De la Cruz Sierra Diana Paola

Noticias o casos relacionados a hackers

El término **hacktivismo** nace de la unión de dos palabras: hacker y activismo. Hace referencia al uso de la tecnología y de internet de forma no violenta, normalmente para reivindicar posturas políticas o sociales. Generalmente estos ataques están dirigidos a gobiernos, instituciones públicas y grandes entidades.

Noticia: 10/feb/2011. Los "hacktivistas" llegan a México por el caso Aristegui.

Un grupo de "hacktivistas" que asegura ser el brazo latinoamericano de la agrupación Anonymous lanzó un ataque virtual contra el sitio de noticias mexicano MVS en protesta por el despido de la periodista mexicana Carmen Aristegui.

La protesta fue bautizada como "Operación Tequila" y logró desconectar la página durante varios minutos utilizando un ataque de negación de servicio (DDoS, en ingles) que satura la conexión de un servidor hasta que éste deja de operar

"Esta protesta, sin precedente en México, tuvo un rotundo éxito gracias a la inmensa participación voluntaria de ciudadanos que están hartos con la situación actual del país", aseguró Anonymous Latinoamérica en un comunicado. Como ha ocurrido en otros países del mundo, los hactivistas aseguraron que realizan los ataques para defender la libertad de expresión.

https://www.bbc.com/mundo/noticias/2011/02/110210_1137_tecnologia_hactivistas_ataque_mvs_anonymous_operacion_tequila_dc

Noticia de hacker blanco: 20/08/21 Un hacker roba 600 millones a una empresa y la víctima le ofrece un contrato de trabajo tras su gran golpe

El ladrón ha devuelto parte del montante robado (aunque no su totalidad). En agradecimiento, la empresa le ha pagado medio millón y le han ofrecido un contrato de asesor jefe de seguridad

Un hacker ha llevado a cabo un audaz golpe gracias al que ha sido capaz de robar 600 millones de euros en criptomonedas.

La víctima fue la empresa Poly Network, una plataforma basada en tecnología blockchain para el intercambio de criptomonedas.

Cuando la empresa se dio cuenta de que les habían sustraído 600 millones, decidió marcar las transacciones de las criptomonedas robadas de forma que fuera casi imposible convertir este dinero en divisas.

Tras esta maniobra de la empresa, en un extraño giro de guión, el hacker decidió devolver la mayor parte del dinero que había robado a Poly Network, pero no la cantidad íntegra.

Sin embargo, la historia aun se vuelve más extraña. Según ha anunciado la propia Poly Network en su blog, la empresa ha explicado que han mantenido un contacto directo a diario con el hacker y que este les ha mostrado su "preocupación" por "la seguridad y la estrategia de despliegue de Poly Network".

Además de mantener una fluida comunicación con la persona que les robó, Poly Network ha entregado una recompensa de 500.000 dólares al hacker por devolver el dinero y por compartir los detalles de su modus operandi con la empresa.

https://www.elmundo.es/tecnologia/2021/08/19/611e2ffdfdddffc57f8b4574.html

Noticia: 30/may/2021 ¿Quiénes son el grupo de hackers que atacó la Lotería Nacional y cómo operan?

Hace unos días se informó que Avaddon, un grupo de hackers dedicados a la extorsión robó información de la Lotería Nacional y pidió un rescate para no revelar datos sensibles. El Avaddon es un ransomware as a service (RaaS) que fue reportado por primera vez en junio de 2020.

De acuerdo con información de Eset, el ransomware tuvo un gran impacto durante la pandemia y cuenta con una sólida reputación en los mercados negros. Este ransomware fue encontrado en correos de phishing con archivos adjuntos en formato ZIP que contienen un archivo javascript malicioso. Los correos de phishing, con archivos adjuntos en formato ZIP que contienen archivos javascript malicioso, fungen como los mecanismos de acceso inicial para que este ransomware entre en los servidores digitales.

Dichos correos cuentan con un mensaje en el cuerpo del correo que buscan despertar la curiosidad del usuario, como una supuesta foto o similar.

De la Cruz Sierra Diana Paola

De no entregar el rescate económico, Avaddon amenazó con dejar inhabilitado el sitio de la institución mediante un ataque de denegación de servicio distribuido (DDoS) que declina las operaciones de una página web, de acuerdo con información difundida por la firma de seguridad Seekurity.

https://www.reporteindigo.com/reporte/quienes-son-el-grupo-de-hackers-que-ataco-la-loteria-nacional-y-como-operan/

Diferencias entre hacker negro, gris y blanco

Un hacker de sombrero negro o Blackhat es una persona que intenta obtener una entrada no autorizada en un sistema o red para explotarlos por razones maliciosas. No tiene ningún permiso o autoridad para llevar a cabo sus objetivos. Intenta infligir daños al comprometer los sistemas de seguridad, alterar las funciones de los sitios web y las redes, o apagar los sistemas. A menudo lo hacen para robar u obtener acceso a contraseñas, información financiera y otros datos personales.

Los hackers de sombrero blanco, se les llama también hackers éticos porque prueban las infraestructuras de Internet existentes para investigar las lagunas en el sistema. Crean algoritmos y realizan múltiples metodologías para entrar en sistemas, solo para fortalecerlos. Los White Hats han sido históricamente fundamentales para garantizar que las grandes corporaciones hayan mantenido un marco de red sólido contra el resto de los intrusos informáticos. Desde ser empleados del Gobierno hasta ser consultores privados, los hackers blancos ayudan a que Internet sea un lugar mejor y más seguro.

El Grey Hat o hacker de sombrero gris se mueve entre los otros dos. Si bien no pueden usar sus habilidades para beneficio personal, pueden, sin embargo, tener buenas y malas intenciones. Por ejemplo, un hacker que piratea una organización y encuentra cierta vulnerabilidad puede filtrarla a través de Internet o informar a la organización al respecto. Todo depende del hacker. Sin embargo, tan pronto como los hackers utilizan sus habilidades de piratería para beneficio personal, se convierten en Black Hats.