.S. pipeline system

The attack on top U.S. operator Colonial Pipeline appears to have been carried out by an Eastern European-based criminal gang

Fuente: https://www-washingtonpost-com.cdn.ampproject.org/c/s/www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/

Contexto Internacional



(The Washington Post)

Fraudes Financieros

Los delincuentes se contactan por mensajes privados y piden los datos de las cuentas.

También, en el caso de recibir una llamada de un representante del banco del que son clientes: no dar datos personales ni bancarios (claves, Token, números completos de tarjetas o cuentas), no realizar transferencias a cambio de futuros beneficios, e informar al banco si recibimos un contacto desde un canal no oficial.

infobae Últimas Noticias Política Sociedad Deportes Tecno Economía Gaming Educación Campo Tendencias Perros y gatos

ECONOMÍA

Alertan sobre una nueva estafa por correo electrónico que permite robar todos los fondos de una cuenta bancaria

El Banco Central alertó que los correos electrónicos que simulan ser legítimos y mensajes de texto falsos son técnicas habituales para acceder a cuentas bancarias. Recomendaciones para evitar el “phishing”

26 de Abril de 2021

Contexto Internacional

BBC Sign in | Home | News | Sport | Reel | Work

NEWS

Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories | En

Tech

Millions of hacked LinkedIn IDs advertised 'for sale'

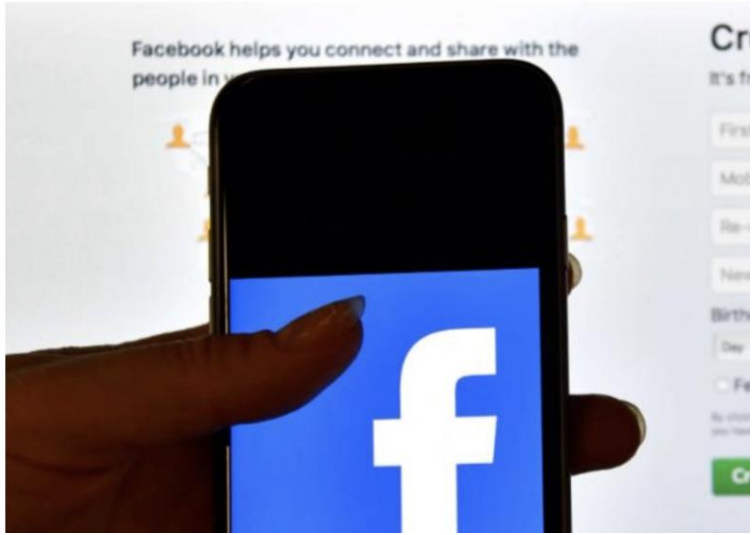
18 May 2016

CNN BUSINESS Markets Tech Media Success Perspectives Videos

Half a billion Facebook users' inform website, cyber experts say

By Donie O'Sullivan, CNN Business

Updated 1101 GMT (1901 HKT) April 5, 2021



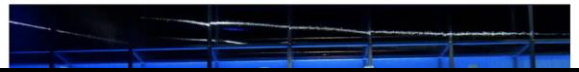
Contexto Internacional

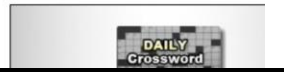
Sections | The Washington Post — Democracy Dies in Darkness | Get one year for $29

Business

Home | Share | 524

533 million Facebook users' phone numbers, personal information exposed online, report says





BBC | Sign in | Home | News | Sport | Reel | Worklife

NEWS

Home | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Sto

Tech

Facebook leak: Irish regulator probes 'old' data dump

59 minutes ago

Reality Check

CNN BUSINESS — Markets | Tech | Media | Success | Perspectives | Videos

Half a billion Facebook users' information posted on hacking website, cyber experts say

By Donie O'Sullivan, CNN Business

Updated 1101 GMT (1901 HKT) April 5, 2021

Facebook Leak

Más de **500 millones** de usuarios de **Facebook** de **106 países.** Esto incluye más de **32 millones** de registros de usuarios de EE. UU., **11.5 millones** en el Reino Unido y 6 millones en la India.

