Blockchain y Ciberseguridad

Autor: Manuel Marco Sanchez
Linkedin: https://www.linkedin.com/in/mmarcosanchez/

#finger

- Profesional de la Seguridad Informática, experto en hacking ético, linux, blockchain, Inteligencia Artificial, Telecomunicaciones , Voip, redes, programación, administración de servidores, asterisk.

  Soy especialista en desarrollo blockchain , ICO, aplicaciones y módulos de Seguridad Informática, Inteligencia Artificial,Base de datos , Sistemas, CRM, Aplicaciones Vozip para Asterisk ,FreePBX,Elastix,Issabel, así como software de control de call center.

UnderCon

La **UnderCon** fue un encuentro de hackers españoles, sobre todo aficionados al phreaking, que se celebró anualmente en Murcia, desde 1997 hasta 2004.

Es la primera convención de la escena hacker de la que se tiene noticia en España. Se celebraba en octubre, usualmente el Puente del Pilar, y la organizaban "hackers murcianos", según decían las crónicas, básicamente gente de CPNE y su grupo adyacente, La Katedral.

Es Seguro Blockchain y su Ecosistema

Revisemos los Hackeos Recibidos

- Unos hackers se llevan cerca de USD 480,000 de la plataforma blockchain Nuls (Diciembre 2019)
- VeChain pierde USD 6.6 millones en tokens VET debido a un ataque a su billetera de recompra (Diciembre 2019)
- En el año 2019 se vieron 12 grandes hackeos en los exchanges de criptomonedas. En total, se robaron más de 292 millones de dólares y más de 500.000 datos de clientes.
- Plataforma DeFi bloquea fondos de los usuarios por un error de tipeo (2020)

Las 5 vulnerabilidades más habituales de los Smart Contracts

- Errores Humanos.
- Errores aritméticos con números enteros
- Vulnerabilidades del límite de *block gas*
- Falta de parámetros o controles de precondición
- Frontrunning
- *Bugs* de lógica simples

Como Proteger Nuestro Entorno Blockchain

- Debemos Tener Como minimo Servidores :
    - Servidor de Produción.
    - Servidor de PreProdución.
    - Backup.
- Debemos Proteger Nuestras API :
    - El uso de APIs y de herramientas para su gestión son una tendencia cada vez más demandada a la hora de usar los modelos de IA.

estirdio de Akamai

    - El 83% de todo el tráfico web va a través de APIs (Fuente Estadio Akamai del 2019).
    - Segun la empresa consultora Gatnert en el año 2022 los abusos derivados de las APIs serán el vector de ataque más frecuente.

Te Gustaría que tu empresa apareciera

en el Listado del 2020

Top 10 Biggest Breaches in 2018

1. API: Aadhar — 1.1 billion
2. Marriott Starwood hotels — 500 million
3. Exactis — 340 million
4. MyFitnessPal — 150 million
5. Quora — 100 million
6. MyHeritage — 92 million
7. Cambridge Analytica — 87 million
8. API: Google+ — 52.5 million
9. Chegg — 40 million
10. API: Facebook — 29 million

Como Securizar una API

Eres Programador Aunque No sepas Como Se puede Hacer.

- OAuth 2.0 (Autorización abierta)
    - OAuth 2.0 es un método de autorización utilizado por compañías como Google, Facebook, Twitter, Amazon, Microsoft, etc. Su propósito es permitir a otros proveedores, servicios o aplicaciones, el acceso a la información sin facilitar directamente las credenciales de los usuarios. Pero tranquilo, únicamente accederán bajo la confirmación del usuario, validando la información a la que se le autorizara acceder.

