UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS
DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

MATERIA:
SEGURIDAD DE LA INFORMACION

MAESTRO:
FRANCO LOPEZ VELARDE, EMMANUEL

TITULO DE INVESTIGACIÓN:
ACTIVIDAD 3: LA VIDA DESPUÉS DE WANNACRY

FECHA ENTREGA:
VIERNES 07 DE SEPTIEMBRE 2018

ALUMNO:
FELIPE DE JESUS RUIZ GARCIA

CODIGO:
214522077

CARRERA: INGENIERIA INFORMATICA (INNI)

SECCION: D02

CALIFICACIÓN Y OBSERVACIONES:

Indice

[RESUMEN] LA VIDA DESPUÉS DE WANNACRY

Cada vez se desarrollan maneras mas sofisticadas de invadir la privacidad, burlar sistemas de autentificacion y demas actividades no legales. La exponencial evolucion de los virus, troyanos, spyware, malware ….Desde el caso Israel hasta nuestros dias .
Creo que avanzan mas rapido los descubrimientos de vulnerabilidades por hackers sombrero negro, que ser descubiertas y parchadas por su industria, o dicho de otras palabras:
La industria no sabe que tienen un bug, hasta que este explota y deben liberar un parche, una solucion a algo evidentemente no planeado.
La vida despues de wannacry marco un antes y un despues, puesto que ha dejado claro, como no estamos preparados ante situaciones donde el peligro llega como la humedad, sin hacer ruido y en el momento menos esperado pierdes el acceso a tu informacion… como un jacke mate no esperado por un peon…
Wannacry nos dejo en claro como la confianza y subestimar de mas puede ser nuestro primer piedra en el camino; si bien, las amenazas informaticas estan a la orden del dia… Porque nosotros no ?

Y es gracias a estos desastres, informacion secuestrada de forma masiva, como las empresas, negocios y usuarios finales se toman en serio la seguridad, la prevencion y estar preparado: tener un plan.
Constante cambio, a medida que aumenta la capacidad de procesamiento de computo, tambien lo hacen las amenazas y es aquí donde entra el juego la preparacion:

before anything preparation is the key to success
- Alexander Graham Bell

Preparacion, eh ahi la clave: si bien, existen comunidades de hacker eticos, sombrero blanco, donde el conocimiento se difunde con el proposito de evitar una mala situacion. Podriamos prepararnos en como se estan desarrollando e implementando ataques, siendo participe en comunidades de hackers, buscando ese conocimiento, con el fin de ser victima del mismo.

Preparnos! Pensando correctivamente tambien, siempre en el peor de los casos… Porque no contemplo todos los detalles de una vez como si ya fuese victima ? Por ejemplo: Yo usuario Felipe con N teras de espacio disponible podria respaldar mi informacion de manera automatica, respaldo de tiempo real o usar tecnicas como en linux anacron con rsync podrian ser bastante efectivos. De esta manera, si ransomware secuestra mi informacion pues, el impacto seria minimo puesto que tengo esa informacion en otro lugar.

WannaCry fue esa piedra que se atraveso en el camino de muchos para ensenarles algo: usuarios y empresas ahora se estan tomando en serio el tema de la seguridad y claro, tener un plan B, restauracion… De cualquier manera,, estar al dia, la amenaza siempre estara un paso adelante… todo un reto, conocimiento, autosuperacion

[NOTICIA] Ransomware Infection Cripples Shipping Giant COSCO's American Network.

https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/

July 25, 2018

A ransomware infection has crippled the US network of one of the world's largest shipping giants —COSCO (China Ocean Shipping Company).

"Due to local network breakdown within our America regions, local email and network telephone cannot work properly at the moment," said the company in a press release. "For safety precautions, we have shut down the connections with other regions for further investigations."

But while the company described the incident as a "network breakdown," according to internal emails seen by several maritime news sites [1, 2], the company referred to the incident as a ransomware infection.
COSCO warns employees not to open suspicious emails

COSCO warned employees in other regions not to open "suspicious emails" and urged its IT staff to perform a sweep of internal networks with antivirus software.

The type of ransomware that infected the company's network is still unknown. COSCO did not respond to multiple requests for comment sent by Bleeping Computer.

The incident took place on Tuesday, July 24, but today, the company's American Region IT infrastructure was still down, including email servers and telephone network, according to a Facebook post. The company's US website was also down and was still down at the time of this article's publication.

The company's US employees have resorted to using public Yahoo email accounts to answering customer problems reported via social media.
Incident not as big as Maersk's NotPetya problems

COSCO is the world's fourth-largest maritime shipping company. A.P. Møller-Maersk, the world's largest shipping firm, also suffered a ransomware

infection last year when it was one of the NotPetya ransomware outbreak's largest victims.

Speaking at a panel on securing the future of cyberspace at the World Economic Forum held in January in Davos, Switzerland, Maersk's CEO said the company's engineers had to reinstall over 4,000 servers, 45,000 PCs, and 2500 applications over the course of ten days in late June and early July 2017, following the NotPetya outbreak.

The COSCO incident is much smaller in size and nature compared to Maersk's NotPetya troubles. Some of Maersk's shipments were trapped in some ports because of NotPetya, something that doesn't seem to have happened to COSCO, according to current reports.

[FEEDBACK] ESPECTACULACIONES

Claro esta, estamos espuestos a ser vulnerados en un ataque informatico... quiza ya lo estamos y no lo sabemos. Por ello, debemos enforcarnos en resguardanos de todo y en todo momento;
obtener la ultimas actualizaciones del software, estar al dia con los CVS estar al dia con las noticias de seguridad. Estar “Un paso adelante” en una situacion critica en el mundo evolutivo de los ransomware.