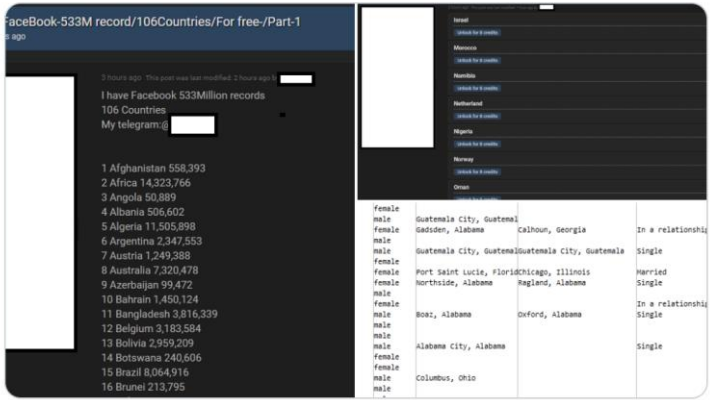
Facebook Leak

Alon Gal (Under the Breach)
@UnderTheBreach

All 533,000,000 Facebook records were just leaked for free.

This means that if you have a Facebook account, it is extremely likely the phone number used for the account was leaked.

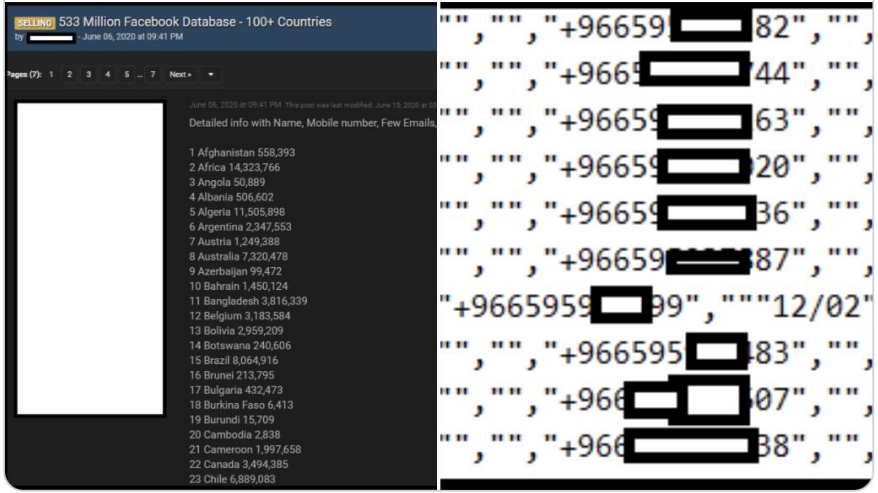
I have yet to see Facebook acknowledging this absolute negligence of your data.



Alon Gal (Under the Breach) @UnderTheBreach

In early 2020 a vulnerability that enabled seeing the phone number linked to every Facebook account was exploited, creating a database containing the information 533m users across all countries.

It was severely under-reported and today the database became much more worrisome 1/2



8:52 AM · Apr 3, 2021

Facebook Leak

A pesar de las afirmaciones de que los datos son "**antiguos**", es preocupante debido a la naturaleza invariable de los datos involucrados. Por ejemplo, es poco probable que los **números de teléfono** hayan cambiado para muchas personas en los últimos dos o tres años, y otra información, como la **fecha de nacimiento** o la ciudad natal, nunca cambia.