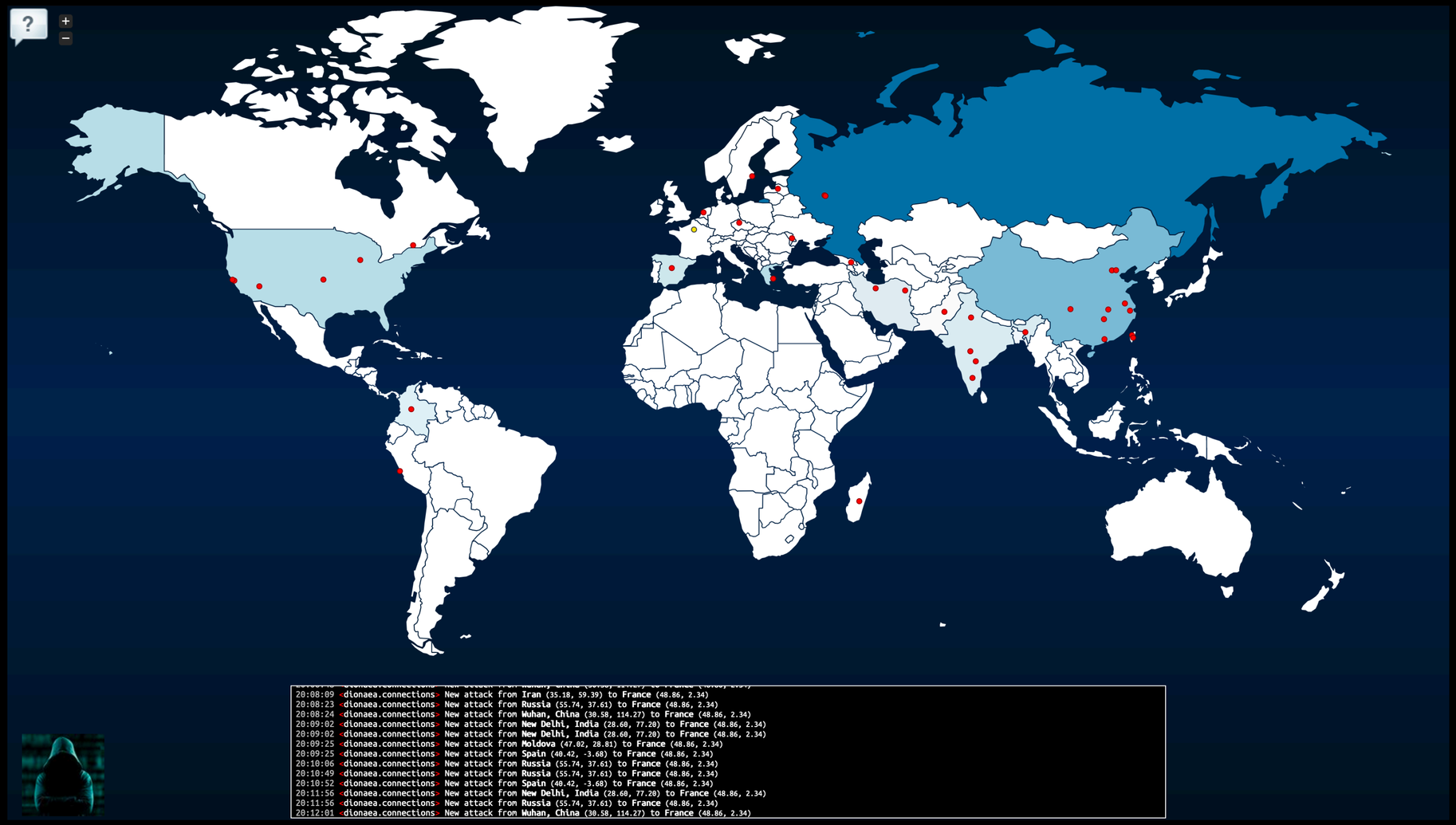
Una vez aprobada la autorización, esta aplicación de terceros podrá acceder a la información permitida mediante una autentificación con un token de acceso.

Puedes usar las bibliotecas cliente a continuación para implementar OAuth 2.0 en tu aplicación. Recomendamos usar una biblioteca de cliente en lugar de escribir tu propio código. El uso de estas bibliotecas de cliente estándar es importante para la seguridad y la seguridad de los usuarios y tu aplicación.