Facebook Leak

Número de Teléfono Completo

Facebook ID

Nombre

Apellido

Sexo

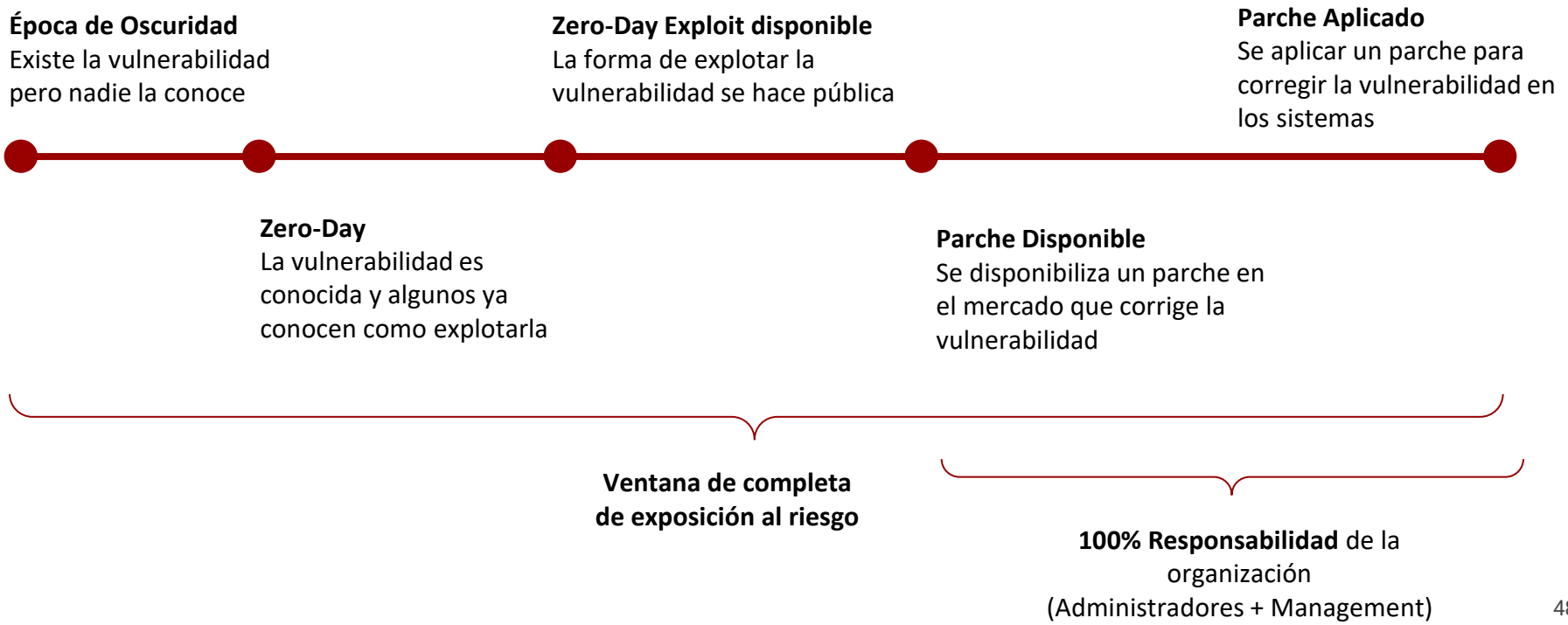
Estado Civil

Ciudad

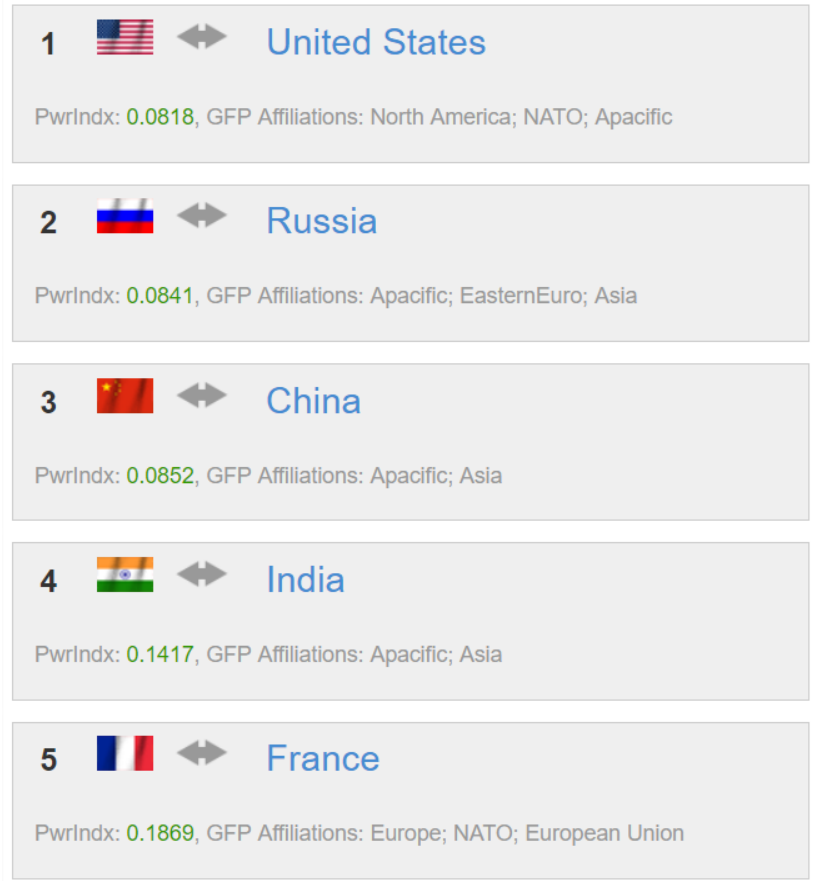
Trabajo/Estudio

E-Mail

Línea de Tiempo



Diferencias



Fuente: https://www.globalfirepower.com

Diferencias

TOTAL POPULATION: 326,625,791
AVAILABLE MANPOWER: 145,215,000
FIT-FOR-SERVICE: 120,025,000
REACHING MILITARY AGE ANNUALLY: 4,220,000
TOTAL MILITARY PERSONNEL: 2,083,100
ACTIVE PERSONNEL: 1,281,900
RESERVE PERSONNEL: 801,200

TOTAL AIRCRAFT STRENGTH: 13,362
FIGHTERS: 1,962
ATTACK: 2,830
TRANSPORTS: 5,248
TRAINERS: 2,856
TOTAL HELICOPTER STRENGTH: 5,758
ATTACK HELICOPTERS: 973

TOTAL NAVAL ASSETS: 415*
AIRCRAFT CARRIERS: 20
FRIGATES: 10
DESTROYERS: 65
CORVETTES: 0
SUBMARINES: 66
PATROL VESSELS: 13
MINE WARFARE: 11

Fuente: https://www.globalfirepower.com

Infraestructuras Críticas

- Una falla en los sistemas de Infraestructuras Críticas puede tener consecuencias catastróficas.
- Al aumentar las dependencias entre los diferentes sistemas, como por ejemplo, el suministro de agua depende de la electricidad para las estaciones de bombeo, la banca moderna que depende de las TIC y los servicios de bomberos que dependen del suministro de agua.
- Los efectos en cascada de una avería en un sistema en otros sistemas interconectados también deben contemplarse.
- Surge de la necesidad de minimizar las interrupciones críticas del servicio, los accidentes y, en particular, las fallas en cascada.

Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus

Through 2025, 30% of critical infrastructure organizations will experience a security breach that will result in the halting of an operations- or mission-critical cyber-physical system.

Fuente: https://www.gartner.com/en/doc/757423-predictive-analytics-cyber-security

Predicciones 2022 - 2023

Predicciones 2022 - 2023

- Ataques a grandes nubes (Amazon, Microsoft, Google)
- Ataques dirigidos a gobiernos con motivos políticos
- Ransomware masivo a organizaciones pequeñas y medianas
- Robo de cuentas de redes sociales corporativas sin 2FA (Instagram, Linkedin, Facebook, etc)
- Ataques utilizando ML & AI (deep fakes)
- Ataques más rápidos frente a nuevas vulnerabilidades detectadas
- Ataques utilizando zero days como consecuencia directa de situación Russia - Ukraine
- Ataques a aplicaciones financieras y fraudes
- Leaks de información

Predicciones 2022 - 2023

- Incorporación de tecnologías de ciberseguridad con capacidades de ML & AI
- Shift left de la seguridad en el desarrollo de software incluyendo SAST, SCA y DAST
- Optimización en la gestión de riesgos de ciberseguridad aún más alineados al negocio
- Menos planillas excel y más automatización de la ciberseguridad
- Mejoras en las campañas de concientización buscando ejemplos claros y reales
- Finalmente asumir la porosidad de nuestras redes considerando amenazas en red interna
- Incorporación de procesos de red team en grandes organizaciones
- SOC & CSIRT como servicios esenciales en organizaciones grandes
- Mayor nivel técnico en simulaciones y ejercicios a nivel gobierno y militares

Tendencias de Ciberseguridad 2022 - 2023

MSc. Ing. Mateo Martínez