- Biblioteca cliente de API de Google para Java
- Biblioteca cliente de API de Google para JavaScript
- Biblioteca cliente de API de Google para Python
- Biblioteca cliente de API de Google para .NET
- Biblioteca cliente de API de Google para Ruby
- Biblioteca cliente de API de Google para PHP
- Biblioteca de OAuth 2.0 para Google Web Toolkit
- Controladores de OAuth 2.0 para Google Toolbox para Mac

También puedes seguir las instrucciones en la sección Invocación de YouTube Data API para modificar el código y así configurar correctamente los valores de token de OAuth 2.0.

- Tener un sistema de detección de ataques:



Ataques en Tiempo Real

- Sistema de Ataque Persistentes.
- Defensa Proactiva frente a la Reactiva.
- Ser conscientes de que alguna vez seremos hackeados con éxito nuestros sistemas deben estar preparados para sufrir el mínimo impacto y seguir dando servicio en un tiempo mínimo (Resilencia)
- Usar las nuevas tecnologías para preveer con antelación el próximo ataque (Inteligencia Artificial)

Consejos para los poseedores de criptomonedas y para los criptoinversores

Para evitar los problemas anteriores, estos consejos te pueden ser de ayuda:

-Verifica siempre la dirección web de un monedero

-Antes de enviar dinero, comprueba la dirección del destinatario, la cantidad a enviar y la comisión.

-Escribe un recordatorio que te permita recuperar contraseña de tu criptomonedero.

-Toma decisiones informadas cuando vayas a hacer una criptoinversión y no te precipites.

-Recuerda que las inversiones en criptomonedas son muy arriesgadas. No inviertas más de lo que estés dispuesto a perder y diversifica las inversiones.

-Usa monederos en hardware.

-Ten activa una protección antivirus.

Bibliografia y Referencias:

https://www.trustnodes.com/2019/01/10/bitcoin-0day-discovers-only-54-worth-of-bitcoin-14-xrp-and-0-00002-eth-are-vulnerable

https://www.technologyreview.es/s/10958/el-masivo-historial-de-robos-demuestra-que-blockchain-no-es-inhackeable

https://es.beincrypto.com/blockchain-creada-combatir-creciente-robo-indentidad-mundo-digital-opinion/

https://www.securityartwork.es/2020/03/10/las-5-vulnerabilidades-mas-habituales-de-los-smart-contracts/

https://www.20minutos.es/noticia/4184908/0/el-robo-de-criptomonedas-roza-los-10-000-millones-de-dolares-desde-2017/

https://www.criptonoticias.com/categorias/seguridad-bitcoin/robo-fraude/

https://www.fundacionctic.org/es/actualidad/blockchain-y-ciberseguridad

https://www.blockchaineconomia.es/blockchain-para-defensa-nacional/

www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari106-2019-alonsolecuit-seguridad-y-privacidad-del-blockchain-mas-alla-de-tecnologia-y-criptomoneda

http://infocoin.net/2019/05/09/piratas-informaticos-retiran-7-000-bitcoins-en-un-fallo-de-seguridad-en-binance-crypto-exchange/

https://ibermaticadigital.com/tecnologia-blockchain-para-securizar-la-generacion-de-documentos/

https://es.cointelegraph.com/news/hackers-grab-nearly-480k-from-blockchain-platform-nuls

https://es.cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year

https://es.cointelegraph.com/news/hacked-italian-exchange-altsbit-to-shut-down-in-may-2020

https://exchange.blockchain.com/es/security

https://101blockchains.com/es/herramientas-de-blockchain/

https://www.youtube.com/watch?v=9Rw5-uckRCY

https://www.youtube.com/watch?v=Td1yUu0EbGo

https://www.youtube.com/watch?v=yubGuNKSsIQ

https://www.youtube.com/watch?v=h5uCMlrZkSE

https://www.youtube.com/watch?v=9Zi8rTXATPQ

https://es.cointelegraph.com/explained/safety-in-the-blockchain-know-the-elements-that-make-it-up

https://www.criptonoticias.com/seguridad-bitcoin/plataforma-defi-bloquea-fondos-usuarios-error-de-tipeo/

PASEMOS

A LA VIDA REAL EN DIRECTO

Disclaimer

La información mostrada en esta demo real es sólo para fines educativos por lo cual no nos hacemos responsables por el uso indebido de la información contenida en ella.

Muchas Gracias a Todos!!!